Green Banking in India: A Study of Various Strategies Adopt by Banks for Sustainable Development

Dipika[1]

[1]*Department of Management Studies, Ganga Institute of Technology and Management, Kablana, Jhajjar, Haryana, INDIA*

Abstract: In this present scenario of globalization, as we pass through 21st century, one thing that we miss very badly is the depletion of greenery. As everybody in this society is becoming more and more concerned and worried about the natural environment, business organizations and corporations have started modifying their working in an attempt to increase greenery to the maximum possible. Green banking means combining operational improvements, technology and changing client habits in banking business. It means promoting environmental-friendly practices. This comes in many forms such as – using online banking instead of branch banking; paying bills online instead of mailing them; opening up CDs and money market accounts at online banks, instead of large multi-branch banks; or finding the local bank in the area that is taking the biggest steps to support local green initiatives. Main emphasis has been made on the concept and scope of green banking in India so as to make our environment human friendly and enrich our economic productivity. This study also covers the recent developments are made by Indian banks for sustainable development and challenges faced by banks in implementation. The research is based on the secondary data. Coming to the findings, there is utmost need to create awareness, implement and follow green banking as much as possible in today's business world of innovative technologies so as to make our environment human friendly and enrich the sustainability.

Key Words: Green banking, Sustainable Development, CD's, Green Mortgage, Green Loan

I. INTRODUCTION

Green Banking is a new phenomenon in the financial world. Banks as the financing agent of the economic and developmental activities have an important role in promoting overall sustainable development. Green banking is the term used by banks to make them much more responsible to the environment. The term green banking means developing inclusive banking strategies which will ensure sustainable economic development.

Green Banking entails banks to encourage environment friendly investments and give lending priority to those industries which have already turned green or are trying to go green and, thereby, help to restore the natural environment. Green banking means combining operational improvements, technology and changing client habits in banking business. It means promoting environmental-friendly practices. This comes in many forms such as – using online banking instead of branch banking; paying bills online instead of mailing them; opening up CDs and money market accounts at online banks, instead of large multi-branch banks; or finding the local bank in the area that is taking the biggest steps to support local green initiatives. Foreign banks are practicing green banking on a much serious note. The Indian banks are still taking baby steps into this form of banking. Still, many of them are keen to actively pursue this strategy.

For example, an investment in a factory that pollutes heavily (and passes on the costs to the society at large) will generally have a higher financial rate of return than a factory that invests in expensive pollution control technology, as a result showing a lower rate of return. How will banks assess the two and which one of the two will be considered first for lending, although everyone knows that the second case will clearly be a better investment option in the long run?

II. ENVIRONMENTAL SUSTAINABILITY

The concept of environmental sustainability started in 1969 with the establishment of the National Environmental Policy Act (NEPA, 2014) in the United States whose purpose is to promote the general welfare, to maintain productive harmony between man and nature and to fulfill the economic and social welfare of the present and future generations.

III. GREEN BANKING

Green Banking is like a normal bank, which considers all the social and environmental factors; it is also called as an ethical bank. Ethical banks have started with the aim of protecting the environment. These banks are like a normal bank which aims to protect the environment and it is controlled by same authorities as what a traditional bank do. There are many differences compared with normal banking, Green Banks give more weight to environmental factors, their aim is to provide good environmental and social business practice, they check all the factors before lending a loan, whether the project is environmental friendly and has any implications in the future, you will awarded a loan only when you follow all the environmental safety standards.

Defining green banking is relatively easy. Green Banking means promoting environmental – friendly practices and reducing your carbon footprint from your banking activities. This comes in many forms

1. Using online banking instead of branch banking.
2. Paying bills online instead of mailing them.
3. Opening up accounts at online banks, instead of large multi-branch banks
4. Finding the local bank in your area that is taking the biggest steps to support local green initiatives.

IV. GREEN BANKING PRODUCTS

Green Loans: means giving loans to a project or business that is considered environmentally sustainable.

Green Mortgages*:* refers to type of mortgage that provides you a money-saving discount or a bigger loan than normally permitted as a reward for making energy-efficient improvements or for buying a home that meets particular energy-efficiency standards.

Green Credit Cards: Be it in form of environmentally friendly rewards or using biodegradable credit card materials or promoting paperless banking, credit cards are going green.

Green Saving Accounts: In case of Green Saving Accounts, banks make donations on the basis of savings done by customer's .The more they save, the more the environment benefits in form of contributions or donations done by banks.

Mobile banking and online banking: These new age banking forms include less paperwork, less mail, and less travel to branch offices by bank customers, all of which has a positive impact on the environment.

V. THE EMERGING TREND OF "GREEN BANKING"

The term "Green Banking" is being heard more often today. According to Indian Banks Association (IBA, 2014) "Green Bank is like a normal bank, which considers all the social and environmental / ecological factors with an aim to protect the environment and conserve natural resources". It is also known as ethical bank or sustainable bank. Green banking can benefit the environment either by reducing the carbon footprint of consumers or banks. On-line banking is an example of an initiative of Green Banking.

Benefits of online banking include less paperwork, less mail and less driving to branch offices by bank customers, which all have a positive impact on the environment. Interestingly, online banking can also increase the efficiency and profitability of a bank. A bank can lower their own costs that result from paper overload and bulk mailing fees if more of their customers use online banking. Green banking also can reduce the need for expensive branch banks. Green banking is also gaining importance in recent times. Most of the banks are undergoing computerization, networking, and offering of online banking to customers reduces the use of paper directly and indirectly resulting in pollution control.

Banks can also support eco-friendly groups, offer green lending and raise money for local environment initiatives. Banks that go to these significant lengths to be Eco-friendly are a little more difficult to find than the banks that claim to be green by merely offering online services. Banks that offer rate incentives on Certificates of Deposits, money market accounts, online savings accounts and checking accounts for online banking also help the green banking cause by rewarding online banking customers.

There has been a remarkable improvement in the working of banks in terms of cutting costs, increasing productivity, improving the profitability, controlling and management of the Non-Performing Assets (NPAs), face the risks, carry out the Asset Liability Management, manage the changes in interest rates, handle the foreign exchange rate fluctuations, comply with the regulator's requirements and finally improve the customer service to their best satisfaction. Hart & Ahuja (1996 studied a positive correlation between environmental performance and financial performance. Initially, banks were doing analysis of their financial performance only, but now it is a time to do analysis of social and environmental performance as well. Green Banking is not only a CSR activity of an organization, but also it is about making the society habitable without any considerable damage.

Internationally and domestically, several voluntary guidelines have been set up for the categorization, assessment and management of environmental and social risk in project financing like Equators Principles, National Environment Policy Act, World Bank E&S Norms, Carbon Disclosure Project, CERCLA, ISO 14000, BSE Greenex, etc.

The Financial Times and International Finance Corporation (IFC), a member of the World Bank Group had launched the Sustainable Finance Awards for the institutions that are integrating social, environmental and corporate governance considerations into their business operations.

The awards highlight the partnership between financial and non financial companies that are finding commercially viable and innovative solutions to sustainability challenges. The five categories of Sustainable Finance awards as per Financial Times (www.ft.com) are:-

- Sustainable Bank of the Year
- Technology in Sustainable Finance
- Sustainable Investment of the Year
- Sustainable Investor of the Year
- Achievement in Inclusive Business

Despite many initiatives taken in the field of Green Banking, it has been found to be at the nascent stage in India.There is only one Indian organization Infrastructure Development Finance Company (IDFC) Ltd, which has signed. Equators Principles for determining, assessing and managing the environmental risks in the projects undertaken (Equator Principles Association, 2014). The section of literature review gives a holistic picture of studies conducted in the field of Green Banking in India and abroad.

VI. REVIEW OF LITERATURE

According to RBI (IRDBT, 2014), green banking is to make internal bank processes, physical infrastructure and IT infrastructure as effective and efficient as possible, with zero or minimal impact on the environment. They had introduced green rating standards for Indian banks, which are termed as 'Green Coin Ratings'. Under this rating system, banks are judged on the basis of carbon emissions from their operations and on the amount of recycling, refurbishment and reuse material being used in their building furnishings and in the systems used by them like servers, computers, printers, networks, etc.They are also being judged on the amount of green projects finance by them and rewards or recognitions given to borrowers for turning their businesses greener.

Green banking services helps the banks towards the sustainable developments of the banks. In this context many authors expressed their opinions on the previous and recent developments and trends in the banking sector relating to the green banking.

Jeucken (2001) highlighted important differences between regions, countries and banks with regard to sustainable banking. Jeucken identified four stages: defensive, preventive, offensive and sustainable banking.

Chowdari Prasad (2002) has studied the Impact of Economic Reforms on Indian Banking and suggested how banking sector will face the changes and challenges.

Hopwood, 2005, highlighted the need for change it would be agreed that transformation in the usual model for the sustainable development is essential in order to understand the evolution of the banking sector towards sustainability.

McKinsey & Co. (2007) On the top of all these, there is certainly the aspect of profitability and productivity for all these banks to achieve.

Douglas (2008) found four key findings: (a) banks are increasingly discussing climate change business opportunities in their annual reports, (b) twenty eight of the forty banks have calculated and disclosed their greenhouse gas emissions from operations, (c) growing demand for climate friendly financial products and services is leading banks into new markets, and (d) investment banks have taken a leading role in supporting emissions trading mechanisms and introducing new risk management products.

Sudip Kar Purkayastha (2010) Such measures also yield the banks in offering top class service to attain Customer Satisfaction, particularly at a time there is stiff competition amongst the different types of banks, i.e., Public, Private, Foreign and others.

Mohmed Aminul Islam (2010) Green Banking is also gaining importance in recent times. While the banking industry is undergoing computerization, networking and offering of on-line banking is naturally gaining momentum.

Ela Sen (2010)Besides several benefits of computerization like speed, accuracy, ambience, efficient handling of sizeable business, etc., there is a factor like paper-less business resulting in waste management, eco-friendliness and pollution control.

Goyal KA and Vijay Joshi (2011) One side bankers are expecting more business through customer satisfaction but on the other side, the technology effect makes the customers not coming to the bank but bank is going to the doorstep of the customers

Nigamanda Biwas (2011) interpreted Green Baking as combining operational improvements, technology and changing client habits in market place. Adoption of greener banking practices will not only be useful for environment but also benefit in greater operational efficiencies, a lower vulnerability to manual errors and fraud and cost reductions in banking activities. He stated that the concept of green baking will be mutually beneficial to the banks, industries and economy. Not only green banking will ensure the greening of the industries but it will also facilitate in improving the asset quality of the bank in future. He has listed several benefits of green banking.

Alice Mani (2011) indicated that as Socially Responsible Corporate Citizens (SRCC), banks have a major role and responsibility in supplementing governmental efforts towards substantial reduction in carbon emission. Bank’s participation in sustainable development takes the form of Green Baking.The author examined and compared the green lending policies of banks in India in the light of their compliance and commitment to environment protection and environment friendly projects. It was opined that Banks in India can implement green lending.

(UNEP) Green Finance or Green Banking refers to diverse financial services and products provided by financial institutions for sustainable development (UNEP FI, 2007).

Green finance was firstly raised at the beginning of 1990’s, when the United Nations Environment Program (UNEP) worked with industry to develop environmental management strategies that they were convinced that the financial industry maintaining their businesses might have a significant influence to the environment (UNEP FI, 2010). In fact, this concept has been mentioned for several years. But to date, it has not yet been normatively defined by any international bodies, as it depends on specific financial entity allocating capital to specific purpose with integrating environmental and sustainability factors. There are some major concerns about environmental issues. Therefore, organization needs to pay attention to their outputs whether they are violating environmental issues or not. At SBI Bank, it is believed that profit should not be earned at the expense of the world's most pressing environmental problems.

That is why they finance organizations from organic food and farming businesses and pioneering renewable energy enterprises, to recycling companies and nature conservation projects.Citizens Bank of Canada has lowered its interest rate on loans for carbon emission cars. These kinds of efforts will surely motivate other banks to promote green banking and consequently in long run environmental issues can be resolved.

Jha & Bhome (2013) did the empirical study on the steps that can be taken for going green in the banking sector and to check the awareness among bank employees, associates and the general public about green banking concept. They did this study by collecting data from 12 bank managers, 50 bank employees and 50 general customers. The authors were of the opinion that online banking, green loans, power saving equipments, green credit card, use of solar and wind energy and mobile banking were some of the strategies that should be followed for going green. The results of the study were, banks should adopt environmental standards of lending, which results in improving the asset quality of banks. The rate of interest on loans given for green projects should comparatively less than the normal rate of interest. Companies can increase their profitability by reducing or recycling of waste generated and also by adopting sustainable measures to go green.

Dharwal & Agarwal (2013) studied that green banking is a key in mitigating the credit risk, legal risk and reputation risk. The author had suggested some green banking strategies like carbon credit business, green financial products, green mortgages, carbon footprint reduction (paperless banking, energy consciousness, mass transportation system, green building), and social responsibility services towards the society.

Malu, Agrawal, & Jajoo (2014) studied that banks can play an important role in reducing the carbon footprint in the society. Earlier economic development means reducing poverty, inequality and unemployment in the society, but the concept of Economic development had changed to Sustainable development which means “development that meets the needs of the present without compromising the ability of future generation to meet their own needs (World Commission Environment and Development 1987).The study suggested that sustainability in the banking sector can take two forms-

1. Banks can change their routine operations through recycling programs, paperless banking, using energy efficient resources, and support for community events for reducing pollution and so on.

2. They can adopt lending and investment strategies to promote environmentally responsible projects and can also develop green products to ensure the sustainability in their core business.

Vikas Nathi, Nitin Nayak & Ankit Goel (2014) concluded that India is running behind their counterparts from developed economies. They have started adopting green practices, but still their impact on the environment is increasing. Green banks are at start up mode in India. They should expand the use of environmental information in their business operations, credit extension and investment decisions. The endeavor will help them proactively improve their environmental performance and creating long term values for their business.

T.Rajesh and A.S. Dileep (2014) concluded that Green Banking is an umbrella term referring to practices and guidelines that make banks sustainable in economic, environment, and social dimensions. Green banking can be an avenue to reduce pollution and save the environment aiding sustainable economic growth. Before making the decision to finance a project, banks must see its environmental risks and ensure the project players have environmental safety measures in their plans, including recycling facilities or smoke and gas arresting units. A framework of incentives for responsible banks and disincentives for pollutants is an essential element for the development of green banking.

VII. OBJECTIVES OF THE STUDY

a) To understand how the green banking strategies are developed by Indian banks.

b) To find out the challenges in implementation of green banking in India.

c) To find out the necessary steps required for proper implementation of green banking in India.

VIII. METHODOLOGY

This is an exploratory research thus methodology was based on literature review and secondary data. The research took place in two phases: The first phase was an up-to-date literature review on Green Banking and sustainable development in the banking sector and particularly in green banking that identified results, and suggested future steps. The second phase included data collection about Indian banks through secondary published sources . Secondary published sources were the reports on Green Banking and other relative information published on the banks and other internet sites.

IX. SCOPE OF GREEN BANKING IN INDIA

There has been a remarkable improvement in the working of banks in terms of cutting costs, increasing productivity, improving the profitability, controlling and management of the Non-Performing Assets (NPAs), face the risks, carry out the Asset Liability Management, manage the changes in interest rates, handle the foreign exchange rate fluctuations, comply with the regulator’s requirements and finally improve the customer service to their best satisfaction. Green banking avoids as much paper work as possible and rely on online/ electronic transactions for processing so that we get green credit cards and green mortgages. Less paperwork means less cutting of trees. It also involves creating awareness to banking business people about environmental and social responsibility enabling them to do an environmental friendly business practice.

Benefits towards the banks: Green banking is very important in mitigating the following risks involving the banking sector:

a) Credit Risk: Due to climate change and global warming, there have been direct as well as indirect costs to banks. It has been observed that due to global warming, there have been extreme weather conditions which affect the economic assets financed by the banks, thus leading to high incidence of credit default. Credit risk can also arise indirectly when banks lead to companies whose businesses are adversely affected due to changes in environmental regulation.

b) Legal risk: Banks, like other business entities, face legal risk if they do not comply with relevant environmental regulation. They may also face risk of direct lender liability for cleanup costs or claims for damages in case they actually take possession of pollution causing assets.

c) Reputation Risk: Due to increasing environmental awareness, banks are more prone to reputation risk, if their direct or indirect actions are viewed as socially and environmentally damaging. Reputation risks emerge from the financing of environmentally objectionable projects.

Benefits of Green Banking in India

a) Avoids Paper Work: Paperless banking almost all banks in India are computerized or operate on a core banking solution (CBS). Thus there is ample scope for the banks to adopt paperless or less paper for office correspondence, audit, reporting etc. these banks can switch over to electronic correspondence and reporting thereby controlling deforestation.

b) Creating Awareness to Business People about Environment: Many NGOs and environmentalists are propagating environment consciousness among the public in general by arranging awareness programs and organizing seminars etc. Banks may associate themselves by sponsoring such programs. Besides, many corporate bodies are organizing similar program in their own line of business such as “free pollution check program” organized by a car manufacturer. Banks may tie with such corporate. These will help to brighten the image of the bank.

c) Loans at Comparatively Lesser Rates: Banks can also introduce green bank loans with financial concessions for environment friendly products and projects such as fuel efficient vehicles, green building projects, housing and house furnishing loans to install solar energy system etc.

d) Environmental Standards for Lending: Banks follow environmental standards for lending, is really a good idea and it will make business owners to change their business to environmental friendly which is good for our future generations.

e) Creating Awareness to Business People about Environment; Many NGOs and environmentalists are propagating environment consciousness among the public in general by arranging awareness programs and organizing seminars etc. Banks may associate themselves by sponsoring such programs.

f) Loans at Comparatively Lesser Rates : Banks can also introduce green bank loans with financial concessions for environment friendly products and projects such as fuel efficient vehicles, green building projects, housing and house furnishing loans to install solar energy system etc.

Other Benefits:

- Improving the service standards

- Automation of manual tasks
- Attracting and retention of staff
- Increase in profitability &sales
- Reducing Cycle time
- Drive customer loyalty
- Reduce costs to serve and sell
- Reduce administrative burden

X. GREEN BANKING STRATEGIES ADOPTED BY INDIAN BANKS

Green Banking in India:

The Reserve Bank of India document titled 'Policy Environment' dated 8th November, 2010 includes on Pages No. 56 and 57 a reference to Green Banking and Green IT initiatives for banks in India. Like any other Corporates, banks in India too are adopting the principle of Corporate Social Responsibility (CSR) and are concerned about the protection of environment. Mainly, the computerized environment and facilities like on-line banking are helping the banks to promote the green banking concept [Shalini Mehta (2011)]. Paper work is being reduced consciously at all levels by bankers and customers. In addition to providing of on-site and off-site ATMs, some banks have gone ahead with innovative ideas like installing Bio-metric ATMs, Solar-based ATMs, White-labelled ATMs, Brown ATMs, SMS alerts, Mobile Banking etc. for the convenience of their customers [Ashok Singh (2010)]. Besides reducing any environmental pollution, these initiatives are helping the banks in reduction in their cost of operations and delays which results in increased customer satisfaction too [Devaprakash R. (2008)]. While offering several simple suggestions for practicing green banking arrangements, the specific initiatives taken by banks in India are - IndusInd Bank introducing solar powered ATMs, SBI adopting green banking policy and offering green home loans, Union Bank of India's energy efficiency measures, IDBI Bank's membership in National Action Plan on Climate Change, ICICI Bank's Corporate Environmental Stewardship initiatives and also Clean Technology Initiatives, YES Bank's community development initiatives, ABN Amro Bank's (now Royal Bank of Scotland) launching of Indian Sustainable Development Fund as also the Role played by RBI in its CSR initiatives. Green Banking goes a long way it serving its objectives. The incorporation of social and environmental strategies into the development goals of the banks helps them in arriving effective environmental management system. According to Krebsbach (2005), the banks, which adopted socially and environmentally responsible lending and investing strategies were altering their processes of bond underwriting, investment banking and corporate lending. These banks were enjoying a competitive advantage over others as society is aware about the environmental issues. But the author had suggested that banks should adopt the green lending principles in such a way that a customer base will not be affected. The author said "Credibility comes from having high standards, but if you push the standards too high too quickly, it may stop some banks from lending and have a serious impact on companies that needs capital".

Environmental management in the banking sector is like risk management because it reduces the credit risk, improves the asset quality and increases the enterprise value. Biswas (2011) revealed some strategies for the adoption of environmental management in the banking sector:-

Banks should do Environmental Impact Assessment (EIA) in which they design the environmental system to evaluate the risk involved before investing in different projects;

They should adopt the Annual Reporting System (ARS) in which they prepare an annual report on environmental risk guidelines for every project they invest or finance;

Theyshould adopt environmentally sustainable technologies which minimizes risk, saves cost and enhance the bank's reputation;

ATM services: John Shepherd-Barron devised what is hailed as the world's first automatic teller machine. First ATM in the world was installed by Barclays bank in Londaon in 1967.First ATM in India was installed by HSBC in Kolkata in 1987 First PSB to install ATM in india is Indian bank.

Debit card: The first debit cards were introduced in the early 1980's to enable consumers to obtain cash from ATMs by debiting their bank account.Corporation Bank is the first Indian Bank to introduce debit card.

VISA & Master Card:

As credit card processing became more complicated, outside service companies began to sell processing services to Visa and MasterCard association members.This reduced the cost of programs for banks to issue cards, pay merchants and settle accounts with cardholders, thus allowing greater expansion of the payments industry.

Credit Card:

"The general-purpose credit card was born in 1966, when the Bank of America established the BankAmerica Service Corporation that franchised the Bank Americard brand (later to be known as Visa) to banks nationwide," Sienkiewicz writes.As the bank card industry grew, banks interested in issuing cards became members of either the Visa association or Master Card association. Their members shared card program costs, making the bank card program available to even small financial institutions. Later, changes to the association bylaws allowed banks to belong to both associations and issue both types of cards to their customers.

Vishwa Yatra Card: State Bank Vishwa Yatra Foreign Travel Card' is a prepaid Foreign Currency Card which travelers going abroad are guaranteed to find useful. It is a Chip based Card which stores encrypted and confidential information.State Bank Vishwa Yatra Foreign Travel Card is available in Eight Foreign Currencies viz.US Dollars (USD), Pound Sterling (GBP), Euro (EUR), Japanese Yen (YEN),Canadian Dollar (CAD), Australian Dollar (AUD), Saudi Riyal (SAR) and Singapore Dollar(SGD).

Gift Card: Gift Card is also a prepaid Indian rupee VISA CARD –an excellent substitute of Gift Vouchers.

Green Channel Counter: The Bank had launched 'Green Channel Counter'(GCC) facility on State Bank Day (01.07.2010), at 57 select branches of the Bank spread across the country. This was an innovative step taken by the Bank towards changing the traditional way of paper based banking in a limited way, to card based 'Green Banking' focusing on reduction in paper usage as well as saving transaction time. This is a pioneering concept which would save both paper and time resources.

Online banking services: Online banking services are helped the customers to reduce the carbon foot prints indirectly and make the convenience to the customer almost most of the important baking services. Some of these services do not require any manual intervention.

- Fund Transfer to Self Accounts
- Third Party Fund Transfer
- Inter Bank Payee Fund Transfer
- PPF transfer
- Setting up Standing Instruction
- E-Tax Payment
- E-ticketing
- Bill Payments
- Visa Money Transfer
- Demat Enquiry
- Online Application for IPO.

Mobile Banking Services: Mobile banking also known as M-Banking. M-banking is a term used for performing balance checks, account transactions, payments, credit applications and other banking transactions through a mobile device such as a mobile phone or Personal Digital Assistant (PDA). The earliest mobile banking services were offered over SMS, a service known as SMS banking. With the introduction of the first primitive smart phones with WAP support enabling the use of the mobile web in 1999, the first European banks started to offer mobile banking on this platform to their customers.

XI. GREEN BANKING INITIATIVES BY VARIOUS INDIAN BANKS

SBI :(SBI) has become the first bank in the country to venture into generation of green power by installing windmills for captive use. As part of its green banking initiative, has installed 10 windmills with an aggregate capacity of 15 MW in the states of Tamil Nadu, Maharashtra and Gujarat. . It has planned to install an additional 20 MW capacity of windmills in Gujarat soon and touch 100 MW power generation through windmills within five years, windmills are set up with a definite objective of reducing the dependence on the polluting thermal power and not on purely economic or business considerations.SBI had launched Green Channel Counter (GCC) facility at their branches in 2010 to change the traditional way of paper based banking (SBI, 2014).The bank had also collaborated with Suzlon Energy Ltd for the generation of wind power for selected branches by setting of windmills in Gujrat, Tamil Nadu and Maharastra (Business Standard, 2014).It has become a signatory to the Carbon Disclosure Project in which they undertake various environmentally and socially sustainable initiatives through its branches spread across the length and breadth of the country (WWF-INDIA, 2014).Export Import Bank of India (EXIM) and SBI entered into an agreement to jointly provide long term loans up to 14 years to Spain based company Astonfield Renewable Resources and Grupo T-Solar Global SA for building solar plant in India (Yadav & Pathak, 2013).

Punjab National Bank (PNB) – According to Corporate Social Responsibility Report 2010-11 (PNB, 2011),they had taken various steps for reducing emission and energy consumption.PNB is conducting Electricity Audit of offices as an energy conversation initiative and maintained a separate audit sheet for assessing the impact of green initiatives taken by them. The bank had organized more than 290 Tree Plantation Drives. It started emphasizing on green building practices such as energy efficient lights, immediate repair of water leakage, printing on both sides of paper, mater censors for lights, fans, etc.The organization had signed a 'Green Pledge' with Ministry of New and Renewable energy under which they had set up the butterfly park at the compound of Guruvayur temple which houses 18 types of medicinal plants. They had formulated guidelines to ensure that all the necessary approvals and permissions, including from Pollution Control Board has been obtained before disbursement of term loans and for the project loans, compliance with environment and social safeguards including rehabilitation and resettlement of project affected people is to be ensured as pre-disbursement condition. The bank is also considering stepping of sustainable development with particular reference to the Equators Principles on project finance. The organization had sanctioned nine wind energy projects with an aggregation limit of 185.81 crore and they were also awarded with a second prize for 'Best Wind Energy Power Financer' by wind power India 2011.

Bank of Baroda – According to the annual report of BOB (2013), they had taken various green banking initiatives such as: -While financing a commercial project, BOB is giving preference to environmentally friendly green projects such as windmills, biomass and solar power projects which help in earning the carbon credits. The organization had made considerable changes in their lending policy, i.e. it is compulsory for industries to obtain 'No Objection Certificate' from the Pollution Control Board and also they are not extending any finance to environmental hazardous industries which are using ozone depletion substances. The bank had taken several technological initiatives such as compliance with e-business guidelines, use of internet banking, mobile banking to promote paperless banking and also increasing the installation of ATM's in most of uncovered areas to reduce the petrol or diesel consumption in travelling and helps in maintaining a clean environment. As a part of green initiative, they had made changes to desktop virtualization; backup consolidation and server virtualization improve data center operational efficiency. The bank is also promoting measures for pollution control and environmental conservation.

Canara Bank – According to Canara Bank (2013), the bank had taken many green initiatives such as: - As a part of green banking initiative, the bank had adopted environmental friendly measures such as mobile banking, internet banking, tele-banking, solar powered biometric operations etc.Canara bank had set up e-lounges for high-tech banking facilities like internet banking, pass book printing kiosk, ATM, online trading, tele-banking and cash/cheque acceptor's The bank had implemented e-governance for HRM function and several other administration areas to reduce the paperwork. In terms of Lending policy, they are giving due preference and weightage to projects which can earn carbon credits like solar energy projects, windmills, etc.The bank is also not extending any finance to the units which are producing ozone depletion substances such as cholorofluoro carbon, carbon tetrachloride, aerosol products, solvents etc.While appraising any project, the organization insists the manufacturing units which are emitting toxic pollutants, to install water treatment projects to process such pollutants and they also ensure that the borrower to obtain No Objection Certificate (NOC) from central or state pollution control board.

ICICI Bank Ltd – ICICI bank had adopted 'Go Green' initiative, which involves activities such as Green products/offerings, Green engagement and green communication with customers as per ICICI Bank (2014):- The bank is offering green products and services like (i) Instabanking: - It is a service which gives convenience to the customers to do banking anywhere and anytime through internet banking, mobile banking, IVR banking, etc. This reduces the carbon footprint of the customers as they do not require the physical statement or travel to the bank branches.They are offering 50% waiver on processing fee of auto loans on the car models which uses alternate sources of energy like the Civic Hybrid of Honda, Tata Indica CNG, Reva electric cars,Mahindra Logan CNG versions, Maruti's LPG version of Maruti 800, Omni and Versa and Hyundai's Santro Eco.The bank had reduced the processing fee for the customers who are purchasing homes in LEED certified buildings.

During Diwali 2013, the organization had conducted an environmental awareness program for employees and customers in which money plant was presented to all the people present there as a token of collective responsibility to protect the environment. It has also become partners with the Green theme CNBC – overdrive auto awards. The bank is celebrating World Environment Day every year on June 5. They perform various activities on that day like green pledge through signature campaigns,plantation and distribution of saplings etc. They are also celebrating Earth hour every year in March in which they switch off the lights of their premises, branches and ATM's between 8:30 pm to 9:30pm.

The bank always insists their customers for online bill payment, online funds transfer and subscription to e-statements which promote 'paperless' and 'commute free' modes of banking transactions.The organization is looking forward for partnerships with national and international green organizations and NGO's. They are partners with Green Governance awards set up by BHNS to appreciate the participant's organization effort beyond the statutory compliance for protection of the environment.

HDFC Bank Ltd – HDFC bank is taking up various measures in reducing their carbon footprints in the area of waste management, paper use and energy efficiencies as per HDFC Bank (2013):- The bank is encouraging their employees to prevent any wasteful use of natural resources and emission of Greenhouse gasses. They are reducing the use of paper through issuing e-transaction advices to their corporate customers, communicating through electronic media with their high net worth customers and encouraging e-statements to their retail customers. The bank is also promoting energy conservation by replacing conventional lighting with CFL, switching off all the lights after 11 pm at all the branches and establishing green data centers with state of the art technologies. The organization is exploring renewable energy by setting up of 20 solar ATMs with a pilot ATM set up in Bihar, and by replacing batteries in ATMs with Lithium-ion batteries. They are also managing their waste by tying up with vendors for recycling of paper and plastic. The bank is procuring green products which are compliant with the norms of the Central Pollution Control Board and which are rated by Energy Star.

Axis Bank Ltd – AXIS bank implementing several initiatives in green banking such as per Axis Bank (2013):-In august 2011, the bank had initiated the process of collecting all the dry waste generated from the corporate office and thirty four branch offices in Mumbai, and recycle it to notepads, notebooks and envelopes. Till date, more than 1, 00,000 kgs of paper has been recycled and converted to 12,000 notebooks, notepads and envelopes which are used at corporate office and branches of the bank; The corporate office of the bank, located in Mumbai, is designed and constructed as a Platinum LEED certified 'Green Building'; Car pooling has been initiated by a bank to reduce carbon footprint; They are also encouraging their customers to use e-statements and other electronic communications to reduce paper consumption; Annual reports are being sent through emails;the organization had initiated Independent ATM Deployment (IAD) model in which ten solar based ATM has been set up in Coimbatore circle.

Kotak Mahindra Bank – Through the 'Think Green' initiative, the bank had taken several initiatives such as to reduce the paper consumption, the bank is encouraging their customers to sign for e-statements and also they have become partners with 'Grow-Trees.com' to plant one sapling for every e-statement on behalf of its customers. 16,623 saplings were planted FY 2012-13.The organization had established the 'Social, Environmental Management System Plan' (SEMSP) to evaluate the environmental and social risk of borrowers which is based on an IFC sustainable framework and performance standards. As per the guidelines of Ministry of Corporate Affairs (MCA), the bank had communicated to their shareholders to adopt electronic copies of annual report instead of physical copies.

In 2009, they had consolidated their data centers into a single facility to improve power usage efficiencies. The rain water harvesting tank has been installed in the premises and also used oil generated from a diesel generator is disposed off through vendors approved by Pollution Control Board.Bihari (2011) had also highlighted the green banking initiatives being taken by the Indus IND Bank, SBI,Union Bank of India, IDBI Bank, ICICI Bank, YES Bank and ABN Amro Bank.. According to the author, Mumbai, Delhi and Chennai are among the ten most polluted cities in the world and the major industries which cause pollution are fertilizers, paper and pulp, pesticides/insecticides, chemicals pharmaceuticals, metallurgical and textiles. SIDBI had made significant changes in their lending principles and implemented a precondition for sanctioning of credit. They had made it compulsory for a company to obtain 'No Objection Certificate' (NOC) from the state pollution control board before establishing the enterprise.

IndusInd: IndusInd Bank, India has initiated its Green Office Project under which it has installed solar powered ATMs in different cities targeting energy saving as well as reducing CO2 emissions.

YES Bank: Yes Bank India have projects portfolio in the areas of alternative energy and clean Technologies

HSBC Group: HSBC has separate targets for data centres, paper consumption and business air travel. The purposes of the targets are to drive efficiency, reduce its operational impact on the environment and generate cost savings.

IDBI: IDBI Bank is providing various services in the field of Clean Development Mechanisms (CDM) to its client.

Table 1: Publication dates of green banking adopted in Indian banks

Green Banking implementation year	Names of the banks operating in India
1996	Union Bank Of India
2003	Citi Group INC, HSBC, ING Vyasa, RBS, Royal bank Of Canada, Syndicate Bank, Statndard Charted
2005	Yes bank, Corporation Bank
2006	Bank Of America, JP Morgan
2007	ICICI, OBC, SBI
2008	Bank Of Baroda, Karnataka Bank, Industrial Bank, Dena Bank
2009	HDFC, Indian Overseas, Indusland Bank, PNB, ABN Amro , Karur Vyasa , Andhra bank
2010	Axis bank, Kotak Mahndra, South Indian Bank
2011	Canara Bank, IDBI, EXIM
2013	IDFC

XII. CHALLENGES

Key challenges faced by banks while implementing green banking strategies. Following are the challenges:

a) Confronting Challenges to Going Green: Green banks support wonderful causes; they do face a lot of challenges as for-profit entities. Just like those socially conscious and environmental mutual funds, they are expected to encounter more obstacles than typical run-of-the-mill bank.

b) Diversification matters: Green banks will be screening their customers and naturally, they'll be limiting and restricting their business to those entities that qualify. With a smaller pool of customers, they'll automatically have a smaller profit base to support them. If they focus their loans on certain industries, they open themselves up to being much more vulnerable to economic shifts.

c) These banks are still startups: Apparently, it takes 3 to 4 years for a typical bank to start making money. Many green banks in business today are very new and are still in startup mode. It doesn't help that these banks are trying to get their footing during a recession.

d) Banks are "specialized":Again, while the main goal of a green bank is to do good by supporting those who are taking care of the environment, the question here is — just how much money is there in these businesses and in the eco-friendly industry? Saving the environment does not necessarily equate to "making a profit". Hopefully though, this premise is proven wrong in this case and that green banks prove that they can survive, even as they face restrictive requirements for doing business.

(iv) Operating expenses and costs are higher: Green banks require specialized talent, skills and expertise as well, due to the kind of customers they are servicing. Employees, such as loan officers, need to have additional background and experience in dealing with green businesses and consumers. Plus, giving breaks to such clients via discounted loan rates can eat at their profit margins.

(v) Reputation Risk: In all likelihood, due to growing awareness about environment safety, banking institutions are more prone to loose their reputations if they are involved in big projects, which are viewed as socially and environmentally damaging. There are also few cases where environmental management system has resulted in cost savings, increase in bond value etc.(Heim, G et al, 2005). In few cases the environmental management system resulted in lower risk, greater environmental stewardship and increase in operating profit. Reputation risks involved in the financing of ecologically and ethically questionable projects.

(vi) Proper legislation is not yet framed: Government must design proper legislation of environmental rules for banks and ensure enforcement. The problems in India are the legislation is not yet framed and in few cases, things are not strictly enforced, but things can change overnight resulting in major compliance problems for the companies concerned and increased risk for the banks that have lent to them. There should be continuous dialogue relating to environmental matters with relevant audiences, including stakeholders, employees, customers, governments and the public.

(vii) Lack of environmental audits: Lack of environmental audits are required to determine the environmental status of a facility, property, and operation and to identify regulatory compliance status, past present problems and potential environmental risks and liabilities associated with the project. These should be done by an independent body or by any environment investigation team.

(viii) Less attention on environmental risk management: Less attention is given for the environmental risk management after the post transaction period.

(ix) Non automation of business process: Mostly banks are not adopting automation process Banks should conduct energy audits in all their offices for effective energy management using compact fluorescent lighting (CFL) can help banks save on energy consumption considerably.

x) Lack of clear policies: Clear policies are required to altering the present management systems to incorporate sustainability issues.

xi) Unavailability of skilled employees: Skilled employees are required to implement the strategies properly.

XIII. SUGGESTIONS

Following are some of the suggestions that can be adopted by the banks for proper implementation of green banking in India:

a) Make customers more and more aware about green banking through their website .

b) Promoting different forms of electronic banking .

c) Creating customer's awareness through the media.

d) Carbon footprint reduction by saving energy and paper.

e) Providing environment friendly rewards to customers.

f) By financing more and more environment-friendly projects

g) Social Responsibility services done by banks.

h) Clear policies are required to altering the present management systems to incorporate sustainability issues.

i) Training and development of relevant skills within bank employees so that they can use

XIV. CONCLUSION

Green Banking has been boosting to improve the environment and promoting economic growth. Until a few years ago, most traditional banks did not practice green banking or actively seek investment opportunities in environmentally-friendly sectors or businesses. Indian banks are far behind their counterparts from developed countries. If Indian banks desire to enter global markets, it is important that they recognize their environmental and social responsibilities. Only recently have these strategies become more prevalent, not only among smaller alternative and cooperative banks, but also among diversified financial service providers, asset management firms and insurance companies.

Further, those industries which have already become green and those, which are making serious attempts to grow green, should be accorded priority to lending by the banks. This concept of "Green Banking" will be mutually beneficial to the banks, industries and the economy. Not only "Green Banking" will ensure the greening of the industries but it will also facilitate in improving the asset quality of the banks in future. There are lot of opportunities and challenges for Indian banks in adopting ‘Green Banking’ as profitable business. Green banking if implemented sincerely will act as an effective ex ante deterrent for the polluting industries that give a pass by to the other institutional regulatory mechanisms. Therefore, for sustainable banking, Indian banks should adopt green banking as a business model without any further delay.

REFERENCES

[1]. Axis Bank. (2013). Annual Report 2012-13. Mumbai: Axis Bank.
[2]. Alice Mani, “Green Banking through Green Lending”,www.ibmtedu.org/GVCG/Papers/IC- 140.pdf, 2011.
[3]. Alpesh Shah et. al. “Indian Banking 2020 – Making the Decade’s Promise Come true”, Report of BCG, FICCI and Indian Banks’ Association, Sept. 2010.
[4]. Bank of Baroda. (2013). 2012-13 Annual Report. Vadodara: Bank of Baroda.
[5]. BankTrack. (2014, 03 06). Home: Bank Track. Retrieved from Bank Track: http://www.banktrack.org/show/pages/about_banktrack.
[6]. Bihari, S. C. (2011). Green banking -towards socially responsible banking in India. IJBIT, 82-87.
[7]. Biswas, N. (2011). Sustainable Green Banking Approach: The Need of the Hour. Business Spectrum, 32-38.
[8]. BSE-INDIA. (2014, 03 06). Downloads:. Retrieved from BSE:
[9]. http://www.bseindia.com/downloads/about/abindices/file/BSE-GREENEX%20Factsheet.pdf
[10]. Business Standard. (2014, 03 06). Article: Business Standard (April 19, 2010). Retrieved from Business Standard:http://www.business-standard.com/article/finance/sbi-to-set-up-windmills-for-captive-use-110041900118_1.html.
[11]. Canara Bank 2013. (2013). 2012-13 Annual Report. Bangalore: Canara Bank.
[12]. Caruntu, G.A. (2008) „Methodology to determine the enterprise‟s profitability‟, Annals of the University of Petrosani, Economics, Vol. 8, No. 1, pp.49–58.
[13]. Centre for Environment Education. (2014, 03 06). Home: Centre for Environment Education. Retrieved from CEE - Centre for Environment Education: http://www.ceeindia.org/cee/index.html.
[14]. Cordeiro, J.J. and Sarkis, J. (1997) „Environmental proactivism and firm performance: evidence from security analyst earnings forecasts, Business Strategy and Environment, Vol. 6, pp.104–114.
[15]. Dash R.N.; “Sustainable ‘Green’ Banking: The Story of Triodos Bank” CAB CALLING October-December, 2008 p. 26-29.
[16]. Dharwal, M., & Agarwal, A. (2013). Green Banking: An Innovative Initiative for Sustainable Development.
[17]. Equator Principles Association. (2014, 03 04). Members and Reporting, Equators Principles. Retrieved from Equators Principles: http://www.equator-principles.com/index.php/members-reporting.
[18]. Financial Times. (2014, 03 4). About Us: ft.com. Retrieved from Financial Times:
[19]. http://aboutus.ft.com/2012/11/16/ft-and-ifc-launch-2013-sustainable-finance-awards/#axzz2uv5IzDup.
[20]. Kotak Mahindra Bank. (2013). Annual Report 2012-13. Mumbai: Kotak Mahindra Bank.
[21]. Punjab National Bank. (2011). 2010-11 Corporate Social Responsibility Report. New Delhi: Punjab National Bank. Retrieved from PNB-India.
[22]. Sahoo Pravakar and Bibhu Prasad Nayak; “Green Banking in India” Discussion Paper Series No. 125/2008 Institute of Economic Growth University of Delhi, Delhi-1100071.
[23]. State Bank of India. (2014, 03 07). Webfiles: State Bank of India, Retrieved from SBI:http://www.sbi.co.in/ .
[24]. Ritwik Mukherjee, ‘SBI launches green policy for paperless banking’, Financial Chronicle, August 27, 2010.
[25]. VIKAS NATH, NITIN NAYAK & ANKIT GOEL, “Green Banking Practices – A Review”, International Journal of Research in Business Management (IMPACT: IJRBM) ISSN (E): 2321-886X; ISSN (P): 2347-4572

GREEN COMPUTING

Vandana Sehgal[1], Sonia Choudhary[2]

[1,2]*Department of Computer Science &Engineering, Ganga Institute of Technology and Management, Kablana, Jhajjar, Haryana, INDIA*

Abstract: Thrust of computing was initially on faster analysis and speedier calculations and solving of mare complex problems but in the recent past another focus has got immense importance and that is achievement of energy efficiency, minimization consumption of e-equipments. It has also given utmost attention to minimization of e-waste and use of non-toxic materials in preparation of e-equipments. World leaders have also taken move towards this by following some principles. Now it is the time for the end users community to follow some rules of thumb to achieve partly benefit of —Green Computing. In India, the implement ability of principle of — Green Computing is facing a dilemma due to many socio-economic matters and those are linked to be soughed out to pull India in the mainstream movement of —Green Computing.

I. INTRODUCTION

Green Computing is a recent trend towards designing, building, and operating computer systems to be energy efficient. While programs such as Energy Star have been around since the early 1990s, recent concerns regarding global climate change and the energy crisis have led to renewed interest in Green Computing. Data centers are assign affiant consumers of energy both to power the computers as well as to provide the necessary cooling. It is a new approach to reduce energy utilization in data centers. In particular, our approach relies on consolidating services dynamically onto a subset of the available servers and temporarily shutting down servers in order to conserve energy. The initial work on a probabilistic service dispatch algorithm that aims at minimizing the number of running servers such that they suffice for meeting the quality of service required by service-level agreements. Given the estimated energy consumption and projected growth in data centers, the proposed effort has the potential to positively impact energy consumption.

Green computing is the practice of using computing resources efficiently. The goals are to reduce the use of hazardous Green computing is a very hot topic these days, not only because of rising energy costs and potential savings, but also due to the impact on the environment. Energy to manufacture, store, operate, and cool computing systems has grown significantly in the recent years, primarily due to the volume of systems and computing that companies now heavily rely upon. Computing power consumption of companies has reached a critical point. For example, an E-commerce business with 100,000 servers can easily spend up to $20 million a year on server power. Add another $10 million for a/c cooling and it tops $30 million a year in power alone. Clearly there is a huge potential for savings in their infrastructure. Despite the huge surge in computing power demands, there are many existing technologies and methods by which significant savings can be made. This series is dedicated to the ways a typical organization can reduce their energy footprint while maintaining required levels of computing performance.

1.3 Objectives

materials, maximize energy efficiency during the product's lifetime, and promote recyclability or biodegradability of defunct products and factory waste. Such practices include the implementation of energy-efficient central processing units (CPUs), servers and peripherals as well as reduced resource consumption and proper disposal of electronic waste (e-waste).

In 1992, the U.S. Environmental Protection Agency launched Energy Star, a voluntarylabeling program which is designed to promote and recognize energy-efficiency in monitors, climate control equipment, and other technologies. This resulted in the wide spread adoption of sleep mode among consumer electronics. The term "green computing" was probably coined shortly after the Energy Star program began; there are several USENET posts dating back to 1992 which use the term in this manner.

Figure 1: Green Computing

1.2 Why Go Green?

1.3.1 Climate Change:

First and foremost, conclusive research shows that CO2 and other emissions are causing global climate and environmental damage. Preserving the planet is a valid goal because it aims to preserve life. Planets like ours, that supports life, are very rare. None of the planets in our solar system, or in nearby star systems have m-class planets as we know them.

1.3.2 Savings:

Green computing can lead to serious cost savings over time. Reductions in energy costs from servers, cooling, and lighting are generating serious savings for many corporations.

1.3.3 Reliability of Power:

As energy demands in the world go up, energy supply is declining or flat. Energy efficient systems helps ensure healthy power systems. Also, more companies are generating more of their own electricity, which further motivates them to keep power consumption low.

Computing power consumption has reached a critical point:

Data centers have run out of usable power and cooling due to high densities.

II. HISTORY OF GREEN COMPUTING

In 1992, the U.S. Environmental Protection Agency launched Energy Star, a voluntary labeling program which is designed to promote and recognize energy-efficiency in monitors, climate control equipment, and other technologies. This resulted in the widespread adoption of sleep mode among consumer electronics. The term "green computing" was probably coined shortly after the Energy Star program began; there are several USENET posts dating back to1992 which use the term in this manner. Concurrently, the Swedish organization TCO Development launched the Certification program to promote low magnetic and electrical emissions from CRT based computerdisplays; this program was later expanded to include criteria on energy consumption, ergonomics, and the use of hazardous materials in construction. When it comes to PC disposal, it is necessary to know everything there is to know in order to be involved in green computing. Basically, the whole green aspect came about quite a few years back when the news that the environment was not a renewable resource really hit home and people started realizing that they had to do their part to protect the environment. Basically, the efficient use of computers and computing is what green computing is all about. The triple bottom line is what is important when it comes to anything green and the same goes for green computing.

This considers social responsibility, economic viability and the impact on the environment. Many businesses simply focus on a bottom line, rather than a green Triple bottom line, of economic viability when it comes to computers. The idea is to make the whole process surrounding computers friendlier to the environment, economy, and society. This means manufacturers create computers in a way that reflects the triple bottom line positively. Once computers are sold businesses or people use them in a green way by reducing power usage and disposing of them properly or recycling them. The idea is to make computers from beginning trend a green product.

2.2 What is Green Computing?

Green computing is the study and practice of using computing resources efficiently. The primary objective of such a program is to account an expanded spectrum of values and criteria for ensuring organizational (and societal) success. The goals are similar to green chemistry; reduce the use of hazardous materials, maximize energy efficiency during the product‘s lifetime, and promote recyclability or biodegradability of defunct products and factory waste.

Figure 2: Green Earth

Modern IT systems rely upon a complicated mix of people, networks and hardware; as such, a green computing initiative must be systemic in nature, and address increasingly sophisticated problems. Elements of such a solution may comprise items such as end user satisfaction, management restructuring, regulatory compliance, disposal of electronic waste, telecommuting.

2.2.1 Origin

In 1992, the U.S. Environmental Protection Agency launched Energy Star, a voluntary labeling program that is designed to promote and recognize energy-efficiency in monitors, climate control equipment, and other technologies. This resulted in the widespread adoption of sleep mode among consumer electronics. Concurrently, the Swedish organization TCO Development launched the TCO Certification program to promote low magnetic and electrical emissions from CRT-based computer displays; this program was later expanded to include criteria on energy consumption, ergonomics, and the use of hazardous materials in construction.

2.2.2. At Present

Currently the ICT industry is responsible for 3% of the world‘s energy consumption. With the rate of consumption increasing by 20% a year, 2030 will be the year when the world‘s energy Consumption will double because of the ICT industry. Organizations use the Green Computing Lifecycle when designing and implementing green computing technologies. The stages in the Lifecycle include Strategy, Design, Implementation, Operations and Continual Improvements. Many governmental agencies have continued to implement standards and regulations that encourage green computing. The Energy Star program was revised in October 2006 to include stricter efficiency requirements for computer equipment, along with a tiered ranking system for approved products.

The 5 core green computing technologies advocated by GCI are Green Data Centre, Virtualization, Cloud Computing, Power Optimization and Grid Computing.

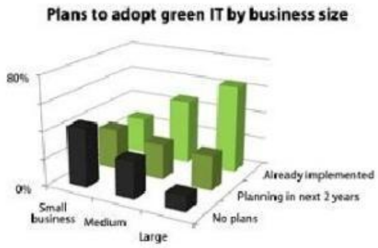


Figure 3: Present Scenario

There are currently many nations that have established state-wide recycling programs forobsolete computers and consumer electronics equipment The statutes either impose a fee foreach unit sold at retail (Advance Recovery Fee model), or require the manufacturers to reclaimthe equipment at disposal (Producer Responsibility model).

2.2.3. Roads to Green Computing

Figure 4: Reduce, Reuse & Recycle[12][2]

Green use:

— reducing the energy consumption of computers and other information systems as well as using them in an environmentally sound manner

Green disposal:

— refurbishing and reusing old computers and properly recycling unwanted computers and other electronic equipment

Green design:

— designing energy-efficient and environmentally sound components, computers, servers, cooling equipment, and data centers.

Green manufacturing:

— manufacturing electronic components, computers, another associated subsystems with minimal impact on the environment

2.3. Regulation and Industry Initiative

2.3.1. From the Government:

Many governmental agencies have continued to implement standards and regulations that encourage green computing. The Energy Star program was revised in October 2006 to include stricter efficiency requirements for computer equipment The European Union's directives 2002/95/EC (RoHS),on the reduction of hazardous substances, and 2002/96/EC (WEEE) on waste electrical and electronic equipment required the substitution of heavy metals and flame retardants like PBBs and PBDEs in all electronic equipment put on the market starting on July 1,2006. The directives placed responsibility on manufacturers for the gathering and recycling of old equipment (the Producer Responsibility model).

2.3.2 From the Industry:

2.3.2.1 Climate Savers Computing Initiative:

CSCI is an effort to reduce the electric power consumption of PCs in active and inactive states. The CSCI provides act along of green products from its member organizations, andinformation for reducing PC power consumption. It was started on 2007-06-12.

2.3.2.2 Green Computing Impact Organization Inc:

GCIO is a non-profit organization dedicated to assisting the end-users of computing products in being environmentally responsible. This mission is accomplished through educational events, cooperative programs and subsidized auditing services. The heart of the group is based on the GCIO Cooperative, a community of environmentally concerned IT leaders who pool their time, resources, and buying power to educate, broaden the use, and improve the efficiency of green computing products and services.

2.3.2.3 Green Electronics Council:

The Green Electronics Council offers the Electronic Products Environmental Assessment Tool (EPEAT) to assist in the purchase of "green" computing systems. The Council evaluates computing equipment on 28 criteria that measure a product‘s efficiency and sustainability attributes. On 2007-01-24, President George W. Bush issued Executive Order 13423, which requires all United States Federal agencies to use EPEAT when purchasing computer systems.

2.3.2.4 The Green Grid:

It is a global consortium dedicated to advancing energy efficiency in datacenters and business computing ecosystems. It was founded in February 2007 by several key companies in the industry

– AMD, APC, Dell, HP, IBM, Intel, Microsoft, rack able Systems, Spray Cool, Sun Microsystems and VMware. The Green Grid has since grown to hundreds of members, including end users and government organizations, all focused on improving data center efficiency.

2.4. Demons behind Green Computing

2.4.1 Power Supply:

Desktop computer power supplies (PSUs) are generally 70– 75% efficient, dissipating the remaining energy as heat. An industry initiative called 80 PLUS certifies PSUs that are at least 80% efficient; typically these models are drop-in replacements for older, less efficient PSUs of the same form factor. As of July 20, 2007, all new Energy Star 4.0-certified desktop PSUs must be at least 80% efficient.

2.4.2 Storage:

Smaller form factor (e.g. 2.5 inches) hard disk drive soften consume less power than physically larger drives. Unlike hard disk drives, solid store data in flash memory or DRAM. With no moving parts, power consumption may be reduced somewhat for low capacity flash based devices. Even at modest sizes, DRAM based SSDs may use more power than hard disks, (e.g., 4GBi-RAM uses more power and space than laptop drives). Flash based drives are generally slower for writing than hard disks.

2.4.3 Video card:

1. A fast GPU may be the largest power consumer in a computer. Energy efficient display options include: No video cards used in a shared terminal, shared thin client, or desktop sharing software if display required.
2. Use motherboard video output - typically low 3D performance and low power.
3. Reuse an older video card that uses little power; many do not require heat sinks or fans.
4. Select a GPU based on average wattage or performance per watt.

2.4.4. Materials:

Computer systems that have outlived their particular function can be repurposed, or donated to various charities and non-profit organizations. However, many charities have recently imposed minimum system requirements for donated equipment. Additionally, parts from outdated systems may be salvaged and recycled through certain retail out lets and municipal or private recycling centers. Recycling computing equipment can keep harmful materials such as lead, mercury, and hexavalent chromiumout of landfills, but often computers gathered through recycling drives are shipped to countries where environmental standards are less strict than in North America and Europe. The Silicon Valley Toxics Coalition estimates that 80% of the post-consumer e-waste collected for recycling is shipped abroad to countries such as China, India, and Pakistan. Computing supplies, such as printer cartridges, paper, and batteries may be recycled as well.

2.4.5. Display:

LCD monitors typically use a cold-cathode fluorescent bulb to provide light for the display. Some newer displays use an array of light-emitting diodes (LEDs) in place of the fluorescent bulb, which reduces the amount of electricity used by the display.

2.4.6. Chilling of data:

To keep servers at the right temperature, companies mainly rely on air conditioning. The more powerful the machine, the more cool air needed to keep it from overheating. By 2005, the energy required to power and cool servers accounted for about1.2 % of total U.S electricity conception. By 2010, half of the Forbes Global 2000companies will spend more on energy than on hardwaresuch as servers.

2.5. Recent implementations of Green Computing

2.5.1. Blackle:

Blackle is a search-engine site powered by Google Search. Blackle came into being based on the concept that when a computer screen is white, presenting an empty word or the Google home, and your computer consumes 74W. When the screen is black it consumes only 59W. Based on this theory if everyone switched from Google to Blackle, mother earth would save750MW each year. This was a really good implementation of Green Computing. The principle behind Blackle is based on the fact that the display of different colors consumes different amounts of energy on computer monitors. 6.2 Fit-PC: a tiny PC that draws only 5w: Fit-PC is the size of a paperback and absolutely silent, yet fit enough to run Windows XP or Linux. Fit-PC is designed to fit where a standard PC is too bulky, noisy and power hungry. If you ever wished for a P

C to be compact, quiet and green â€œ then Fit- PC is the perfect fit for you. Fit-PC draws only5 Watts, consuming in a day less power than a traditional PC consumes in 1 hour. You can leave Fit-PC to work 24/7 without making a dent in your electric bill.

2.5.2. Zonbu Computer:

The Zonbu is a new, very energy efficient PC. The Zonbu consumes just one third of the power of a typical light bulb. The device runs the Linux operating system using a 1.2 gigahertz processor and 512 Meg of RAM. It also contains no moving parts, and does even contain a fan. You can get one for as little as US$99, but it does require you to sign up for a two- year subscription.

2.5.3 Sunray thin client:

Sun Microsystems is reporting increased customer interest in its Sun Ray, a thin desktop client, as electricity prices climb, according to Subodh Bapat, vice president and chief engineer in the Eco Responsibility office at Sun. Thin clients like the Sun Ray consume far less electricity than conventional desktops, he said. A Sun Ray on a desktop consumes 4 to 8 watts of power, because most of the heavy computation is performed by a server. Sun says Sunrays are particularly well suited for cost-sensitive environments such as call centers, education, healthcare, service providers, and finance. PCs have more powerful processors as well as hard drives, something thin clients don't have. Thus, traditional PCs invariably consume a substantially larger amount of power. In the United States, desktops need to consume 50 watts or less in idle mode to qualify for new stringent Energy Star certification.

2.5.4 The Asus Eee PC and other ultra portables:

The "ultra-portable" class of personal computers is characterized by a small size, fairly low power CPU, compact screen, low cost and innovations such as using flash memory for storage rather than hard drives with spinning platters. These factors combine to enable them to run more efficiently and use less power than a standard form factor laptop. The Asus Eee PC is one example of an ultraportable. It is the size of a paperback, weighs less than a kilogram, has built-in Wi-Fi and uses flash memory instead of a hard drive. It runs Linux too.

2.6 Advantages of Green Computing:

- Reduced energy usage from green computing techniques translates into lower carbon dioxide emissions, stemming from a reduction in the fossil fuel used in power plants and transportation.
- Conserving resources means less energy is required to produce, use, and dispose of products.
- Saving energy and resources saves money.
- Green computing even includes changing government policy to encourage recycling and lowering energy use by individuals and businesses.
- Reduce the risk existing in the laptops such as chemical known to cause cancer, nerve damage and immune reactions in humans.
- System Wide Green Computing and Individual Green Computing is the best possible way to practice Green Computing. Companies implementing System Wide Green Computing and employees and individuals practicing individual green computing techniques help ina long way in creating an impact to save the planet.

2.7 Facts about Green Computing

- Computer technology use accounts for 2% of anthropogenic CO2
- Roughly equivalent to aviation industry
- IT energy usage will double next 4 years
- A typical desktop PC with a 17-inch LCD monitor requires about 145 watts, 110 watts for the computer and 35 watts for the monitor.
- For every 12 consumers who keep power settings enabled for their on their monitors and PCs, CO2 emissions equivalent to removing one average automobile from the road will be avoided.

III. ANALYSIS AND APPROACHES

3.1 Why GREEN COMPUTING?

Our so called technically successful world almost sounds fake .We have great machines and equipments to accomplish our tasks, great gadgets with royal looks and features make our lives more impressive and smooth. Today almost all streams weather its IT, medicine, transportation, agriculture uses machines which indirectly requires large amount of power and money for its effective functioning.

Newton‘s Third Law of Motion states that

—For every action, there is an equal and opposite reaction, therefore consumption of energy sources has a negative reaction on the environment. Data centers use a large amount of power and consequently cooling energy is needed to counteract the power usage. It can be an endless circle of energy waste.

Hence the three main reasons that made us realize the need for growing green are:-

1. Release of harmful gases from electronics.
2. More utilization of power and money.
3. Increase of E-waste and improper disposal.

3.2 Approaches to Green Computing

3.2.1. Virtualization:

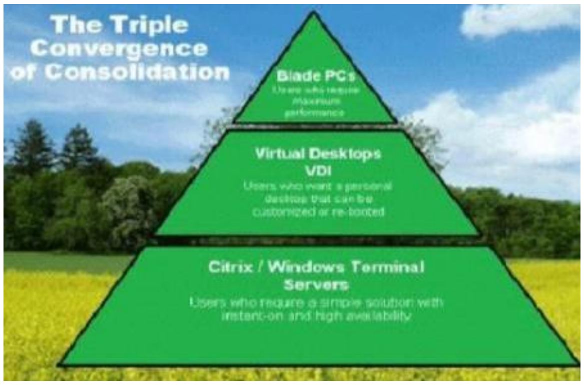

The Triple Convergence of Consolidation
Blade PCs
Users who require maximum performance
Virtual Desktops VDI
Users who want a personal desktop that can be customized or re-booted
Citrix / Windows Terminal Servers
Users who require a simple solution with instant-on and high availability

Figure 5: Virtualization [18]

Computer Virtualization means abstraction of computer resources, such as the process of running two or more logical computer systems on one set of physical hardware. Through Virtualization, a system administrator can combine several physical systems into virtual machines on one single, powerful system, thereby reducing power and cooling consumption. In the longer run, more profits and less expenses.

Reducing the number of hardware components and replacing them with Green Computing systems reduces energy costs for running hardware and cooling as well as reducing carbon dioxide emissions and conserving energy.

The phrase —green computing may conjure up some humorous images if you‘re not familiar with the term. Normally, we think of gas guzzling cars, factories, pesticides, and such when considering environmental concerns. So what does the term —green signify in the context of everyday computing? In a world where computers are everywhere, and environmental concerns are growing by the day, we need to consider how we can build, use and dispose of computers in a manner

that‘s conducive to the health of the environment. That includes reducing the use of lead and other hazardous materials in manufacturing, being careful about energy consumption and paper waste by computer users, and concern for salvage or recycling of old computers. Millions of computers are dumped into landfills each year. That equates to a lot of lead, cadmium, mercury and brominates flame retardants, which will contaminate both water and air.

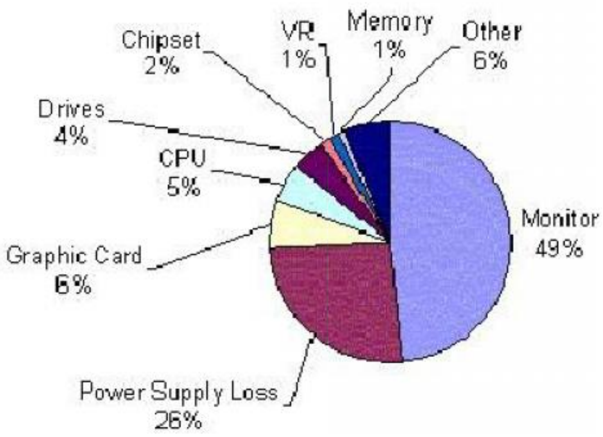


Figure 6: Component Wattage [19]

3.2.2 Algorithm Efficiency

The efficiency of algorithms has an impact on the amount of computer resources required for any given computing function and there are many efficiency trade-offs in writing programs. As computers have become more numerous and the cost of hardware has declined relative to the cost of energy, the energy efficiency and environmental impact of computing systems and programs has received increased attention.

The ‗energy cost of a single Google search. The Green 500 list‚ rates super computers by energy efficiency.

3.2.3 Power management

The Advanced Configuration and Power Interface (ACPI), an open industry standard, allows an operating system to directly control the power saving aspects of its underlying hardware. This allows a system to automatically turn off components such as monitors and hard drives after set periods of inactivity. In addition, a system may hibernate, where most components (including the CPU and the system RAM) are turned off. ACPI is a successor to an earlier Intel-Microsoft standard called Advanced Power Management, which allows a computer‘s BIOS to control power management functions.

3.2.4 Power Supply

Desktop computer power supplies (PSUs) are generally 70-75% efficient, dissipating the remaining energy as heat. An industry initiative called 80 PLUS certifies PSUs that are at least80% efficient; typically these models are drop-in replacements for older, less efficient PSUs of the same form factor. As of July 20, 2007, all new Energy Star 4.0-certified desktop PSUs must be at least 80% efficient.

3.2.5 Storage

Smaller form factor (e.g. 2.5 inch) hard disk drives often consume less power per gigabyte than physically larger drives. Unlike hard disk drives, solid-state drives store data in flash memory or DRAM. With no moving parts, power consumption may be reduced somewhat for low capacity flash based devices. Even at modest sizes, DRAM-based SSDs may use more power than hard disks, (e.g., 4GB I-RAM uses more power and space than laptop drives). Flash based drives are generally slower for writing than hard disks.

3.2.6 Display

LCD monitors typically use a cold-cathode fluorescent bulb to provide light for the display. Some newer displays use an array of light-emitting diodes (LEDs) in place of the fluorescent bulb, which reduces the amount of electricity used by the display.

3.2.7 Materials Recycling

Computer systems that have outlived their particular function can be repurposed, or donated to various charities and non-profit organizations. However, many charities have recently imposed minimum system requirements for donated equipment. Additionally, parts from outdated systems may be salvaged and recycled through certain retail outlets and municipal or private recycling centers. Recycling computing equipment can keep harmful materials such as lead, mercury, and hexavalent chromium out of landfills, but often computers gathered through recycling drives are shipped to developing countries where environmental standards are less strict than in North America and Europe. The Silicon Valley Toxics Coalition estimates that 80% of the post-consumer e-waste collected for recycling is shipped abroad to countries such as China, India, and Pakistan. Computing supplies, such as printer cartridges, paper, and batteries may be recycled as well.

3.2.8 Telecommuting

Teleconferencing and telepresence technologies are often implemented in green computing initiatives. The advantages are many; increased worker satisfaction, reduction of greenhouse gas emissions related to travel, and increased profit margins as a result of lower overhead costs for office space, heat, lighting, etc. The savings are significant; the average annual energy consumption for U.S. office buildings is over 23 kilowatt hours per square foot, with heat, air conditioning and lighting accounting for 70% of all energy consumed. Other related initiatives, such as hotel ling, reduce the square footage per employee as workers reserve space only when they need it. Many types of jobs — sales, consulting, and field service— integrate well with this technique.

3.3 Role of IT Vendors

3.3.1 APPLE

Four areas of particular attention are product and packaging design, materials, energy efficiency, and recycling. Each aspect of the design cycle provides significant challenges, yet our efforts in these areas have resulted in some impressive results.

Figure 7: Apple cycle [21]

3.3.1.1 Product design:

It all begins here. Reducing the environmental impact of our products starts with the product design phase. Design dictates the quantity of raw materials as well as the type and recyclability of materials used. It also determines how much energy is consumed during manufacturing and product use. For example, the amazingly slim 20-inch iMac is made from highly recyclable glass
andaluminum and it is so energyefficient it consumes about the s
ame amount of power as astandard light bulb when on.

3.3.1.2 Materials:

Apple helps to safeguard the environment - as well as consumers, safety –by restricting the use of environmentally harmful compounds in our materials and manufacturing processes. In addition to the substances that have already been restricted or eliminated, Apple is removing elemental forms of bromine and chlorine from our products, not just polyvinylchloride (PVC) and brominates flame retardants (BFRs). Then MacBook family also uses mercury-free light-emitting diode (LED) displays, with arsenic-free display glass.

3.3.1.3 Energy efficiency:

A devices greatest contribution to greenhouse gas emissions comes from its consumptions of energy over time. Apple has made great strides in recent years to optimize the energy efficiency of our hardware and created tools, such as the Energy Saver feature in Mac OSX, that allow consumers to manage the power consumption of their computers. Since 2001, Apple desktop computers, portable computers, and displays have earned the energy starting.

3.3.1.4 Recycling:

Apple‘s holistic, lifecycle approach to recycling includes using highly recyclable materials in products in addition to providing extensive take-back programs that enable consumers and businesses to safely dispose of used Apple equipment. Since our first take-back initiative began in Germany in 1994, we have instituted recycling programs in 95 percent of the countries where our products are sold - diverting over 53million pounds of electronic equipment from landfills worldwide. Apple is on track to eliminate toxic chemicals from our products. In the 2008 Environmental Update Steve Jobs provides an overview on Apple‘s progress to eliminate mercury and arsenic from displays and Brominates Flame Retardants (BFR‘s) and Polyvinyl Chloride (PVC) from internal components. Steve Jobs also talks about Apple‘s policy on climate change, steps taken to improve product energy-efficiency as well as overall recycling performance during 2007.

3.3.2 WIPRO

Wipro Limited, a leading player in Global IT and R&D services, is committed towards environmental sustainability by minimizing the usage of hazardous substances and chemicals which have potential impact on the ecology. Ithas joined hands with WWF India, one of the largest conservation organizations in thecountry, to directly deal with issues of climate change, water andwaste management and biodiversity conservation.

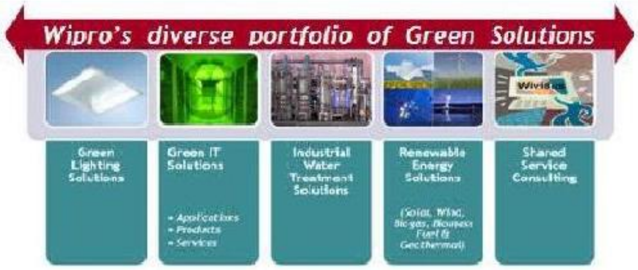

Wipro's diverse portfolio of Green Solutions
Wivision
Green Lighting Solutions
Green IT Solutions
• Applications
• Products
• Services
Industrial Water Treatment Solutions
Renewable Energy Solutions
(Solar, Wind, Bio-gas, Biomass Fuel & Geothermal)
Shared Service Consulting

Figure 8: Wipro's portfolio

3.3.2.1 Green Lighting Solutions:

1. Complete range of Brightness Management Products for Green Buildings. Ability to integrate lighting and lighting management systems for Green Building performance standards. Role of Lighting for GREEN buildings: 17%– 20% of the overall building‘s energy usage.
2. Optimize Energy Performance
3. Green Computing24 Department of IT
4. High efficiency luminaries design.
5. High efficiency light sources
6. Compact Fluorescent Lamp, LED, etc.
7. Lighting controls.
8. High efficiency control gear.
9. Personalized controls through task lighting intelligent lighting systems.

3.3.3. GOOGLE

Google's mission is to organize the world's information and make it universally accessible and useful. Hundreds of millions of users access our services through the web, and supporting this traffic requires lots of computers. We strive to offer great internet services while taking our energy use very seriously. That's why, almost a decade ago; we started our efforts to make our computing infrastructure as sustainable as possible. Today we are operating what we believe to be the world's most efficient data centers. The graph below shows that our Google-designed data centre's use considerably less energy -both for the servers and the facility itself - than a typical data centre. As a result, the energy used per Google search is minimal. In fact, in the time it takes to do a Google search, your own personal computer will use more energy than we will use to answer your query.

Individuals and businesses to adopt greener lifestyles and work styles, in terms of the environmental debate computing is definitely both part of the problem and part of the solution. Through more environmentally aware usage (such as more effective power management and shut-down during periods of inactivity), and by adopting current lower power technologies, computers can already be made significantly more energy efficient. Indeed, just as we now look back and wonder why automobiles a decade or two ago used to guzzle so much petrol, in a decade's time we will no doubt be staggered that a typical desktop PC used to happily sit around drawing 100-200W of power every hour night and day, and when accomplishing no more than displaying a screen saver. The computing industry is more prepared and far more competent than almost any other industry when it comes to facing and responding to rapid change. Environmentally it is not a good thing that most PCs -- especially in companies -- have typically entered a landfill after only a few years in service. However, this reality does at least mean that a widespread mindset already exists for both adapting to and paying money for new computer hardware on a regular basis. Hence, whereas it took decades to get more energy efficient cars on the roads, it will hopefully only take a matter of years to reach a state of affairs where most computers are using far less power than they needlessly waste today.

IV. FUTURE SCOPE

As 21st century belongs to computers, gizmos and electronic items, energy issues will get a serious ring in the coming days, as the public debate on carbon emissions, global warming and climate change gets hotter. If we think computers are nonpolluting and consume very little energy we need to think again. It is estimated that out of $250 billion per year spent on powering computers worldwide only about 15% of that power is spent computing- the rest is wasted idling. Thus, energy saved on computer hardware and computing will equate tones of carbon emissions saved per year. Taking into consideration the popular use of information technology industry, it has to lead a revolution of sorts by turning green in a manner no industry has ever done before. Opportunities lie in green technology like never before in history and organizations are seeing it has a way to create new profit centers while trying to help the environmental cause. The plan towards green IT should include new electronic products and services with optimum efficiency and all possible options towards energy savings.

4.2 Steps to Green Computing

As of Oct. 20, there are new performance requirements to qualify for the Energy Star rating for desktop and notebook computers, workstations, integrated computers, desktop-derived servers and game consoles. These specifications go into effect on July 20.

But businesses don‘t have to wait until then to initiate more environmentally-friendly computing practices. Here are five first steps you can take toward a green computing strategy.

4.2.1 Develop a sustainable green computing plan

Discuss with your business leaders the elements that should be factored into such a plan, including organizational policies and checklists. Such a plan should include recycling policies, recommendations for disposal of used equipment, government guidelines and recommendations for purchasing green computer equipment. Green computing best practices and policies should cover power usage, reduction of paper consumption, as well as recommendations for new equipment and recycling old machines. Organizational policies should include communication and implementation.

4.2.2 Recycle:

Discard used or unwanted electronic equipment in a convenient and environmentally responsible manner. Computers have toxin metals and pollutants that can emit harmful emissions into the environment. Never discard computers in a landfill. Recycle them instead through manufacturer programs such as HP' Planet Partners recycling service or recycling facilities in your community. Or donate still-working computers to a non-profit agency.

4.2.3 Make environmentally sound purchase decisions

Purchase Electronic Product Environmental Assessment Tool registered products. EPEAT is a procurement tool promoted by the nonprofit Green Electronics Council to:

•Help institutional purchasers evaluate, compare and select desktop computers, notebooks and monitors based on environmental attributes.

•Provide a clear, consistent set of performance criteria for the design of products.

4.2.4 Reduce Paper Consumption:

There are many easy, obvious ways to reduce paper consumption: e-mail, electronic archiving, use the ―track changes‖ feature in electronic documents, rather than red-line corrections on paper. When you do print out documents, make sure to use both sides of the paper, recycle regularly, use smaller fonts and margins, and selectively print required pages.

4.2.5 *Conserve energy:*

Turn off your computer when you know you won‘t use it for an extended period of time. Turn on power management features during shorter periods of inactivity. Power management allows monitors and computers to enter low-power states when sitting idle. By simply hitting the keyboard or moving the mouse, the computer or monitors awakens from its low-power sleep mode in seconds. Power management tactics can save energy and help protect the environment

V. CONCLUSION

- So far, consumers have not cared about ecological impact when buying computer s, they have cared about speed and price.
- Now green materials are developed every year, and many toxics ones are already beings replaced by them.
- The greenest computer will not miraculously fall from the sky one day, it will be the product of year of improvements.

REFERENCES

[1]. http://seminarprojects.com/Thread-green-computing-a-seminar-report#ixzz1shD7uo8i

[2]. http://www.scribd.com/doc/8574409/green-computing

[3]. http://www.scribd.com/doc/28697765/Green-Computing

[4]. http://igreenik.com/innovations/green-computing/green-computing/212/

[5]. http://firstfiledir.com/search.php?q=green+computing+pdf

[6]. http://seminarprojects.com/Thread-green-computing-a-seminar-report

[7]. http://www.seminarpaper.com/2011/12/seminar-report-on-green-computing.html

Heat Transfer Augmentation In Rectangular Channel Using Three Triangular Prisms

Manoj Kumar[1], Sunil Dhingra[2]

[1] Department of Mechanical Engineering, Ganga Institute of Technology and Management, Kablana, Jhajjar, Haryana, INDIA

[2] Department of Mechanical Engineering, UIET, Kurukshetra University, Kurukshetra, Haryana, INDIA

***Abstract*--The aim of this study is to investigate the heat transfer and fluid flow characteristics in a rectangular channel in the presence of triangular prisms in the laminar and turbulent flow regime. The computations are performed for Reynolds number 50 to 500 for laminar and 5000 to 20000 for turbulent flow. The Navier-Stokes equation and the energy equation are solved by using Fluent [14.0]. The quadrilateral meshing method is used for the computational domain. By using three triangular prisms attached with channel wall, the heat transfer is augmented considerably. This is due to the large vortices produced by the prisms as compared to the plane channel. The results shows that in the presence of the triangular prism with circle at their edges, the average Nusselt number is 9.72 % more as compared to presence of triangular prism without circle. It is further observed that the heat transfer increases with the increase in Reynolds number (Re).The enhancement is due to the formation of vortices which travels long way in the downstream direction. However the heat transfer enhancement is associated with greater pressure drop.**

***Keyword:* Heat transfer enhancement, Triangular Prism, Reynolds Number, Nusselt Number**

I. INTRODUCTION

Heat exchangers are used in a wide range of engineering applications, such as, power generation, auto and aerospace industry, electronics and HVAC. Typical heat exchangers experienced by us in our daily lives include condensers and evaporators used in air conditioning units and refrigerators. Boilers and condensers in thermal power plants are examples of large industrial heat exchangers. There are heat exchangers in our automobiles in the form of radiators and oil coolers. Heat exchangers are also abundant in chemical and process industries. There is a wide variety of heat exchangers for diverse kinds of uses; hence the construction also would differ widely. Thermal performance of heat transfer devices can be improved by heat transfer enhancement techniques. Many techniques based on both active and passive methods are used to enhance heat transfer in these applications. Among these methods one can find systems involving vortex generators such as fins, prisms, turbulence promoters and other cylinders. The geometrical characteristics of vortex generators play a significant role in the rate of heat transfer. Disturbance promoters increase fluid mixing and interrupt the development of the thermal boundary layer, leading to enhancement of heat transfer. The current research work is undertaken to compute the heat transfer enhancement in a channel flow with three triangular prisms.

II. LITERATURE REVIEW

Recently, vortex generators have been used by many researchers for the heat transfer enhancement in various thermal systems. For example, [1] numerically studied the effect of longitudinal vortex generator on the heat transfer in a fin-andtube heat exchanger. The results reveal that the transverse flow of air stream through the punched holes disturbs the air flow in the lower channel, enhancing the heat transfer on the under surface of fin. Reference [2] proved that the use of a triangular prism could enhance significantly the heat transfer in a channel. Reference [3] obtained numerically the rate of heat transfer enhancement in a channel due to the presence of a triangular element. The results indicate that heat transfer in the channel is augmented by around 15%. Turbulent flow and heat transfer in a heated channel with a triangular prism has been investigated, numerically by [4]. The results showed larger heat transfer augmentation. The control of laminar steady forced convection heat transfer in a channel, with three blocks and a triangular adiabatic control element, has been studied numerically by [5]. It has been shown that the heat transfer is enhanced and the best element position determined.

Reference [6] conducted a numerical study to analyze the unsteady flow and heat transfer in a horizontal channel with a built-in heated cylinder. The heat transfer was found to be slightly affected by the blockage ratio and correlations for the Nusselt number were obtained. Heat transfer and fluid flow characteristics in a channel, with the presence of a triangular prism, has been numerically investigated in the laminar flow regime by [7]. It has been found that the average Nusselt number is augmented and the heat transfer increases with the blockage ratio. Heat transfer enhancement for triangular dual prisms has been found to be larger than that for the case of a single triangular prism, for the same blockage ratio. Reference [8] studied the fluid flow and heat transfer across a long equilateral triangular cylinder set in a horizontal channel for a fixed blockage ratio of 0.25. It has been found that the average Nusselt number increases with the Reynolds number. Simple correlations for Nusselt numbers have also been obtained. Two dimensional laminar forced convection heat transfers around a horizontal triangular cylinder in an air flow have been investigated numerically by [9]. Two orientations of the triangular cylinder have been considered, the first corresponds to the case for which the vertex of the triangle is facing the flow. As for the second case, the base of the triangle is facing the flow. Correlations are obtained and local Nusselt numbers have been found to be in qualitative agreement with corresponding data reported in the literature. Reference [10] analyzed the effect of wall proximity of a triangular cylinder on the heat transfer and flow in a horizontal channel. Results showed that when the triangular element is close to the wall, the vortex shedding is removed and subsequently the heat transfer rate decreases at low Reynolds number.

Experimental investigations have been reported by [11] on steady forced convection heat transfer from the outer surfaces of horizontal triangular cylinders in an air flow. Local Nusselt numbers around the obstacles are observed to decrease, at the beginning, up to the separation points and then increase, in the transition regime, up to the turbulent limit where they decrease again. Reference [12] studied the heat transfer and fluid flow in a channel using an inclined block as an obstacle. By the use of the inclined block, larger vortices were produced and thus heat transfer was augmented considerably. A heat transfer optimization of a channel with three blocks attached to its bottom wall and an inserted triangular cylinder has been carried out by [13]. The goal of the study is to maximize the heat transfer rate as well as achieving heat flux uniformity above the blocks. A genetic algorithm combined with a Gaussian process has been used as an optimization algorithm for that purpose. The results showed that the larger value of the standard deviation multiplier is the more uniform Nusselt numbers are. Moreover, the optimum position of the vortex generator has been found to be above the first block. In this study we present a numerical simulation of flow and heat transfer by forced convection in a rectangular channel. In order to enhance heat transfer, four triangular prisms acting as a vortex generator, arranged in staggered manner are used. The triangular prisms best position, allowing maximal heat dissipation, has been determined. k−ε turbulence model is used to predicting the heat transfer and fluid flow characteristics in turbulent flow.

III. GEOMETRY AND GOVERNING EQUATIONS

Fig.1 represents a two dimensional computational domain. Two neighboring plates form a rectangular channel of height "H" and length “8.4 H”. The distance between the plates is taken as unity i.e. H = 1 m. The blockage ratio (BR = B/H) is taken as 0.25, where “B” is the base of the prism. The sides of the prism form an equilateral triangle. The computations are performed for two different arrangements of prisms in the Reynolds number range 50-500 in laminar and 5000-20000 in turbulent; is carried out for the analysis of heat enhancement. The first triangular prism base is placed at a distance of 2 H from the start of channel and the last triangular prism is placed at a distance of 2 H from the rear end of the channel.

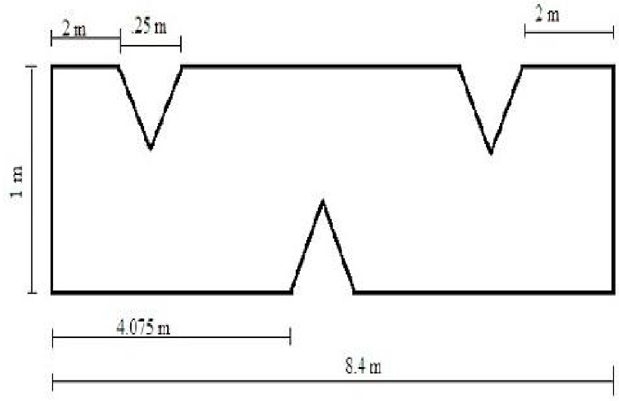


Fig.1: A 2-D rectangular channel having three triangular prisms, without circle at their edges

Fig.2: shows a 2-D rectangular channel consists of three triangular prisms with built-in circles at their edges. The diameter of circle is .15 m

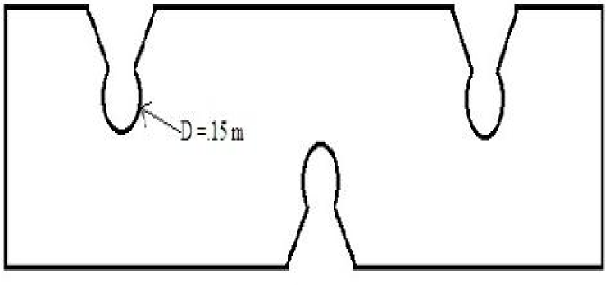


Fig.2: A 2-D rectangular channel having three triangular prisms, with circle at their edges

A. *Governing Equations*

The governing two-dimensional equations, in a Cartesian coordinate system, for incompressible, steady, with constant fluid properties, are as follows:

1) Continuity equation

$$\frac{\partial U}{\partial X}+\frac{\partial V}{\partial Y}=0$$

2) Mometum equation

$$\frac{\partial U}{\partial^2}+\frac{\partial\left(U^2\right)}{\partial X}+\frac{\partial(UV)}{\partial Y}=-\frac{\partial P}{\partial X}+\frac{1}{\mathrm{Re}}\left(\frac{\partial^2 U}{\partial X^2}+\frac{\partial^2 U}{\partial Y^2}\right)$$

$$\frac{\partial V}{\partial^2}+\frac{\partial(UV)}{\partial X}+\frac{\partial\left(V^2\right)}{\partial Y}=-\frac{\partial P}{\partial X}+\frac{1}{\mathrm{Re}}\left(\frac{\partial^2 V}{\partial X^2}+\frac{\partial^2 V}{\partial Y^2}\right)$$

3) Energy equation

$$\frac{\partial\overline{\ }}{\partial^2}+\frac{\partial U\overline{\ }}{\partial X}+\frac{\partial V\overline{\ }}{\partial Y}=\frac{1}{\mathrm{Re}\,\mathrm{Pr}}\left(\frac{\partial^2\overline{\ }}{\partial X^2}+\frac{\partial^2\overline{\ }}{\partial Y^2}\right)$$

The solution domain of the considered two dimensional flows is geometrically simple, which is a rectangle on the x – y plane, enclosed by the inlet, outlet and wall boundaries. The working fluid is air. The inlet temperature of air is considered to be uniform at 300 K. On walls, no-slip boundary conditions are used for the momentum equations. A constant surface temperature of 400 K is applied to the top and bottom wall of the channel. A uniform one dimensional velocity is applied as the hydraulic boundary condition at the inlet of the computational domain. The pressure at the outlet of the computational domain is set equal to zero gauge. No-slip boundary conditions are taken for the prism. Aluminum is selected as the material for prism.
The properties of air taken are standard.

Density(ρ) kg/m3	Specific heat(cp) J/kg-k	Thermal conductivity(k) W/m-k	Viscosity(μ) Kg/m-s
1.225	1006.43	0.0242	1.7894e-5

IV. TURBULENCE MODEL

One of the most widely spread models is the standard k-є model proposed by Launder and Spalding. This model implies two transport equations i.e. turbulent kinetic energy and the dissipation of turbulent kinetic, as follows:

Transport Equation for Turbulent Kinetic Energy k

$$\frac{\partial(\rho k)}{\partial t}+div\,(\rho k\mathbf{U})=div\left(-\overline{p'\mathbf{u}'}+2\mu\,\overline{\mathbf{u}'e_{ij}'}-\rho\,\tfrac{1}{2}\,\overline{u_i'.u_i'u_j'}\right)$$

Transport Equation for Turbulent Dissipation Rate ε

$$\frac{\partial(\rho\varepsilon)}{\partial t}+div\,(\rho\varepsilon\mathbf{U})=div\left[\frac{\mu_t}{\sigma_\varepsilon}grad\ \varepsilon\right]+C_{1\varepsilon}\frac{\varepsilon}{k}$$

and the eddy viscosity is define as:

$$\mu_t = \rho c_\mu \frac{k^2}{\varepsilon}$$

The model coefficients are (σk; σε; C1ε; C2ε; Cμ) as follows:

Cμ	C1ε	C2ε	σ_k	σε
0.09	1.44	1.92	1.00	1.30

V. NUMERICAL PROCEDURE

The CFD software (Fluent) is used to simulate the fluid flow and temperature field. The required mesh for computational domain is generated with the help of FLUENT mesh tool. The domain is discretized and equations are formulated using finite volume method. The finite difference governing equations are discretized using the finite volume method. The SIMPLE algorithm is used for the convective terms in the solution equations. The second order up-winding scheme is used to calculate the flow variables. The under relaxation factor is varied between 0.3 and 1.0. The residuals for continuity, momentum and energy equations are all taken as 10-7. The solver iterates the equations till the convergence is obtained for the set residuals.

VI. RESULT AND DISCUSSION

A. *Flow Characteristics*

The flow structure in presence of triangular prisms can be discerned by looking at velocity vector plots. The velocity vector plots for both the orientations are shown below The flow passage decreases as the flow moves towards the prism and the flow passage increases as the flow moves away from the prism. The figures 3 and 4 show the velocity contours of the computation domain of the plane channel for both the arrangements of triangular prisms.

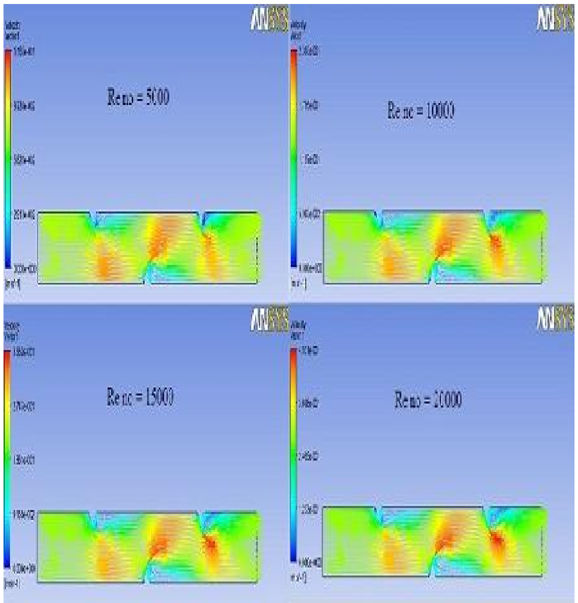


Fig: 3 Velocity vector plot for Re no 5000 to 20000, triangular prism without circle

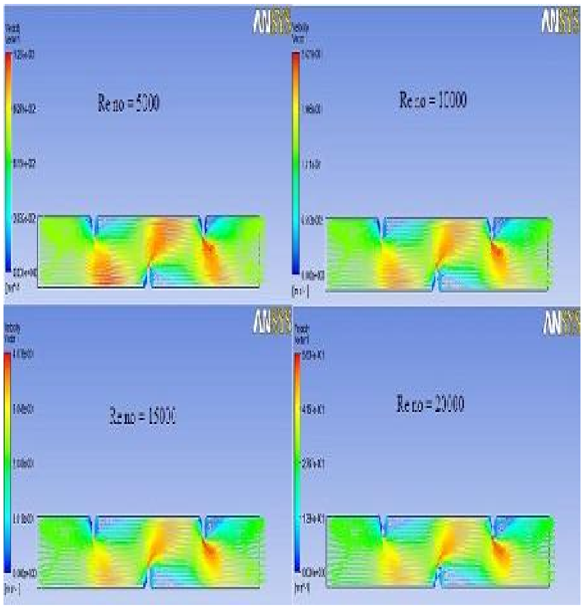


Fig: 4 Velocity vector plot for Re no 5000 to 20000, triangular prism with circle

B. *Temperature Contours and Heat Transfer Characteristics*

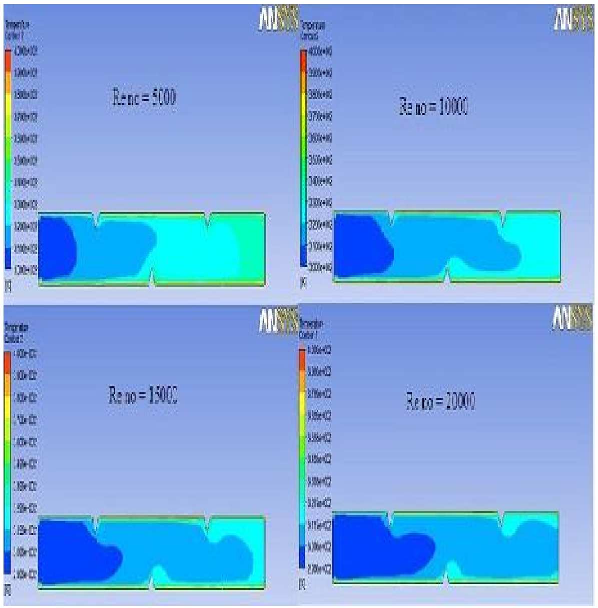


Fig: 5 Temperature contours for Re no 5000 to 20000, triangular prism without circle

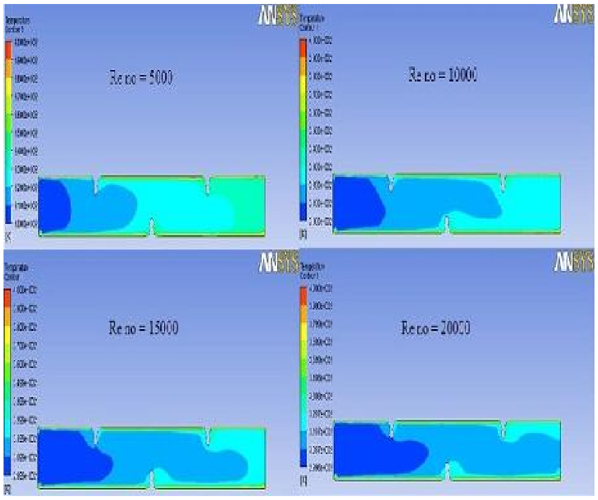


Fig: 6 Temperature contours for Re no 5000 to 20000, triangular prism with circle

The above figures show the temperature contours of the computation domain of the plane channel for both the arrangements of triangular prisms with or without circle at their edges. The presence of the obstacle causes the formation of counter rotating vortices which cause the mixing of fluid and hence and increase in the heat transfer coefficient of the fluid and hence the temperature of the fluid increases. The rate of increment in temperature at outlet is more in arrangements having triangular prisms with circle at their edges.

C. *Pressure contours and characteristics*

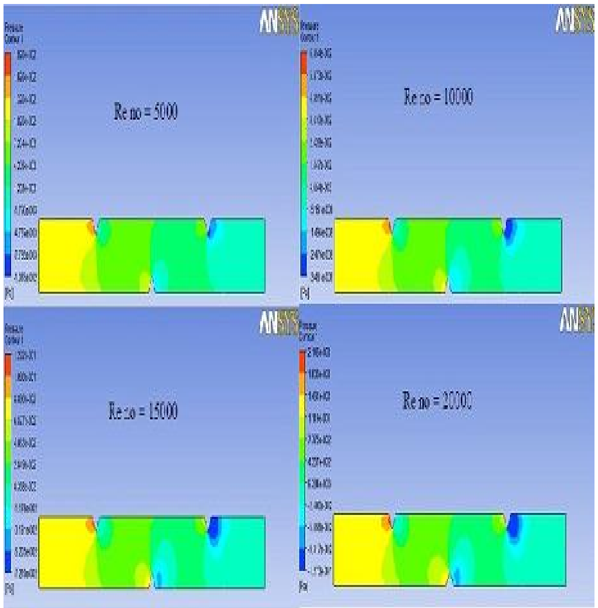


Fig: 7 Pressure contours for Re no 5000 to 20000, triangular prism without circle

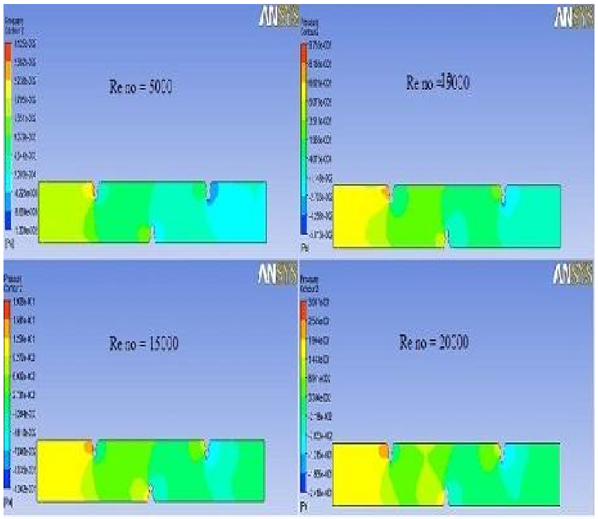


Fig:8 Pressure contours for Re no 5000 to 20000, triangular prism with circle

Pressure contours shows the pressure drop across the channel length and heat transfer through the channel walls. The heat enhancement is due the more pressure drop in the channel.

The enhancement of heat transfer achieved by using triangular prisms is associated with an increase in the pressure loss. Figure 9 and 10 shows the pressure variation along the channel length. The figures shows that the maximum pressure drop occurs just downstream of the triangular prism because of the form drag and then pressure is recovered and approaches a stabilized value till the end.

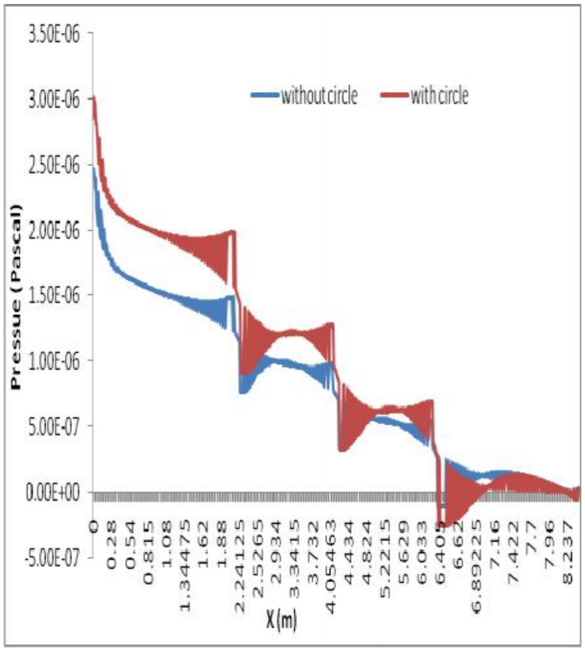


Fig. 9: Pressure variations along the channel length in laminar flow zone

D. *Nusselt number (Nu) vs. Reynolds number (Re)*

E.

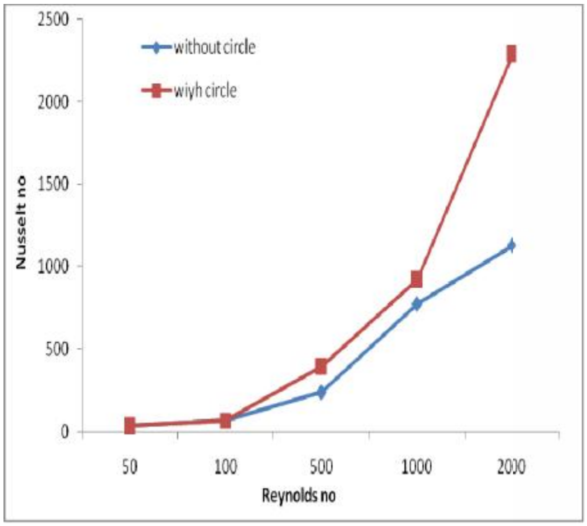


Fig. 10: Nusselt number (Nu) vs. Reynolds number (Re) in laminar flow

The above figures show the variation of Nusselt number vs. Reynolds number. Figures clearly define the value of Nusselt number with the increase of Reynolds number.

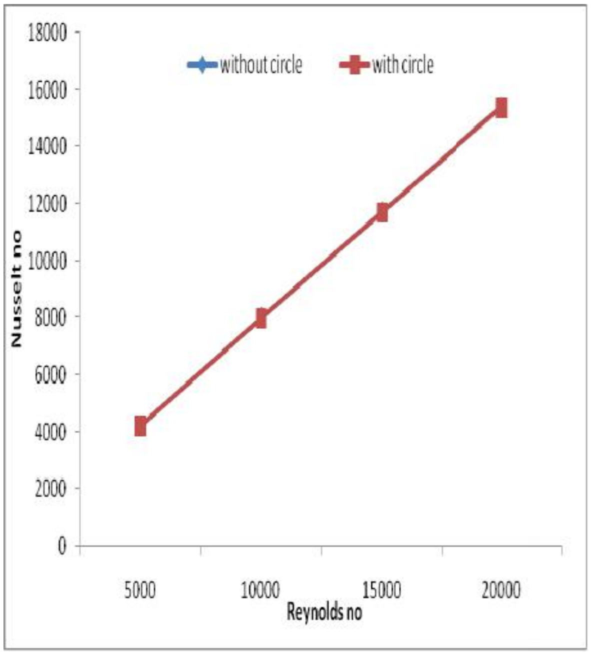


Fig 11 : Nusselt number (Nu) vs. Reynolds number (Re) in turbulent flow

F. *Pressure vs. Reynolds number (Re)*

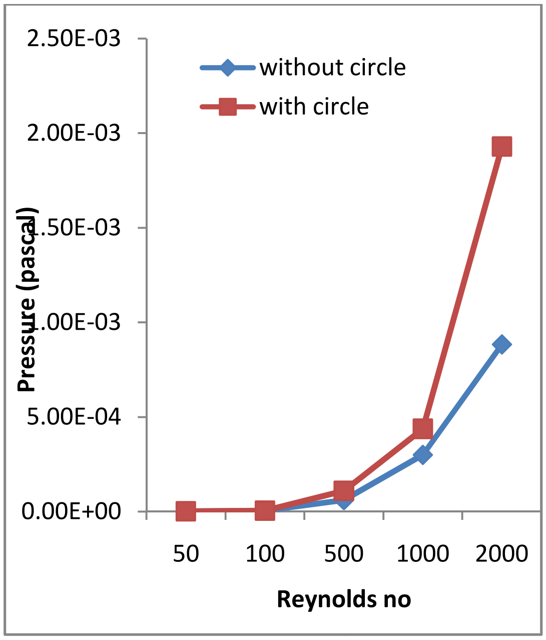


Fig.12: Pressure vs. Reynolds number (Re) in laminar flow

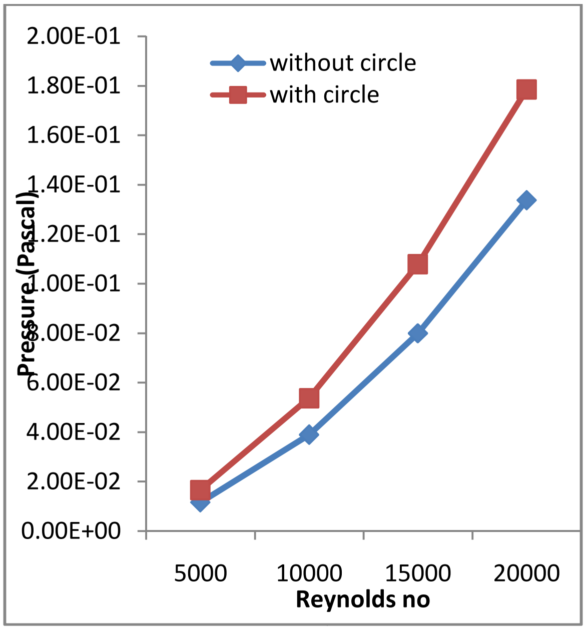


Fig 13: Pressure vs. Reynolds number (Re) in turbulent flow

These are the pressure vs. Reynolds number plots which gives the value of pressure difference between the inlet to outlet. The value of pressure difference is clearly shown in plots. There is more pressure drop when prism with circular edge is used in the channel flow.

VII. CONCLUSION

In the present problem, the CFD analysis of heat transfer enhancement in 2-D rectangular channel is studied in detail. The flow regimes are laminar and turbulent. The heat transfer characteristics and flow characteristics are studied in detail.

On the basis of the results obtained, the following conclusions are made:

1) The presence of more than single triangular prism significantly improves the heat transfer enhancement. The % increase in heat transfer enhancement in the presence of three triangular prisms at Re no= 500, is5.34 % more as compare to single prism at Re no = 500.
2) In laminar flow regime up to Reynolds no 100, the prisms arrangement having without circle at their edges gives better performance as compare to other arrangement. The % increase in average Nusselt number at Re no 100 is 1.59 % more as compare to other at Re no 100.
3) After Reynolds number 100, the prisms having circles at their edges gives better performance as compare to the other. The % increase in average Nusselt number at Re no 1000 is 16.08 % more as compare to other arrangements having prisms without circle at their edges at Re no 1000.
4) Also the % increase in Nusselt number with respect to Reynolds number is more in arrangement having prisms with circle at their edges.
5) The pressure loss is also increased with the increase of Reynolds number due to the presence of three triangular prisms.

VIII. NOMENCLATURE

a	area of the rectangular channel, m2
h	average heat transfer coefficient, W/m2K
H	characteristic length dimension (distance between the plates), m
L	length of the channel, m
V	mean velocity, m/s
Cp	specific heat capacity of air, J/kg K
k	thermal conductivity of air, W/m K
Nu	Nusselt number
ΔP	pressure drop, Pa
Re	Reynolds number
q	heat flux, W/m2
T_o	average temperature of outlet
T_i	Inlet temperature
Greek Symbols	
ρ	density of air, kg/m3
μ	fluid dynamic viscosity, kg/m-s
μ_t	eddy viscosity

REFERENCES

[1] J. M. Wu and W. Q. Tao, “Effect of longitudinal vortex generator on heat transfer in rectangular channels,” Applied Thermal Engineering, vol. 37, pp. 67-72, 2012.

[2] H. Abbassi, S. Turki, and S. Ben Nasrallah, “Numerical investigation of forced convection in a horizontal channel with a built-in triangular prism,” Int. J. Thermal Sciences, vol. 40, pp. 649-658, 2001.

[3] H. Chattopadhyay, “Augmentation of heat transfer in a channel using a triangular prism,” Int. J. Thermal Sciences, vol. 46, pp. 501-505, 2007.

[4] A. C. Benim, H. Chattopadhyay, and A. Nahavandi, “Computational analysis of turbulent forced convection in a channel with a triangular prism,” Int. J. Thermal Sciences, vol. 50, pp. 1973-1983, 2011.

[5] H. F. Oztop, Y. Varol, and D. E. Alnak, “Control of heat transfer and fluid flow using a triangular bar in heated blocks located in a channel,” Int. Comm. in Heat and Mass Transfer, vol. 36, pp. 878-885, 2009.

[6] S. Turki, H. Abbassi, and S. B. Nasrallah, “Two-dimensional laminar fluid flow and heat transfer in a channel with a built-in heated square cylinder,” Int. J. Thermal Sciences, vol. 42, pp. 1105-1113, 2003.

[7] B. Budania and H. Shergill, “Simulation Heat Transfer Enhancement in a Laminar Channel Flow with Built-in Triangular Prism,” Int. Journal on Emerging Technologies vol. 3, no. 1, pp. 92-96, 2012.

[8] S. Srikanth, A.K. Dhiman, and S. Bijjam, “Confined flow and heat transfer across a triangular cylinder in a channel,” International Journal of Thermal Sciences, vol. 49, pp. 2191-2200, 2010.

[9] O. Zeitoun, M. Ali, and A. Nuhait, “Convective heat transfer around a triangular cylinder in an air cross flow,” International Journal of Thermal Sciences, vol. 50, pp. 1685-1697, 2011.

[10] M. Farhadi, K. Sedighi, and A. M. Korayem, “Effect of wall proximity on forced convection in a plane channel with a built-in triangular cylinder,” Int. J. Thermal Sciences, vol. 49, pp. 1010-1018, 2010.

[11] M. Ali, O. Zeitoun, and A. Nuhait, “Forced convection heat transfer over horizontal triangular cylinder in cross flow,” International Journal of Thermal Sciences, vol. 50, pp. 106-114, 2011.

[12] M. Gupta, U. Khod, and S. Kumar, “Heat Transfer Augmentation Using an Inclined Block in Laminar Channel Flow,” Recent Trends in Engineering Research, vol. 1, no.1, pp. 105-108, Dec. 2011.

[13] S. A. Beig, E. Mirzakhalili, and F. Kowsari, “Investigation of optimal position of a vortex generator in a blocked channel for heat transfer enhancement of electronic chips,” International Journal of Heat and Mass Transfer, vol. 54, pp. 4317-4324, 2011.

[14] Manoj Kumar, Sunil Dhingra and Sumit Kumar, (2014). Heat transfer enhancement in a channel flow with built in equilateral triangular prisms in zig-zag arrangement. International Journal for Scientific Research & Development, 2321-0613.

[15] Manoj Kumar, Sunil Dhingra and Gurjeet Singh, (2014). Heat Transfer Augmentation In Rectangular Channel Using Four Triangular Prisms Arrange In Staggered Manner. International Journal of Enhanced Research in Science Technology & Engineering, 2319-7463.

Hiding Information in Images by Digital Watermarking Technique

Rakesh Joon[1]

[1]*Department of Electronics and Communication Engineering, Ganga Institute of Technology and Management, Kablana, Jhajjar, Haryana, INDIA*

ABSTRACT : Watermarking is a branch of information hiding which is used to secrete proprietary information in digital media like photographs, digital song, music or digital video. Watermarking can be used for proprietor identification to identify the content owner, finger printing, to identify the buyer of the content, for broadcast monitoring to determine royalty payments and authentication, to determine whether the data has been altered in any manner from its original form. This research proposes a technique that uses the DWT, DCT as well as the SVD. The Host image is transformed using the DCT then DWT divided in to frequency then the SVD of each frequency block is taken. The watermark image is divided in to sub band using DWT then SVD of each block is taken. The watermark is embedding into host image then inverse SVD, Inverse DWT and inverse DCT results in the watermarked image. The proposed technique uses the DWT, DCT as well as the SVD; this makes the proposed technique better as compared to the existing technique that uses only the DWT and the SVD in a different manner. The simulation of the proposed algorithm is done using the MATLAB. The simulation result shows that the proposed algorithm is better than the existing algorithm. The PSNR values analyzed over different image are better for the proposed algorithm as compared to the existing algorithm. The proposed algorithm is more imperceptible as compared to the existing algorithm.

Keywords: Watermarking, DWT, SVD, DCT.

I. INTRODUCTION

Watermarking is a branch of information hiding which is used to hide proprietary information in digital media like photographs, digital music or digital video. The ease with which digital content can be exchanged over the Internet has created copyright infringement issues [1]. Copyrighted material can be easily exchanged over peer-to-peer networks and this has caused key concerns to those content providers who produce these digital contents. In order to protect the interest of the content providers, these digital contents can be watermarked. Watermarking can be used for owner identification to identify the content owner, finger printing, to identify the buyer of the content, for broadcast monitoring to determine royalty payments and authentication, to determine whether the data has been altered in any manner from its original form. There are some properties of watermarks [2] that are Robustness, Tamper-resistance, Bit rate, Scalability etc. Digital watermarking [3] refers to specific information hiding techniques whose purpose is to embed secret information inside multimedia content like images, video, or audio data.

Many digital watermarking methods have been proposed over the last decade [4].Digital watermarking methods can also be roughly categorized into two types: non-blind and blind. Non-blind methods require the original image at the detection end, whereas blind methods do not. Blind methods are more useful than non-blind ones because the original image may not be available in actual scenarios [3].

Digital watermarking plays an increasingly vital role for proving authenticity and copyright protection. Unfortunately the currently available formats for image in digital form do not allow any type of copyright protection. A potential solution to this kind of trouble is an electronic stamp or digital watermarking which is intended to complement cryptographic process [5].

The process of embedding the watermark into a digital data is known as Digital Watermarking. It embeds some marking information directly into the digital carrier (including multimedia, documents or software), but it is not easily noticed by human perception. Digital watermarking is a way of hiding a secret or personal message to provide copyrights and the data integrity. The concept of digital watermarking is also associated with the steganography. It is defined as covered writing, which hides the vital message in a covered media while, digital watermarking is a way of hiding a secret or personal message to provide copyrights and the data integrity. It is a innovative approach, which is appropriate for medical, military, and archival based applications. The embedded watermarks are difficult to remove and typically imperceptible, could be in the form of text, image. [4].

II. DISCRETE WAVELET TRANSFORM

Discrete Wavelet transform (DWT) is a mathematical tool for hierarchically decomposing an image. It is useful for processing of non-stationary signals. The transform is based on small waves, called wavelets, of varying frequency and limited duration. Wavelet transform provides both frequency and spatial description of an picture. Unlike conventional Fourier transform, temporal information is retained in this transformation process. Wavelets are created by translations and dilations of a fixed function called mother wavelet. This section analyses suitability of DWT for image watermarking and gives advantages of using DWT as against other transforms [6].

For 2-D images, applying DWT corresponds to processing the image by 2 -D filters in each dimension. The filters divide the input image into four non-overlapping multi-resolution sub-bands LL1,LH1, HL1 and HH1. The sub-band LL1 represents the coarse-scale DWT coefficients while the sub-bands LH1, HL1 and HH1 represent the fine-scale of DWT coefficients. To obtain the next coarser scale of wavelet coefficients, the sub-band LL1 is further processed until some final scale N is reached. When N is reached we will have 3N+1 subbands consisting of the multi-resolution sub-bands LL_N and LHx, HLx and HHx where x ranges from 1 until N. Due to its excellent spatiofrequency localization properties, the DWT is very suitable to identify the areas in the host image where a watermark can be embedded effectively. In general most of the image energy is concentrated at the lower frequency sub-bands LLx and therefore embedding watermarks in these sub-bands may degrade the image significantly. Embedding in the low frequency sub-bands, however, could increase robustness significantly. On the other hand, the high frequency subbandsHHx include the edges and textures of the image and the human eye is not generally sensitive to changes in such sub-bands. This allows the watermark to be embedded without being perceived by the human eye [6].

III. PROPOSED TECHNIQUE

The proposed technique uses the DWT, DCT as well as the SVD (Singular Value Decomposition). The Host image is transformed using the DCT then DWT divided in to frequency then the SVD of each frequency block is taken. The watermark image is divided in to sub band using DWT then SVD of each block is taken. The watermark is embedding into host image then inverse SVD, Inverse DWT and inverse DCT results in the watermarked image. This process must provide better PSNR. The whole process can also be given in form of algorithm.

PROPOSED ALGORITHM

```
1.  Input Host image say Ih
2.  Take DCT of host image to get transformed image
        IHT=DCT2(Ih)
3.  Take DWT of IHT . [LL LH HL HH]= DWT(IHT)
4.  Take SVD of Each sub Frerency
        [u1  LLd v1]=svd(LL)
        [u2  LHd v2]=svd(LH)
        [u3  HLd v3]=svd(HL)
        [u4  HHd v4]=svd(HH)
5.  Input Watermark Image say Iw
6.  Take DWT of IW.
        [LLwLHwHLwHHw]= DWT(Iw)
7.  Take SVD of Each sub Frerency
        [u1w  LLdw v1w]=svd(LLw)
        [u2w  LHdw v2w]=svd(LHw)
        [u3wHLdw v3w]=svd(HLw)
        [u4w  HHdw v4w]=svd(HHw)
8.  Add
        WLL=LLd  +const * LLdw
        WLH=LHd  +const * LHdw
        WHL=HLd  +const * HLdw
        WHH=HHd  +const * HHdw
9.  Take inverse SVD
        WLL1= ISVD(WLL)
        WLH1= ISVD(WLH)
        WHL1= ISVD(WHL)
        WHH1= ISVD(WHH)
10. Take inverse DWT
        Res=Idwt2(WLL1 WLH1 WHL1 WHH1)
11. take inverse DCT
        res=iDCT2(res)
12. Res is the resultant Watermarked Image
```

Extraction Algorithm

```
1.  Input Watermarked image say Ih
2.  Take DCT of host image to get transformed image
        IHT=DCT2(Ih)
3.  Take DWT of IHT . [LL LH HL HH]= DWT(IHT)
4.  Take SVD of Each sub Frerency
        [u1  LLd v1]=svd(LL)
        [u2  LHd v2]=svd(LH)
        [u3  HLd v3]=svd(HL)
        [u4  HHd v4]=svd(HH)
5.  Input HOST Image say Iw
6.  Take DWT of IW.
        [LLwLHwHLwHHw]= DWT(Iw)
7.  Take SVD of Each sub Frerency
        [u1w  LLdw v1w]=svd(LLw)
        [u2w  LHdw v2w]=svd(LHw)
        [u3wHLdw v3w]=svd(HLw)
        [u4w  HHdw v4w]=svd(HHw)
8.  Add
        WLL=LLd  -const * LLdw
        WLH=LHd  -const * LHdw
        WHL=HLd  -const * HLdw
        WHH=HHd  -const * HHdw
9.  Take inverse SVD
        WLL1= ISVD(WLL)
        WLH1= ISVD(WLH)
        WHL1= ISVD(WHL)
        WHH1= ISVD(WHH)
10. Take inverse DWT
        Res=Idwt2(WLL1 WLH1 WHL1 WHH1)
11. take inverse DCT
res=iDCT2(res)
12. Res is the resultant Watermark
```

The proposed algorithm can be implemented using the MATLAB and result can be compared with the existing Algorithm.

IV. RESULTS

- *Imperceptibility*

Embedding extra information in the original image will cause distortion in the image quality. The watermark is truly imperceptible if human cannot distinguish between the host image and the watermarked image. To evaluate imperceptible is to conduct subject tests where both original and watermarked image are presented to human subject. The most common evaluation method is to compute the peak signal to noise ratio (PSNR) between the host and watermarked image. PSNR is the measure of the image quality. Generally when PSNR is 40db or greater, then the original and the watermarked images are virtually indistinguishable by human observer. In our proposed watermarking scheme the value of PSNR ranges from 52 to 56 which mean that our algorithm is highly imperceptible. PSNR is defined as follows :

$$\text{PSNR} = 10\log_{10}\frac{255^2}{\text{MSE}} \quad \text{and} \quad \text{MSE} = \frac{1}{n}\sum_{i=1}^{n}\left(I_m(i) - I_w(i)\right)$$

Where I_m and I_w are the original and watermarked image, respectively, n is the number of pixels. Higher the PSNR, the better the image quality.

The table 1 shows the comparison of the PSNR values of the existing and the proposed algorithm over various images. These images are shown in the appendix 2 with their names. The table shows only names of the images.

Table 1: Analysis Values of Existing and Proposed Algorithms

Host Image	Watermark image	PSNR(Existing technique)	PSNR(Proposed Technique)
Gitu.jpg	P2.jpg	44.9157	84.3259
P1.JPG	P2.JPG	44.7694	87.1814
P2.JPG	P1.JPG	44.7203	87.0347
P2.jpg	Gitu.jpg	45.9341	88.3960
P1.jpg	Gitu.jpg	45.9580	88.4787
Gitu.jpg	P1.jpg	44.8594	84.2619

The results shown in the above table can be plotted graphically. The comparison shows that the PSNR of the proposed algorithm is better than the existing algorithm. The increase in the PSNR value confirms the better performance of the proposed algorithm.

The figure 1 shows the original Host image. It is the Gitu.jpg and the watermark image will be hided in this image.

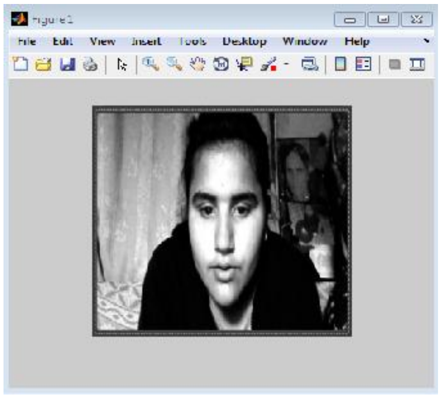


Figure 1: Original Image

The figure 2 shows the watermark image. It is the P1.jpg that will be watermarked in the host image shown in figure 1.

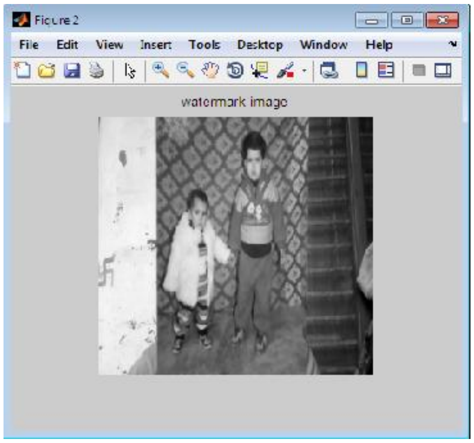


Figure 2: Watermark Image

The figure 3 shows the water marked image. This is the resultant image after inserting the watermark image into the host image. There is no visual difference in this and the host image. This means the proposed technique is effective.

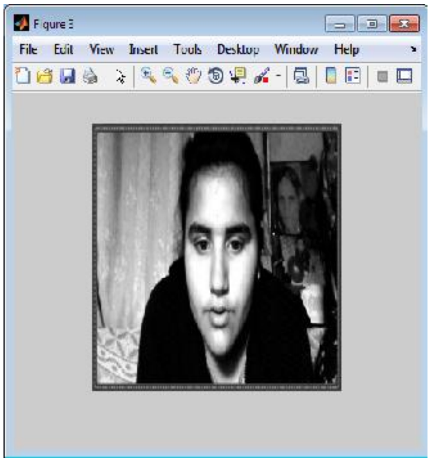


Figure 3: Watermark Extracted From Watermarked Image

The graphical comparison of the PSNR values of the existing and proposed algorithm is shown in the figure 4.

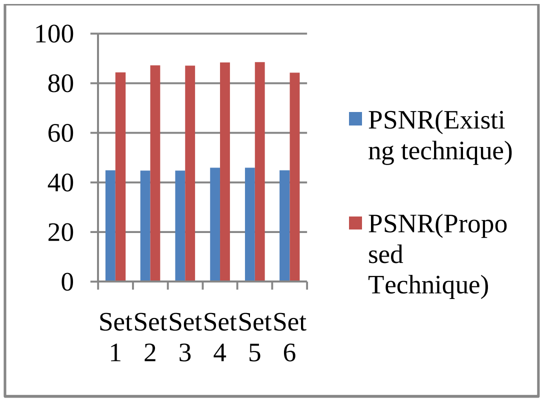


Figure4: PSNR of Existing And Proposed Technique

The results confirm the better performance of the proposed algorithm as compared to the existing algorithm. The proposed algorithm has better PSNR value as compared to the existing algorithm and there is no visual difference between the HOST image and the watermarked image.

V. DIGITAL WTERMARKING : APPLICATIONS

The applications of watermarking are following:

1. Digital copyright protection
2. Transaction tracing and fingerprinting
3. Digital content management
4. Copy control
5. Digital content authentication and verification
6. Broadcasting Synchronization System
7. Forgery Prevention
8. Lyric syn services

VI. CONCLUSION

This research proposes a technique that uses the DWT, DCT as well as the SVD. The Host image is transformed using the DCT then DWT divided in to frequency then the SVD of each frequency block is taken. The watermark image is divided in to sub band using DWT then SVD of each block is taken. The watermark is embedding into host image then inverse SVD, Inverse DWT and inverse DCT results in the watermarked image. The proposed technique uses the DWT, DCT as well as the SVD; this makes the proposed technique better as compared to the existing technique that uses only the DWT and the SVD in a different manner. The simulation of the proposed algorithm is done using the MATLAB. The simulation result shows that the proposed algorithm is better than the existing algorithm. The PSNR values analyzed over different image are better for the proposed algorithm as compared to the existing algorithm. The proposed algorithm is more imperceptible as compared to the existing algorithm.

REFERENCES

[1] Potdar, V. M., Han, S., & Chang, E. (2005, August). A Survey Of Digital Image Watermarking Techniques. In *Industrial Informatics, 2005.INDIN'05. 2005 3rd IEEE International Conference on* (pp. 709-716). IEEE.

[2] Cox, I. J., & Miller, M. L. (1997, June). Review of Watermarking And The Importance Of Perceptual Modeling. In *Electronic Imaging'97* (pp. 92-99). International Society for Optics and Photonics.

[3] Minamoto, T., & Aoki, K. (2010). A Blind Digital Image Watermarking Method Using Interval Wavelet Decomposition. *International Journal of Signal Processing, Image Processing & Pattern Recognition*, *3*(2)..

[4] Cox, I. J., Miller, M. L., Bloom, J. A., &Honsinger, C. (2002). *Digital watermarking* (Vol. 53). San Francisco: Morgan Kaufmann.

[5] Verma, Vishal. Digital Image Watermarking Techniques: A Comparative Study.*International Journal of Advances in Electrical and Electronics Engineering*,IJAEEE ,Volume2, Number 1.

[6]Chaturvedi, Navnidhi. "Various Digital Image Watermarking Techniques And Wavelet Transforms." *International Journal of Emerging Technology and Advanced Engineering* 2.5 (2012): 363-366

HUMANOID ROBOTICS

Nisha Rani1, Neetu Sharma[2]

[1, 2]*Department of Computer Science & Engineering, Ganga Institute Of Technology & Management, Kablana, Jhajjar, Haryana, INDIA*

***Abstract*—This Paper is about *HUMANOID ROBOTICS*. The field of humanoids robotics is widely recognized as the current challenge for robotics research .The humanoid research is an approach to understand and realize the complex real world interactions between a robot, an environment, and a human. The humanoid robotics motivates social interactions such as gesture communication or co-operative tasks in the same context as the physical dynamics. This is essential for three-term interaction, which aims at fusing physical and social interaction at fundamental levels.**

People naturally express themselves through facial gestures and expressions. Our goal is to build a facial gesture human-computer interface from use in robot applications. This system does not require special illumination or facial make-up. By using multiple Kalman filters we accurately predict and robustly track facial features. Since we reliably track the face in real-time we are also able to recognize motion gestures of the. Humanoid Robot technology is one of the fast growing technology is military, health, security, automobiles industries. These robots are playing important role in reducing manual risks and helping doctors to perform risky operations with simple robotic mechanisms. Humanoid Robot is helpful for Human Beings.

I. INTRODUCTION

Humanoid Robotics includes a rich diversity of projects where perception, processing and action are embodied in a recognizably anthropomorphic form in order to emulate some subset of the physical, cognitive and social dimensions of the human body and experience.

Humanoid Robotics is not an attempt to recreate humans. The goal is not, nor should it ever be, to make machines that can be mistaken for or used interchangeably with real human beings. Rather, the goal is to create a new kind of tool, fundamentally different from any we have yet seen because it is designed to work with humans as well as for them.

Humanoids will interact socially with people in typical, everyday environments. We already have robots to do tedious, repetitive labor for specialized environments and tasks. Instead, humanoids will be designed to act safely alongside humans, extending our capabilities in a wide variety of tasks and environments.

At present, Humanoid Robotics is not a well-defined field, but rather an underlying impulse driving collaborative efforts that crosscut many disciplines. Mechanical, electrical and computer engineers, roboticists, computer scientists, artificial intelligence researchers, psychologists, physicists, biologists, cognitive scientists, neurobiologists, philosophers, linguists and artists all contribute and lay claim to the diverse humanoid projects around the world. Inevitably, some projects choose to emphasize the form and mechanical function of the humanoid body.

II. ASIMO: A HUMANOID ROBOT

ASIMO, an acronym for *Advanced Step in Innovative Mobility*, is a humanoid robot designed and developed by Honda. Introduced on 21 October 2000, ASIMO was designed to be a multi-functional mobile assistant.With aspirations of helping those who lack full mobility, ASIMO is frequently used in demonstrations across the world to encourage the study of science and mathematics. At 130 cm (4 ft 3 in) tall and 48 kg (106 lb).

ASIMO was designed to operate in real-world environments, with the ability to walk or run on two feet at speeds of up to 6 kilometers per hour (3.7 mph). In the USA, ASIMO is part of the Innoventions attraction at Disneyland and has been featured in a 15-minute show called "Say 'Hello' to Honda's ASIMO" since June 2005.] The robot has made public appearances around the world, including the Consumer Electronics Show (CES), the Miraikan Museum and Honda Collection Hall in Japan, and the Ars Electronica festival in Austria.

III. STATE-OF-ART

The distinctive feature of full-body humanoids is bipedal locomotion., Walking and running on two legs may seem simple, but humanoid robots still have serious difficulties with it. I see two opposite approaches to bipedal walking. The first-one is based on the zero-moment-point theory (ZMP), introduced by Vukobratovic [1]. The ZMP is defined as the point on the ground about which the sum of the moments of all the active forces Equals zero. If the ZMP is within the convex hull (support polygon) of all contact points between the feet and the ground, a bipedal robot is dynamically stable. The use of the ZMP to judge stability was a major advance over the center-of-mass projection criterion, which describes static stability.

Perception: Humanoid robots must perceive their own state and the state of their environment in order to act successfully. For proprioception, the robots measure the state of their joints using encoders, force sensors, or potentiometers. Important for balance is the estimation of the robot attitude. This is done using accelerometers and gyroscopes. Many humanoid robots also measure ground reaction forces or forces at the hands and fingers. Some humanoid robots are covered with force-sensitive skin. One example for such a robot is CB2 [7], developed at Osaka University.

Although some humanoid robots use super human senses, such as laser range under or ultrasonic distance sensors, the most important modalities for humanoid robots are vision and Audition. Many robots are equipped with two movable cameras.

These cameras are used as active vision system, allowing the robots to focus their attention towards relevant objects in their environment. Movable cameras make depth estimation from disparity more difficult, however. For this reason, fixed calibrated cameras are used for stereo. Most humanoid robots are equipped with onboard computers for image interpretation.

Interpreting real-world image sequences is not a solved problem, though. Hence, many humanoid vision systems work well only in a simplified environment. Frequently, key objects are color coded to make their perception easier.

IV. HUMAN-ROBOT INTERACTION

Many humanoid research projects focus on human-robot interaction.

The general idea here is that the efficient techniques which evolved in our culture for human-human communication allow also for intuitive human-machine communication. This

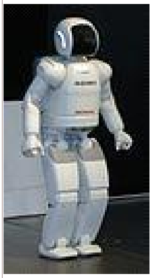
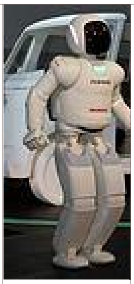
includes multiple modalities like speech, eye gaze, facial expressions, gestures with arms and hands, body language, etc. These modalities are easy to interpret by the human sensory system.Because we practice them since early childhood, face recognition, gesture interpretation, etc. seem to be hard wired in our brains. A smile from a robot does not need much explanation.

Dexterous Manipulation: Another key human capability is dexterous manipulation. The human hand has about thirty degrees of freedom. It is not easy to reproduce its strength, flexibility, and sensitivity. Among the most advanced robotic hands are the Shadow hand, which is driven by 40 air muscles [21] and the four-finger hand developed by DLR and HIT [22]. Dexterous manipulation not only requires capable hands, but also hand-arm coordination and the coordination of two hands and the vision system. Due to the high number of joints involved, controlling grasping and manipulation is challenging.

Three examples for manipulation-oriented humanoid robots are the Robonaut [9], which is using the space tools designed for humans, Justin, for which DLR developed an impedance-based control scheme [23], and Twendy-One, which is equipped with passive impedances in the actuators

V. SPECIFICATIONS

Model	2000, 2001, 2002	2004	2005, 2007	2011	2014
Mass	52 kg	54 kg		48 kg	55 kg
Height	120 cm	130 cm		130 cm	130 cm
Width	45 cm	45 cm		45 cm	
Depth	44 cm	37 cm		34 cm	
Walking speed	1.6 km/hour	2.5 km/ hour	2.7 km/hour 1.6 km/hour (carrying 1 kg)		
Running speed	–	3 km/hour	6 km/hour (straight) 5 km/hour (circling)	9 km/hour (straight)	
Airborne time (Running motion)	–	0.05 seconds	0.08 seconds		
Battery	Nickel metal hydride 38.4 V / 10 Ah/ 7.7 kg 4 hours to fully charge	Lithium ion 51.8 V / 6 kg 3 hours to fully charge			
Continuous operating time	30 minutes	40 mins to 1 hour (walking)		1 hour (running/ walking)	
Degrees of Freedom	26 (head: 2, arm: 5×2, hand: 1×2, leg: 6×2)	34[29] (head: 3, arm: 7×2, hand: 2×2, torso: 1, leg: 6×2)		57[24][30] (head: 3, arm: 7×2, hand: 13×2, torso: 2, leg: 6×2)	57 (head: 3, arm: 7×2, hand: 13×2, torso: 2, leg: 6×2)
Languages				Japanese only	English & Japanese [31]

Images				

VI. HUMANOID ROBOT APPLICATION

Technology Demonstration: Famous humanoid robots like the Honda Asimo [32] or the Toyota Partner Robots [33] do not accomplish any useful work. They are, however, presented to the media and demonstrate their capabilities like walking, running, climbing stairs, playing, musical instruments or conducting orchestras on stage and during exhibitions. Such a showcase of corporate technology attracts public attention and strengthens the brand of the car manufacturers. Hence, the huge development costs of these advanced humanoids might be covered from the marketing budgets

Conducting an orchestra

Space Missions: Another area where money is not much of an issue is missions to space. Since human life support in space is costly and space missions are dangerous, there is a need to complement or replace humans in space by human-like robots. The two prominent projects in this area are the NASA Robonaut [9] and DLR's Justin [23]. Both use a humanoid torso mounted on a wheeled base. The humanoid appearance of the robots is justified, because they can keep using space-certified tools which have been designed for humans and because the humanoid body makes teleoperation by humans easier.

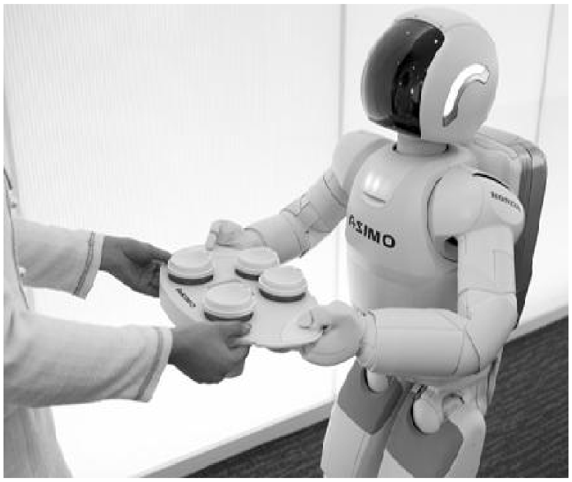
Manufacturing: While in industrial mass production robot arms are used which are not anthropomorphic at all, the Japanese company Yaskawa sees a market for human-like dual-arm robots in manufacturing.It recently announced the Motoman-SDA10 robot [34] which consists of two 7DOF arms on a torso that has an additional rotational joint. Each arm has a payload of 10kg. Yaskawa aims to directly replace humans on production lines. The robot is able to hold a part with one arm while using a tool with the other arm. It can also pass a part from one arm to the other without setting it down. Sales target for the SDA10 is 3000 units/year.

Household: An obvious domain for the use of humanoid robots is the household. Some humanoid projects explicitly address this domain. They include the Armar series of robots developed in Karlsruhe, Twendy-One developed at Waseda University, and the personal robot PR1 developed in Stanford. While these robots demonstrate impressive isolated skills needed in a household nvironment, they are far from autonomous operation in an unmodified household.

VI. NEW TECHNOLOGY IN ASIMO

ASIMO can deliver objects on a tray to a specified destination. By detecting the movement of the person through the eye camera in its head and force sensors on its wrists, ASIMO can move in concert with the person and accurately receive or hand over the tray.

Handing the tray: While carrying the tray, ASIMO uses its entire body to control the tray to prevent spilling of the objects on the tray. Even if the tray slides and is about to fall, ASIMO's wrist sensors detect the weight differences on its hands and automatically stop walking before it drops the tray.



(Handling the tray)

Walking with the tray: When the force sensors on its wrists detect reduction of the load on the wrists as the tray touches the surface of the table, ASIMO sets the tray on the table. By using the entire body to set the tray down, ASIMO can work with tables of different heights.

(Walking with tray)

*Putting the tray on a table:*When the force sensors on its wrists detect reduction of the load on the wrists as the tray touches the surface of the table, ASIMO sets the tray on the table. By using the entire body to set the tray down, ASIMO can work.

With tables of different heights:

Handling a Cart: It can transport heavy loads by handling a wagon in a flexible manner. Being able to handle a cart freely, ASIMO is now capable of carrying heavy objects. ASIMO is capable of handling a cart freely while maintaining an appropriate distance from the cart by adjusting the force of its arms to push a cart using the force sensor on its wrists. Even when the movement of the cart is disturbed, ASIMO can continue maneuvering by taking flexible actions such as slowing down or changing directions. (The maximum load is 10 kg.)

VII. BENEFITS

- Robots offer specific benefits to workers, industries and countries. If introduced correctly, industrial robots can improve the quality of life by freeing workers from dirty, boring, dangerous and heavy labor. it is true that robots can cause unemployment by replacing human workers but robots also create jobs: robot technicians, salesmen, engineers, programmers and supervisors.
- The benefits of robots to industry include improved management control and productivity and consistently high quality products. Industrial robots can work tirelessly night and day on an assembly line without an loss in performance.
- Consequently, they can greatly reduce the costs of manufactured goods. As a result of these industrial benefits, countries that effectively use robots in their industries will have an economic advantage on world market.

VIII. CONCLUSION

Humanoid robot can be used as workers at Exhaustive task. Robots are taking over task which are deemed full, dirty and dangerous. Finally, as the technology improves, there will be new ways to use robots which will bring new hopes and new potential.

Robots are useful in many ways. For instance, it boosts economy because businesses need to be efficient to keep up with the industry competition. Therefore, having robots helps business owners to be competitive, because robots can do jobs better and faster than humans can, e.g. robot can built, assemble a car. Yet robots cannot perform every job; today robots roles include assisting research and industry. Finally, as the technology improves, there will be new ways to use robots which will bring new hopes and new potentials.

REFERENCES

[1] M. Vukobratovic and B. Borovac. Zero-moment point, thirty five years of its life. Int. J. of Humanoid Robotics, 1:157{173, 2004.

[2] T. McGeer. Passive dynamic walking. International Journal of Robotics Research, 9(2):68{82, 1990.

[3] S. Collins, A. Ruina, R. Tedrake, and M. Wisse. E_cient bipedal robots based on passive-dynamic walkers. Science 307, pages 1082{1085, 2005.

[4] R. Playter, M. Buehler, and M.

Raibert. BigDog. In Proc. Of SPIE Unmanned Systems Technology VIII,

2006.[5] http://asimo.honda.com

[6] ASIMO Honda [online]. Available from:http://world.honda.com/HDTV/ASIMO/ Access 11 June 2005.

[7] F. Faber and S. Behnke. Stochastic optimization of bipedal walking using gyro feedback and phase resetting. In Proc. of 7th IEEE-RAS Int. Conf. on Humanoid Robots, 2007.

IN OIL AND GAS
REFINERIES THE APPLICATION OF ROBOTICS

Om Prakash Azad [1]

[1] *Department of Mechanical Engineering, Ganga Institute of Technology and Management, Kablana, Jhajjar, Haryana, INDIA*

Abstract: Oil and gas from conventional and non-conventional resources will become more and more challenging. The oil and gas industry will continue to boom in the coming future. Obtaining This intensifying need will impose very considerable demands on work force, financial and technology capabilities. Since the future supplies of oil and gas are to expand, advanced technology will become increasingly necessary to obtain access to more challenging conventional and non-conventional resources. Therefore oil and gas technologies will be very costly to operate in the coming future due to hostile, hard-to-reach environments. The offshore oil industry will become a complicated many of advanced equipment, structures, and work force. The present work identify potential applications and research directions of robotics in the oil & gas field and explore the obstacles and challenges of robotics applications to this area. This research performs the necessary survey and investigation about the work conditions of robotics and its equipment in the oil and gas industry, especially offshore oil rigs. The oil & gas industry processes are first investigated. The personals and tasks are then explored. Furthermore, this paper reviews the current robotics technology applied to various oil and gas industries. The challenges and requirements are identified for robotics in the oil and gas industry. The requirements of robotics and automation in the oil & gas industry are presented.

I. INTRODUCTION

The oil and gas demand will grow rapidly in the next two decades. The oil and gas industry will continue to boom in the coming years. The intensifying need to obtain oil and gas from more hostile, hard-to-reach environments will increase the operation cost rapidly in the coming future. Hence, the oil and gas industry keeps looking for lower-cost solutions. To be competitive and to improve their profit margins, oil & gas companies are committed to cost reduction. They also look for ways to minimize employee costs and improve manufacturing efficiencies and quality besides seeking lower-cost suppliers and less-expensive raw materials. Because of the rising cost of employee salary and benefits like health care, the cost reduction effort in oil & gas companies is offset. Also high employee turnover adds the costs of retraining. Therefore, the oil and gas companies are looking for new technologies to reduce the labour cost. Also safety is a big concern in the oil and gas production. Using robotics in inspection, maintenance and repair could greatly improve the safety and efficiency. The oil & gas industry's presence is evident in its global networks of market supply and demand relationships. When there are fluctuations, regardless of their origins, consumers are affected in all over the world. Prices respond to changing markets with upward volatility because of an inelastic demand for oil and petroleum products. One solution to both the need for efficiency and maximum production and the capabilities required to further exploration is to implement robotics and automation in offshore oil & gas environments. Because the offshore oil & gas processes require advanced technologies, offshore environments will deploy the safest, most secure and consistent operations by utilizing industrial robotics and automation, and the latest software and mechanical devices. In order to investigate the challenges of robotics and automation in oil and gas industry, the necessary survey and investigation about the oil & gas industry processes, the personals and tasks should be explored first. The work conditions must be discussed to explore the requirements of robotics and automation equipment in the oil and gas industry, especially on offshore rigs. To meet the requirements and develop robotics and automation equipment in such work conditions, this paper reviews the current technology that has been developed and discusses the future research opportunities in the oil and gas industry.

II. INDUSTRIAL PROCESSES IN OIL AND GAS INDUSTRIES

Robot for painting is one of the earliest applications for industrial robot, however, the precision and finishing for the painting is an important issue for any painting job. Two software packages were used in this project. The Computer Aided Design (CAD) of the system work-objects and end effector was programmed based on Solid works software. Robot studio Software used to program the paths and target of the alphabets to be painted by the IRB1400 Robot which generate a RAPID GUI code used for robot interfacing. The final results demonstrate that implementation such system helps to boost the quality of painting, reduce paint consumption and improve safety. The result was able to boost the quality of painting, safety was improved with the usage of all the painting materials, and the cost of painting was reduced by using less paint. The integration of all the components of a typical robot was the driving factor in achieving the project objective. The offshore oil & gas industry is a complicated several of advanced equipment, structures, and work force. With a proper knowledge of offshore oil and gas rig environments, the applications of industrial robotics and automation are less abstract. Before any real vision of the potential roles robotics and automation in offshore oil processes can emerge, those processes must be enumerated appropriately. There are many products and services related to oil and gas with an equally substantial potential for markets within the industry. There are three stages through which petroleum products pass: upstream, downstream and midstream models. The upstream oil sector commonly refers to the searching for, recovery and production of crude oil and natural gas. It is also known as the exploration and production (E & P) sector, including searching for potential oil and gas fields, drilling of exploratory wells, and subsequently operating the wells to recover and bring the crude oil and/or natural gas to the surface.

The midstream oil and gas sector is the relay point for the upstream sector's products.

Midstream processes commonly refer to processing, transport, and storage of these products.

Because it is possible to produce pipeline quality gas for direct sale to an interstate or intrastate natural gas pipeline in the midstream sector, some treatment or processing of natural gas may occur in the midstream sector and bypass the downstream oil and gas sector completely. The midstream typically links the supply of the oil industry to the demand for energy commodities. The downstream oil sector refers to the refining of crude oil and the selling and distribution of natural gas, as well as other products derived from crude oil such as liquefied petroleum gas (LPG), gasoline or petrol, jet fuel, diesel oil, other fuel oils, asphalt and petroleum coke. The downstream industry touches consumers through thousands of products. These products include petrol, diesel, jet fuel, heating oil, natural gas and propane to asphalt, lubricants, synthetic rubber, plastics, fertilizers, antifreeze, pesticides, and pharmaceuticals. The oil and gas processes and the three sector model they fall into tend to parallel acrossthe onshore and offshore industries, however the processes will be distinguished when necessary if a distinct observation is being made.The major oil and gas extraction processes include the materials and equipment used and the processes employed.

There are four major processes in the oil and gas extraction industry:

(1) Exploration,

(2) Well development

(3) Production

(4) Site abandonment

After these processes are completed, the production process enters. It is likely the process in

which robotics and automation have the largest potential to increase efficiency and create a safer

environment for offshore oil and gas rigs, all while cutting construction costs for human necessitated rig designs. After the Deep Water Horizon oil spill in 2010, the Bureau of Ocean Energy Management, Regulation and Enforcement (BOEMRE) has implemented new mandatory regulations to replace old protocols for the offshore oil & gas industry. This is one area of operation that robotics and automation can dramatically improve efficiency, precision, safety, and decrease costs to companies. It is no stretch of imagination to suggest that robots and automation will soon be the primary means to effectively satisfy many of these new regulations.

Oil and Gas Refineries Challenges

The deep waters of the Gulf of Mexico, the frigid regions of Russia, and the hot, dusty, undeveloped deserts of the Middle East are merely the geographic challenges facing today’s oil and gas exploration and production industry. The work conditions on offshore installations are the first thing to look at when analyzing the environments.

The most important ones are as follows:

- Atmosphere: The atmospheric conditions on offshore platforms are quite unfriendly. Due to the substances used and generated during the processing of hydro carbon resources, the following three types of gases can occur separately and combined: explosive, toxic and corrosive.
- Heavy weather: Wind with high speed and squalls, rain, hail and snow. All these weather conditions occur more often and more intense offshore than onshore.
- Extreme ambient temperature: Depending on the region the platform is located there can be extreme high and low temperatures. Humidity is also ranging from lower values up to condensing.
- Constraint space and/or walkways: The width of typical walkways is about 0.7 - 0.75 m.

Offshore rigs have further logistical issues: (a) it is highly expensive to have people working on the rig as they must be housed and protected; (b) in the case of emergency, it must be possible to evacuate personnel quickly.

As oil and gas exploration pushes into more hostile and remote regions, these difficulties become serious obstacles to the financial viability of an offshore installation. Reason for such hesitation derives from the logistical challenges that come with the implementation of a robot or an automated system in an offshore environment, as well as from a general lack of prototypes on the market. The oil and gas industry has grown accustomed to the use of systems controlled remotely by expert operators. But now projects that are underfoot could turn remotely operated vessels (ROVs) into highly specialized robotic systems. The industry is now to decide whether the use of robotics in subsea environments is inevitable and, if so, how much it will cost. Robots have clear advantages in some applications and safety is often a big factor in favouring their use in hazardous environments. There are so many tasks robots could do easily, far beyond inspection and maintenance. Now the challenge is to get oil and gas companies to use robots.

III. ROBOTICS USEFUL FOR OIL AND GAS INDUSTRIES

Robotics is a leading supplier of industrial robots - also providing robot software, peripheral equipment, modular manufacturing cells and service for tasks such as welding, handling, assembly, painting and finishing, picking, packing, palletizing and machine tending. Key markets include automotive, plastics, metal fabrication, foundry, electronics, machine tools, pharmaceutical and food and beverage industries. A strong solutions focus helps manufacturers improve productivity, product quality and worker safety. ABB has installed more than 200,000 robots worldwide. At the end of the 1980s, ABB and, later, Robot Norge invested in this wave and almost became the sole supplier to the Norwegian automotive parts manufacturing industry. Several hundred ABB robots were supplied to companies such as Farsund Automotive Casting, Hydro Structure Aluminium, Fundo Aluminium, Steertech, Raufoss Technology, Plastal, KA Automotive, Fibo and several others.

New Sources of Offshore Environmental Data

As oil and gas companies face increasing operational demands and technical complexities, access to new sources of offshore environmental data will be increasingly important. Traditional offshore environmental data acquisition methods (e.g. support ships, satellites and ROVs) for monitoring and surveying provide a valuable service. However, they are limited in range and mission duration and are expensive to use and maintain. Implementing innovative remote monitoring and survey technologies at lower acquisition costs and with greater operational efficiencies provides a significant business advantage. Liquid Robotics Oil & Gas brings this advantage through the delivery of continuous real time measurement solutions for applications including seep and containment loss detection, meteorology/oceanography (METOC), and subsea communications, in a highly cost effective manner. Delivered securely and on-demand, these services help customers meet the increasing demands that come from operating in ever more challenging environments.

IV. COMPONENTS OF A ROBOT

1 End Effector

End effector is the device at the end of a robot manipulator; it is designed to interact with the environment. This too l is used to perform the programmed application based on the required task.

For example a spray gun of a painting tool is used as the end effector for the painting robot.

Similarly, a design has to be developed for the robot end effector for the application of oil refineries according to their task. Every end effector has its specific design and dimensions. It requires the power input from external source that also has to be identified and make available for the operation.

2 Actuators

Actuators are like the muscle of the manipulator. They are controlled using the robot controller. They convert stored energy into movement [9]. The robot controller actuator uses air compressor when operational. A directional control valve was used in the direction of air fluid. The directional control valve have a fast response time of 12ms or less at a pressure of 0.5MPa without light/surge voltage suppressor and 15ms or less at a pressure of 0.5MPa with light/surge voltage suppressor. It has to response as fast as the movement of the robot set by the programming.

3 Sensor, Controller, Processor, Software and Object

Sensors are used to collect information about the internal state of the robot or to communicate with the outside environment. Sensors integrated into the robot send information about each joint or link to the controller, which determines the configuration of the robot. The integrated signal supply of the IRB1410 Robot is 12 single on upper arm with an integrated air supply of maximum 8bar on upper arm. For example of a robot painting, 24VDC relays is used as the sensor, to send signal to the directional control valve indicating when to activate the air compressor. This signal is usually sent to omron relay from the input/output signal controller of the robot. The controller of the robot controls the motion. It receives its data from the computer; control the motion of the actuators, and coordinates of the motion with the sensory feedback information. The IRC5 controller is used to control the IRB1410 ABB Robot and Virtual Flex Pendant is used to control the IRC5 controller. They are both connected by a cable. The processor is the brain of the robot. It calculates the motions of the robot joints, determines how much and how fast each joint must move to achieve the desired location and speeds, and oversees the coordinated actions of the controller and the sensors. The processor is a computer, which works like other computers, but is dedicated to a single process. It requires an operating system, programs, monitors, and have capability of a computer processor. The leFx Pendant is used as the controller for the IRB1410 ABB Robot. It works as the operating device for the robot. All application task and they program are being uploaded into the flex pendant. Base Ware Operating System is the processor operating system of IRC5 controller of the 1RB1410 ABB Robot. The Base Ware OS controls every aspect of the Robot, like motion control, development and execution of application programs communications [15]. There are three groups of software used in the robot. Base Ware OS is the operating system of the robot, Robot studio programming is used in programming the robot task and Solid work is used in Computer Aided Design (CAD) of the programming tools.

4 Software Developments

The most important aspect of any project is choosing the right end effector for the particular application. The manipulator is programmed based on the functionality of the end effector.

Depending on the end effector, the application process can be determined and therefore programmed. The end effector, and the work object (Board) is designed using the Solidwork software, and then imported to Robot studio as a CAD file for the programming of the paths and targets. Sometimes the program has to done using the backup system of the Robot. Afterwards, the digital output configuration of the air compressor was created using the Rapid Editor. This is to determine when the air compressor should be on/off. Finally, a backup system of the program is created and saved in a flash drive. The backup program is uploaded into the FlexPendant of the designed Robot connected to the specified controller. When the instruction is given to the Controller, it sends the information to the manipulation to perform the path and target being instructed. The air compressor comes on only when an ON signal is given by the Controller digital output signal to the directional control valve, which then controls the flow of air to actuate the end effector. The end effector goes off when OFF signal is given through the Controller digital output signal. When all the paths and targets of the program is completed, the robot goes back to its home position. The same procedure takes place when that designed Robot is taught using the FlexPendant on how to follow its paths and targets. In this case, no program needs to be uploaded into the system. The FlexPendant generate its program according to how the Robot is taught.

5 Hardware developments

The hardware design covers the Mechanical and Solid work design of the end effector and its attachment holder and the Work object to the Robot.

6 Robot Interfacing

Interfacing with the robot is the most important aspect of any project and as such is said to be most complicated aspect. Monitoring the movement and functionality of the robot and its joint, considering the entire safety factor and ensuring all procedure is met, understanding the use of the

Flex Pendant and how it works with the particular Controller. The end effector is mounted on the

Robot during interfacing process and the Tool Center Point (TCP) test was performed.

7 Manipulator

This is the main body of the robot; it consists of the links, the joints, and other structural elements. The weight of the robot is roughly 225kg. The robot is equipped with an operating system Base Ware OS. The Base Ware OS control every aspect of the robot, such as motion control, development and execution of application programs communications. The Robot can also be equipped with optional software for application support.

V. CONCLUSION

In this research, a brief introduction to the oil & gas industry processes is performed. The challenges and requirements for the robotics are explored. Future research opportunities including robot manipulator, mobile platform, tele-operation, and subsea robotics are discussed. Overall, one can assume that there are many opportunities in the oil and gas industry and some research is currently in progress to develop robotic and automation applications. Therefore, it is an optimal time to develop robotic and automation systems that can satisfy the oil & gas requirements. These examples represent high-risk operations for humans and therefore provide opportunities to improve health, safety and environmental performance. In addition to productivity and efficiency gains, robots used for high-risk tasks will also lead to improvements in health, safety and environmental performance. Such tasks are not necessarily always predictable and represent unusual robot activities. The robot will therefore require features that extend the "eyes, ears, and hands" of the human decision makers as they carry out inspections and maintenance operations on the process infrastructure. Reduced commissioning and operation costs, together with improved Environmental, Health and Safety (EHS) are some of the potential benefits of having normally unmanned topside oil platforms. However, such oil & gas platforms require advanced methods and tools for remote control and monitoring of inspection and maintenance operations.

REFERENCES

[1] ABB Robotics (2011). Basic Robot Programming Training IRC5, Malaysia.
[2] World Nuclear Association (2012) Uranium, Electricity and Climate Change.
    a. Upstream (Petroleum Industry). (2014).
[3] Upstream Oil and Gas. (2014). http://www.upstreamoilandgas.com/.
[4] GE Energy. (2011). http://www.ge-energy.com/solutions/index.jsp#tabs-industries.
[5] US Environmental Protection Agency (2000) US EPA Office of Compliance Sector
    a. Notebook Project: Profile of the Oil and Gas Extraction Industry, US Environmental
    b. Protection Agency, Washington DC.
[6] Meeting the Challenges of Today's Oil and Gas Exploration and Production Industry.
    a. http://www-935.ibm.com/services/us/gbs/bus/pdf/g510-3882-meeting-challenges-oil-gasexploration. pdf.
[7] Niku, S. B. (2008). Introduction to Robotics: Analysis, Systems, Applications. Prentice.
[8] [10] Esposito, A. (2004). Fluid Power with Applications. Prentice Hall 7th Edition.
[9] Haugan, K.M. (1974). Spray Painting Robots: Advanced paint shop automation. Industrial Robot: An International Journal, 270 - 272.
[10] Hertling, P., Hog L., Larsen R., Perram J.W.& Petersen, H.G. (1996). Task Curve Planning for Painting Robots, Part I: Process Modeling and Calibration. IEEE Transactions on Robotics and Automation.
[11] ABB Robotics (2004). IRC5 with FlexPendant Manual.
[12] Gary, J.H. and Handwerk, G.E. (1984) Petroleum Refining Technology and Economics. 2nd Edition, Marcel Dekker, Inc., New York.
[13] Ijeoma W. Muzan1 ET AL., "Implementation of Industrial Robot for Painting Applications", International Symposium on Robotics and Intelligent Sensors 2012 (IRIS 2012), Procedia Engineering 41 (2012) 1329 – 1335.

INFRASTRUCTURE FINANCE

Sheela Malik[1], Amit Singhal[2], Lokesh Yadav[3]

[1,2,3]*Department of Civil Engineering , Ganga Institute of Technology and Management, Kablana,Jhajjar, Haryana, INDIA*

Abstract : **There is huge demand for continuing investments in all the areas of civil engineering. This includes infrastructural development (real estate, residential complexes), transportation (railways, airports, docks and harbors), Power Generation and transmission. The Key issue is the while the need of the project exists, how these projects financed. This paper will basically focus the characteristics of infrastructure finance, identifying new sources of risk capital with the existing types of risk capitals and reducing the amount of required risk capital.**

Keywards: Role of Banks, Characteristics of Infrastructure Finance, Risk Capital Required.

I. INTRODUCTION

There is a need for large and continuing amounts of investment1 in almost all areas of infrastructure in India. This includes transportation (roads, ports, railways, and airports), energy (generation and transmission), communications (cable, television, fiber, mobile and satellite) and agriculture (irrigation, processing and warehousing). The key issue is, while the need exists, how these projects will get financed. In the past the government has been the sole financier of these projects and has often taken responsibility for implementation, operations and maintenance as well. There is a gradual recognition that this may not be best way to execute/finance these projects. This recognition is based on considerations such as:-

A. Cost Efficiency

Privately implemented and managed projects are likely to have a better record of delivering services of a higher quality. The India Infrastructure Report (2008) estimates that the Indian economy's growth rate would have been higher by about 2.5% if the delays and cost overruns in public sector projects had been managed efficiently. The report goes on to state that the predominant cause for such delays / overruns was not under-funding of the projects, but arose, "on account of clearances, land acquisition problems, besides factors internal to the entity implementing the project".

B. Equity Considerations

Since it is hard to argue that every infrastructure project uniformly benefits the entire population of the country, it may be more appropriate to impose user charges which recover the cost of providing these services directly from the user rather than from the country as a whole (the latter is the effect if the government builds the project from its own pool of resources). If users are to be charged a fair price then the project acquires a purely commercial character with the government then needing to play the role only of a facilitator.

C. Allocational Efficiency

Since users are likely to pay for services that they need the most, private participation and risk-return management has the added benefit that scarce resources are automatically directed towards those areas where the need is the greatest.

D. Fiscal Prudence

Both at the centre and state levels, for a variety of reasons, there is a growing concern that the absolute and relative (to GDP and GSDP respectively) levels of fiscal deficit are high and that incurring higher levels of deficit to finance infrastructure projects is infeasible.

II. CHARACTERISTICS OF INFRASTRUCTURE FINANCE

Infrastructure projects differ in some very significant ways from manufacturing projects and expansion and modernisation projects undertaken by companies.

A. Longer Maturity

Infrastructure finance tends to have maturities between 5 years to 40 years. This reflects both the length of the construction period and the life of the underlying asset that is created. A hydro-electric power project for example may take as long as 5 years to construct but once constructed could have a life of as long as 100 years, or longer.

B. Larger Amounts

While there could be several exceptions to this rule, a meaningful sized infrastructure project could cost a great deal of money. For example a kilometre of road or a mega-watt of power could cost as much as US$ 1.0 million and consequently amounts of US$ 200.0 to US$ 250.0 million (Rs.9.00 billion to Rs.12.00 billion) could be required per project.

C. Higher Risk

Since large amounts are typically invested for long periods of time it is not surprising that the underlying risks are also quite high. The risks arise from a variety of factors including demand uncertainty,14 environmental surprises, technological obsolescence (in some industries such as telecommunications) and very importantly, political and policy related uncertainties.

D. Fixed and Low (but positive) Real Returns

Given the importance of these investments and the cascading effect higher pricing here could have on the rest of the economy, annual returns here are often near zero in real terms. However, once again as in the case of demand, while real returns could be near zero they are unlikely to be negative for extended periods of time. Returns here need to be measured in real terms because often the revenue terms of the project are a function of the underlying rate of inflation.

III. TYPES OF RISK CAPITAL REQUIRED

There are two types of risk capital that are deployed in any project:

A. Explicit Capital

This is typically the equity that a developer or a sponsor commits to the project. Here while the downside is unlimited if the project does well, there is no limit on the upside either. The sponsor seeks to conserve his capital and maximise the returns on it by deploying unique and project specific skills and by managing the underlying risks associated with the project. Given a limited supply of capital, the promoter also tends to concentrate his energies and capital in a small number of relatively lumpy investments so that he does not spread himself and his resources too thinly. In a typical infrastructure project, the developer puts together a consortium of capital providers who not only commit capital to the overall project but also assume complete operational and financial responsibility for specific risks thus, lowering the capital requirements from the developer.

B. *Implicit Capital*

This is typically the risk capital that is committed by a lender to the project. Loans have the characteristic that while the downside is unlimited the upside is limited to the rate of interest charged on the loan. Secondly, the loans typically involve much larger amounts of money relative to the equity investments. Given the fact that a typical lender raises money from retail deposits he needs to hold a reasonably high amount of capital to assure his depositors that irrespective of the fate of the project, he will be able to meet his obligations. Assuming that the desired rating aspiration for the lender is AAA an unsecured loan to a typical ten year infrastructure project) could require as much as 25% tier 1 capital to be committed to it. Since the capital is required to cover the lender against all the uncertainties surrounding a specific project, the lender seeks to reduce the amount of capital deployed by diversifying across projects and by ensuring that to the extent possible, the explicit capital is sufficient to cover the risks beyond the worst-case scenarios. The lender seeks to be compensated for this capital through the rate of interest charged on the project loan.18 Given the relatively large amounts of funds required for each project and the comparatively smaller number of such providers, lenders in the past have typically not had the opportunity to sufficiently diversify their risks19 nor have they had a sufficient amount of tier 1 capital. Not unexpectedly, having held significantly less than the required amount of implicit capital, they have very quickly found themselves undercapitalised relative to the level of credit rating that they had committed to their depositors and in some cases have even defaulted to them. The risk capital required for infrastructure projects is the most scarce and, therefore, very expensive resource. Given the risks, amounts and maturities involved, required rates of return on such capital could well be excess of 25% to 30%per annum even in today’s low interest rate environment. Given the large amounts of risk capital that could potentially be required this would have a significant impact on the cost of the eventual service that is sought to be provided. In the past, the sources that have been tapped for this capital have included professional developers, manufacturers of equipment, contractors, domestic and international equity investors and in several cases the government itself. The whole question of ‘Sources of Infrastructure Finance’ then becomes a much narrower question of ‘Sources of Risk Capital for Infrastructure Finance’ in the first instance and then secondarily a question of the manner in which these funds may be intermediated from the providers to the borrowers.

This paper attempts to address these issues along four dimensions:

a) Reducing the amount of capital required by each project;

b) Increasing the supply of this capital;

c) Facilitating the flow of funds to this sector, and

d) Enhancing the role of banks as intermediaries.

IV. REDUCING THE AMOUNT OF REQUIRED RISK CAPITAL

As a first step, before looking for new sources of this risk capital, given its extreme scarcity and very high cost, every attempt needs to be made to limit the amount of capital that is required by ensuring the following:

A. *Removal of the Effect of Controllable Uncertainties*

All controllable uncertainties (such as those imposed by unexpected changes in policy, tax rates and political considerations) are either eliminated or the government directly takes the financial responsibility for them22 in a timely23 manner. This has the effect of imposing a general tax on the entire country for these uncertainties and taking it away from individual projects. This is, of course, relatively easy to articulate but much harder to implement in a democratic polity where governments and their political compulsions change frequently but the importance of a stable, even if imperfect, policy environment cannot be overemphasized. Ease in contract administration and adherence to these contracts by all entities including state entities is a good example of a controllable uncertainty that has the potential24 to reduce the quantum of total capital required.

B. *National Diversification Benefit*

Even though a developer may be implementing only a small project in a small command area, if the desire is to ensure that the cost of the service provided by it is benchmarked at a national level and does not vary a great deal from region to region, the benefit of national or state level diversification could be made available to each project.25 From a lender’s point of view, it should be possible to diversify away as many components of the risk as possible through the use of credit and equity derivatives. Credit derivatives and other related contracts have the effect of allowing the reduction of capital consumption through diversification without necessarily having to incur the costs of buying or selling the underlying credit exposure.

C. *Global Diversification Benefit*

Several infrastructure projects involve exposure to global risks such as rainfall, temperature and fuel and other commodity prices. Permitting lender to access these markets directly or through brokers will allow them to reduce their exposure to many of these risks, thus once again, reducing their consumption of implicit capital.

V. NEW SOURCES OF RISK CAPITAL

In terms of new sources of capital, in addition to convincing the existing set of capital providers to commit more capital by creating an enabling policy environment, the following ideas could be explored:

A. *First Loss Default Guarantee Funds (FLDGs) created by the Government*

This is a very important idea, particularly in a situation where the overall supply of funds is adequate but there is a constraint in the supply of total risk capital and the government is seeking to operate within its fiscal limits. As a concept it requires governments to (a) stop spending the money required for projects; (b) focus on eliminating the effects of uncertainties caused by it and (c) to the extent that uncertainties remain, provide risk capital in a manner that preserves the incentives of all the other players to act in a consistent manner. FLDGs seek to provide non-event specific partial credit guarantees to lenders (unlike the partial credit guarantee being explored by World Bank - refer earlier footnote), are limited to only a part of the loan (say 25.0%) and operates on a first loss basis (i.e., in case of 25.0% FLDG the first 25.0% of the loss would be absorbed by the Fund). This manner of providing capital is in many ways superior to recapitalising existing intermediaries or creating new ones with Government capital.

- The corpus which supports the FLDGF may be invested in interest bearing government securities so that the corpus continues to grow and there is no net impact on the government deficit (i.e. is cash neutral).

- Unlike in the case of recapitalisation where the government capital becomes the primary or the sole risk capital being deployed, in the case of FLDGs even if they are administered mechanically, the government capital is secondary capital. The primary capital being deployed is the implicit capital supporting the balance 75.0% of the loan. The FLDG has the effect of reducing the total quantum of the implicit capital that is needed but not to zero. The belief is that in seeking to maximise the return even on a lower amount of implicit capital the lender would be equally diligent. And, it may also bring in smaller and more specialised providers of implicit capital and loan funds.

- FLDG concept draws its value from the diversification benefits inherent in a larger number of projects. FLDG pool makes this diversification benefit available to the lenders by reducing the project risk borne by them. In the US markets, monolithic insurance companies like the MBIA29 provide such credit supports for urban local bodies and other borrowers.

B. Securitisation

A large project loan could then be broken up into several smaller pieces which could then be bought by insurance companies, individuals, banks, pension funds, etc. each of whom would have other diversified investments. This would typically be done in conjunction with a FLDG of the sort described earlier so that the securitised instrument acquires an investment grade character and can be subscribed to even by highly (credit) risk-averse lenders. In addition, if well established, active trading of such paper has the effect of establishing a pricing benchmark for such project risk and if packaged along with other securities, could even produce a very high quality paper.30 However, for this to happen at a large scale a great deal of facilitative legislation and incentive structures would have to be built.

Facilitating the Flow of Funds.

1). Redefine NDTL to include only cash or cash-like instruments: Currently Net Demand and Time Liabilities (NDTL) are defined to include almost all the liabilities of a bank. The definition is important because under the Banking Regulation Act, SLR and CRR are defined with reference to NDTL. SLR and CRR obligations impose a financial cost on the bank but are important37 where a bank is performing a maturity transformation role. However, where a bank is mobilising fixed maturity deposits or bonds, particularly where the original maturities are greater than one year, it is not clear why CRR and SLR would be required to be maintained. One of the rationales for the continuance of specialised DFIs for infrastructure finance has been they are able to issue long-term bonds at low spreads over the G-Sec rate and do not have to maintain CRR and SLR on them. This is an anomaly which can easily be addressed within the Banking Regulation Act so that banks will be able to issue long maturity bonds (including 25 year Deep Discount Bonds) at identical rates.

2). Strongly Encourage the use of Derivatives: Typically, equity, commodity, forex and interest rate derivatives form the primary products in the derivative markets while the insurance companies, banks, hedge funds and large corporate are the larger participants. Derivatives markets are important for the risk transformation roles they play. In the Indian context, these markets are underdeveloped due to a large number of regulatory issues. Currently credit derivatives are not permitted in the Indian markets while the banks are not permitted to trade in equity and commodity derivatives. Further, the market for interest rates derivatives is very thin because there are strict restrictions on the participation of banks in the exchange traded derivatives. While Over-the-Counter (OTC) derivatives may be traded by the banks, the large public sector banks are largely absent from the market. Insurance companies, the other natural counter-parties, have not yet received permission from the Insurance Regulatory and Development Authority (IRDA). Through the use of such derivatives it will be possible for participants to design products which are capital efficient and are tailored to the requirements of infrastructure finance. For example, floating nominal rates give more fixed real rates of interest than do fixed nominal rates of interest. Given the preference for fixed nominal rates on the part of the long-term retail investor, derivative markets provide the only bridge between them.

3). Free up the allocation of funds from Insurance Companies and Provident Funds: This is a much harder challenge and before this is done the following questions would have to be clearly answered:

- In the absence of these funds, will there be a decline in the availability of funds

for the central/ state governments.

- Currently insurance companies and provident funds hold no capital against credit risk and interest rate risk but nevertheless have to deliver promised returns to their investors in a default free manner. Nor presumably do they have the expertise to manage these risks. This could be one possible reason why these entities may have been allowed to lend to DFIs but not directly to the underlying borrowers. Where will this capital come from and how will these competencies be built.

1). Eliminate the distinction between an advance and an investment: Given the importance of instruments such as commercial paper and bonds in providing finance to companies and the ease with which borrowers move between one form of financing and another, there is a strong case that this distinction should no longer be made even in the balance sheets of banks. Even though both sets of instruments increase the level of credit risk borne by the bank in an identical manner, considerations such as credit / deposit ratio, priority sector requirements and a strong regulatory preference for “Advances” over “Investments” create a distorted set of preferences.

2). Require detailed product and client segment level profitability, NPA, provisioning and consumption of capital to be reported: This is important because otherwise income streams and growth from a few segments mask the underperformance of the bank in other segments.44 This reduces incentives to build specialisation in each area of business that the bank is engaged in and creates the potential for future catastrophes once the positive returns from the few sectors disappears. This reporting will ensure that right from the beginning the banks are engaged in infrastructure finance in a disciplined manner.

3). De-emphasise the role of the Non Performing Asset Ratio as an Independent Performance Measure: In its evaluation of banks, despite the fact that strong provisioning guidelines and capital adequacy rules have been imposed, in its recent guidelines, the RBI has started to emphasise the NPA Ratio as a standalone performance measure. This is both inconsistent and counter-productive. If provisioning has been done properly45 then the Non Performing Asset is actually the “good” part of the loan (the “bad” part has already been provisioned away) and more importantly if the lender has engaged in high-risk, high-return businesses (such as infrastructure finance), he is likely to have a higher proportion of assets which are not performing relatively to a lender that has only engaged in low-risk businesses. The question to ask would be, are the risk-return models in balance, i.e., what is the return on equity after an appropriate level of provision has been taken and what is the capital adequacy. This independent emphasis on the NPA ratio is sending a strong signal to banks that they need to move away from businesses such as infrastructure finance.

4). Directed Credit: If banks behave as risk-neutral intermediaries, in order to get them to participate in any sector the only requirement would be to ensure that the risks and the returns of the sector are in balance. However, if the concern is that banks are behaving in a risk-averse manner and there is a belief that the positive externality of a rupee of investment in infrastructure exceeds that of a similar rupee in any other sector, it would be very useful to explore the inclusion of infrastructure as a component of the priority sector. However, this should be done while also ensuring that banks are able to meet these requirements by purchasing suitable instruments in the market and not only through originating every asset themselves. RBI has taken a step in this direction with the recent circular dated July 20, 2004 with respect to “Investment by banks in Mortgage Backed Securities - Lending to Priority Sector under Housing Loans”

VI. CONCLUSION

Infrastructure growth is a critical necessity to meet the growth requirements of the country. Government led infrastructure financing and execution cannot meet these needs in an optimal manner and there is a need to engage more investors for meeting these needs. Even though the Indian financial system has adequate liquidity, the risk aver-sion of Indian retail investors, the relatively small capitalisation (compared to the large quantum and long duration funding needs of infrastructure finance) of various financial intermediaries requires adoption of innovative financial structures and revisiting some of the regulations governing the Indian financial system. The risk capital required in the infrastructure sector can be understood as the Explicit Capital brought in as equity by the project sponsors and the Implicit Risk Capital provided by the project lenders. Implicit Capital providers seek to manage their risk-return reward by ensuring availability of adequate Explicit Capital and diversification across various projects. Given this profile of the Explicit Capital, greater flow of this risk capital can be ensured by removing the effects of controllable uncertainties in the policy environment and making available the benefits of diversification through alternate mechanisms. New sources of this risk capital can be sourced by providing partial risk guarantees (in form of First Loss Deficiency Guarantees), formation of highly capitalized financial intermediaries and encouraging securitization transactions. In addition to above, various regulatory initiatives and market reforms are required to enable the commercial banking system to participate more vigorously in providing infrastructure financing.

REFERENCES

[1] Gray, Philip, and Timothy Irwin; “Exchange Rate Risk: Reviewing the Record for Private Infrastructure Contracts”, Viewpoint, World Bank, Private Sector and Infrastructure Network, Washington, D.C., June 2003.
[2] Hess Ulrich, Kaspar Richter, Andrea Stoppa (2000); “Weather Risk Management for Agriculture and Agri-Business in Developing Countries”, 2000
[3] Malhotra, Sandeep and Kamal Nigam (2003); “Infrastructure Finance in India”, ICICI research centre. org and CAFS Working Paper, July 2003
[4] Mohan, Rakesh “Infrastructure Development in India: Emerging Challenges”, Working Paper presented at the World Bank Annual Conference on Development Economics, Bangalore, May 2003
[5] Morris, Sebastian (2003); “Efficacy of Government Expenditures”, India Infrastructure Report, 2003
[6] “India Infrastructure Report”, 2003
[7] Williams, Julie L. (2003); “Regulatory Considerations In the Evolution of Risk Management”, Speech by the 1st Senior Deputy Comptroller of the Currency and Chief Counsel Office of the Comptroller of the Currency, at Risk USA 2003 Conference, Boston, Massachusetts, June 10, 2003
[8] Zhou Xiaochuan(2004), Governor of The People’s Bank of China (2004); “Some Issues Concerning the Reform of the State-owned Commercial Banks”, Speech made at the IIF Spring Membership Conference, Shanghai, April 16, 2004

Internet Mining and its Phases

Manisha[1], Joni Birla[2], Gurpreet[3]

[1,2,3]*Department of Computer Science & Engineering, Ganga Institute of Technology and Management, Kablana, Jhajjar, Haryana, INDIA*

Abstract— In this paper, we describe the data warehousing and data mining. Data Warehousing is the process of storing the data on large scale and Data mining is the process of analyzing data from different perspectives and summarizing it into useful information - information that can be used to increase revenue, cuts costs, or both.

As massive amount of data is continuously being collected and stored, many industries are becoming interested in mining some patterns (association rules, correlations, clusters etc) from their database. Association rule mining is one of the important tasks that are used to find out the frequent itemset from customer transactional database. Each transaction consists of items purchased by a customer in a visit.

Internet mining is the application of data mining techniques to discover patterns from the Internet. Internet Usage Mining (IUM) is the process of application of data mining techniques over web data. The data sources are mainly the web server logs, proxy server logs and cookies stored in the user's computer. IUM is composed of three phases namely, preprocessing, pattern discovery and pattern analysis. This paper describes these phases in detail. A necessary introduction to Internet Mining is also provided for the purpose of background knowledge.

Keywords— Data warehousing and its architectures, Data Mining, Techniques of Data Mining, Internet mining.

I. INTRODUCTION

Data warehousing helps us to store the data. Data warehouse architecture is primarily based on the business processes of a business enterprise taking into consideration the data consolidation across the business enterprise with adequate security, data modeling and organization, extent of query requirements, meta data management and application, warehouse staging area planning for optimum bandwidth utilization and full technology implementation.

The Data Warehouse Architecture includes many facets. Some of these are listed as follows:

Process architecture
Date Model architecture
Technology architecture
Information architecture

Resource architecture

PROCESS ARCHITECTURE

Describes the number of stages and how data is processed to convert raw / transactional data into information for end user usage. The data staging process includes three main areas of concerns or sub- processes for planning data warehouse architecture namely “Extract”, “Transform” and “Load”.

These interrelated sub-processes are sometimes referred to as an “ETL” process.

1) Extract- Since data for the data warehouse can come from different sources and may be of different types, the plan to extract the data along with appropriate compression and encryption techniques is an important requirement for consideration.

2) Transform- Transformation of data with appropriate conversion, aggregation and cleaning besides de-normalization and surrogate key management is also an important process to be planned for building a data warehouse.

3) Load- Steps to be considered to load data with optimization by considering the multiple areas where the data is targeted to be loaded and retrieved is also an important part of the data warehouse architecture plan.

DATA MODEL ARCHITECTURE

In Data Model Architecture (also known as Dimensional Data Model), there are 3 main data modeling styles for enterprise warehouses:

3rd Normal Form - Top Down Architecture, Top Down Implementation

Federated Star Schemas - Bottom Up Architecture, Bottom Up Implementation

Data Vault - Top Down Architecture, Bottom Up Implementation

Technology Architecture

Scalability and flexibility is required in all facets. The extent of these features is largely depending upon organizational size, business requirements, nature of business etc.

Technology or Technical architecture primary evolved from derivations from the process architecture, meta data management requirements based on business rules and security levels implementations and technology tool specific evaluation.

Besides these, the Technology architecture also looks into the various technology implementation standards in database management, database connectivity protocols (ODBC, JDBC, OLE DB etc), Middleware (based on ORB, RMI, COM/DOM etc.), Network protocols (DNS, LDAP etc) and other related technologies.

Information Architecture

It is the process of translating the information from one form to another in a step by step sequence so as to manage the storage, retrieval, modification and deletion of the data in the data warehouse.

Resource Architecture

Resource architecture is related to software architecture in that many resources come from software resources. Resources are important because they help determine performance. Workload is the other part of the equation. If you have enough resources to complete the workload in the right amount of time, then performance will be high. If there are not enough resources for the workload, then performance will be low.

II. DATA MINING

Data mining involves the use of sophisticated data analysis tools to discover previously unknown, valid patterns and relationships in large data sets. These tools can include statistical models, mathematical algorithms, and machine learning methods (algorithms that improve their performance automatically through experience, such as neural networks or decision trees). Consequently, data mining consists of more than collecting and managing data, it also includes analysis and prediction.

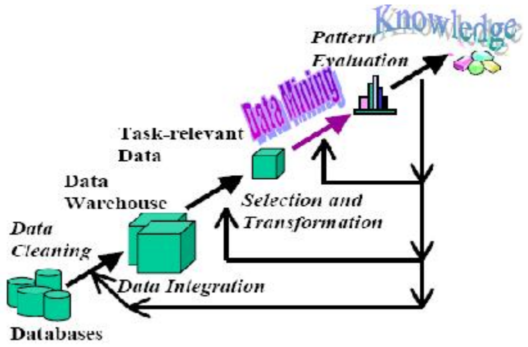


Fig:1 Data Mining is the core of Knowledge Discovery process

Data mining has its own tools and techniques to mine interesting information. When these tools and techniques are applied to the World Wide Web [as is or with some modifications and adaptations for the www environment], it can be called as Internet Mining.

So, Internet mining refers to discovery and analysis of useful information over the World Wide Web. Internet mining can be broadly classified into three categories:

- Content Mining
- Structure Mining
- Usage Mining

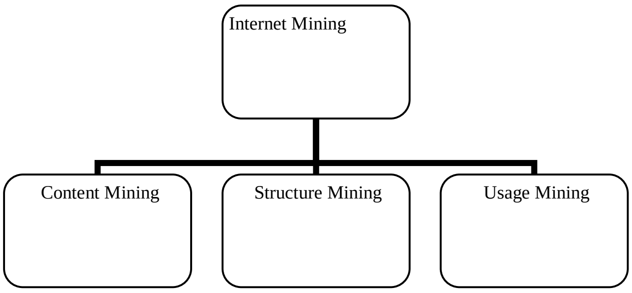


Fig:2 Types of Internet Mining

Content Mining:

Content Mining refers to mining of desired content over World Wide Web. Various search engines exists for the content mining, such as altavista, Lycos, WebCrawlar, MetaCrawlar etc.

Structure Mining:

Structure mining tries to discover the link structure of the hyperlinks at the inter-document level to generate structural summary about the Website and Web page.

Usage Mining:

Usage Mining refers to automatic knowledge mining of user access patterns from web servers. It includes,

Preprocessing
Pattern Discovery Tools
Pattern Analysis Tools

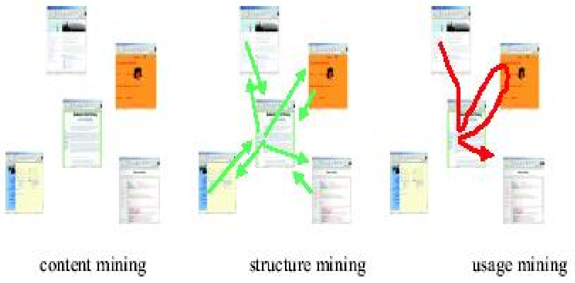


Figure 3: Types of Internet Mining

III. THE INTERNET USAGE MINING

Internet Usage Mining refers to automatic knowledge mining of user access patterns from different web servers.. It is the application of various techniques used in Data Mining to discover and analyze the usage patterns of web data.

Why Internet Usage Mining?

Internet has been growing at explosive rate since last decades. Lots of information is available on the internet. Millions of Websites exists and more are uploaded daily containing a lot of information. Billions of users browse on internet for different reasons, each searching for some interesting information. By Interesting Information, we refer to the information for which the user is browsing on internet, rest all information doesn’t seems to be interesting to him. How interesting the information is to a particular user, is identified by interestingness measures. Interestingness measures are used based on data mining techniques such as clustering, classification and association. These users needs tool and techniques [e.g. browsers], so that they can find needed information in a less time with more accurate results.

Another perspective is from the engineers, developers, web designers, and such professionals who strive to create more and more structured information, on structured websites. They are responsible for managing the structure of websites and providing interesting information in an interesting manner. They design tools and techniques for this and use them to manage websites by their content, and structure.

A very different perspective is from the companies who have invested millions into the web and web technologies. These are the organizations which are mostly based on E-Commerce, selling their products and services over the World Wide Web. For these organizations, it is very essential to keep the patterns of user visits, their profiles and their interestingness measures. This gives requirement for the development of client and server side intelligent systems that can mine knowledge across web.

So, it is essential to have some techniques and tools for satisfying the above said requirements. All these requirements give rise to “INTERNET MINING”. The term INTERNET MINING is very broad in its sense. But a special kind of internet mining called “INTERNET USAGE MINING” is the focus of the work presented here.

A number of organizations has invested highly on web technologies and carrying out business there. For example Amazon.com, ebay.com, buy.com etc. A lot of people access their websites across the world and does business with them. Analyzing this data can provide these organizations with the value of the customers. It helps the organizations to identify the “Good”, “Valued” and “Bad” customers based on their access patterns. This data also helps them for cross marketing strategies, their campaigns and others. Organizations can identify the effectiveness of their websites and also the effectiveness of their advertisements on different websites. Web Usage Mining helps them to identify the market segment and target interesting customers.

From where the data comes:

All the data, regarding the users is stored in their server access logs. Other sources include referrer logs which contains the information about referring pages from which the user has been referred to a particular page. User forms, survey results are also used as input. In Internet Usage Mining, data is collected at Web Servers, proxy servers, and organization's own database. Various methods such as cookies, CGI Script, Java Script, forms, session tracking, query data, click streams and page views are frequently used in web usage mining.

The data that is required to perform includes web server logs, cookies, proxy server logs, surveys, registration forms filled by users, access patterns of users (click stream) etc. The data sources can be classified into three categories:

Collection of Data from Server:

These data sources include logs from web server. Web server logs are important because they provide major user access patterns. All the works that user performs on a website are recorded in logs in the web server. Web servers are the computers having special software installed on them which are used to fulfill the user requests. A web server software may be Apache Tomcat, BEA WebLogic, IBM's WebSphere, Sun Microsystem's J2EE Application server etc. Logs that are maintained can be in different formats.

So, care should be taken when data is collected from more than one web server. A web usage mining tool must be capable of processing logs of more than one web server software.

However, the logs stored in web servers cannot be called the complete input, as there are different levels of caching in the internet architecture. Often, clients are first directed to cache and then web servers. Moreover there are different data that are not logged in the web servers such as information passed through POST method. Other sources includes cookies. Cookies are special files that are generated by web servers to collect information about individual clients. For creating cookies, user must authorize web server to created cookies, as cookies concern with privacy. Various scripting languages such as CGI Script, Java Script, VB Script and Perl Script are also used to handle the data that is sent back to the web server from client browsers.

Collection of Data from Clients:

Client side collection requires user cooperation. The technologies includes Java Applets, and various scripts which requires users to enable them. Data from clients can also be collected by using modified browsers. But user must be made willing to use that browser. Different companies like NetZoro[9], YouMint[10] and AllAdvantage[11] offers users incentives for using modified browsers and clicking on the advertisements on them.

Collection of Data from Proxy Servers:

Data collection only from web servers is not efficient to perform web usage mining. This is because, not all the requests reach the web servers each and every time. To speed up the browsing of internet, proxy servers are also used thus reducing the load on a web server. So, proxy servers also acts as servers and also contain user access logs. These logs should also be analyzed to perform web usage mining.

IV. PROCESS OF INTERNET USAGE MINING

The process of internet usage mining is composed of three steps. As given in the figure,

1. Pre-processing
2. Pattern Discovery
3. Pattern Analysis

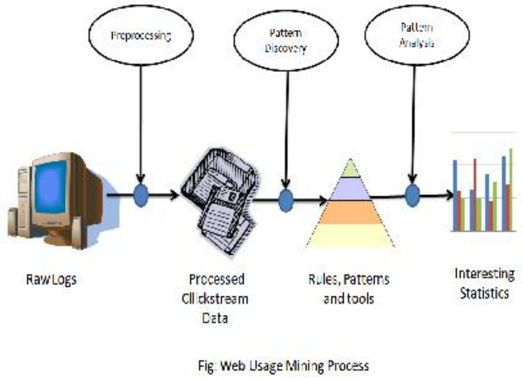

Preprocessing
Pattern Discovery
Pattern Analysis
Raw Logs
Processed Clickstream Data
Rules, Patterns and tools
Interesting Statistics
Fig: Web Usage Mining Process

Figure 4: Web usage mining process

Pre-processing:

Pre-processing is the process of preparing data received through server logs, proxy server logs and other data ready for pattern discovery and analysis task. The pre-processing task includes many processes. These are:

a. Data Cleaning: Involves removal of those log entries, which does not contribute to the data mining task. These unnecessary entries may be called noise.
b. Identification of users: Involves identification of users. It associates a page reference with a particular user. User identification is not an easy task because (i) a single IP address can be used by multiple users, (ii) Different IP addresses can be used by a single user
c. Identification of session: involves identification of session over a web server. It associates a group's web page references into user/server session. It also involves some issues: (i) a single IP address can have multiple server sessions, such as in case of proxy servers. (ii) Multiple IP address can have a single server session.
d. Path Completion: Due to proxy servers, and caching, it is not always possible to get complete data from web servers. The access paths shown in web server are incomplete if some page is referenced through proxy servers or cache. Path completion is the process of completing those incomplete paths.

Pattern Discovery:

Once the necessary transactions have been identified, the next step is the discovery of patterns. Pattern discovery phase extensively uses data mining algorithms. Various pattern discovery methods are:

Statistical Analysis: Statistical Analysis techniques are most commonly used techniques. These include frequency distribution, Mean, Mode, Median etc upon the web server logs. These techniques provide the basis for the IUM process. It provides the statistical data, and thus provides support for making market decisions.

Clustering: Clustering is division of data into groups of similar objects. A cluster represents objects that are similar between themselves. From machine learning perspective clusters corresponds to hidden patterns. Many clustering algorithms have been devised. Some major algorithms includes: Hierarchical Methods, K-means method, Grid based Clustering etc. In IUM, two type of clusters needs to be discovered: Usage Clusters and Page Clusters. Usage clusters helps to identify groups of users having similar browsing patterns. Page clusters helps to identify groups of pages with similar content. A dynamic clustering based model based on Markov Analysis is presented in [15]

Classification: Classification is a procedure in which individual items are placed into groups based on quantitative information on one or more characteristics inherent in the items (referred to as traits, variables, characters, etc) and based on a training set of previously labeled items. Formally, the problem can be stated as follows: given training data {(x1, y1),….,(xn,yn)} produce a classifier $h : \mathcal{X} \rightarrow \mathcal{Y}$ which maps any object $\mathbf{x} \in \mathcal{X}$ to its true classification label $y \in \mathcal{Y}$ defined by some unknown mapping $g : \mathcal{X} \rightarrow \mathcal{Y}$ (ground truth). For example, if the problem is filtering spam, then $\mathbf{x_i}$ is some representation of an email and y is either "Spam" or "Non-Spam". Statistical classification algorithms are typically used in pattern recognition systems. In WUM, we are interested in profiling users from same class. Classification algorithms includes: K-Nearest-Neighbor (KNN) Algorithm, Naïve Bayesian (NB) Algorithm, Concept Vector based Algorithms etc.

Association: Association Algorithms find correlations between different attributes in a dataset. The most common application of this kind of algorithm is for creating association rules, which can be used in a market basket analysis. For example, Microsoft association Algorithm. In IUM, association algorithms are used to relate web pages which were referenced by a user in a single session.. Algorithms like Apriori can be used for association rule mining.

Sequential patterns: Sequential patterns tend to find inter-transaction patterns in such a way that one pattern is followed by another in a time sequential manner. Web logs are periodically recorded in Web Servers. These log entries also includes time-stamps associated with each user visit on the link. These sequential patterns can help organizations to predict the future visit time of the user over their website. It can also help to establish the relation that which file/page was visited most during which user session/day/time/week/month.

Pattern Analysis:

Pattern Analysis is the last step in our IUM process. This helps to analyze organizations that how customers are accessing their website, and which are the pages they mostly visits. The purpose of pattern analysis is to filter out uninteresting rules and analyze the interesting rules which were found during the pattern discovery process. The major techniques included in this phase include:

SQL Queries

Visualization Techniques

OLAP Techniques and

Usability analysis.

V. CONCLUSIONS

The Internet Usage Mining is special case of Data Mining where the usage patterns of web pages are analyzed. Web pages can be on one or more servers, and also can be in different formats. Internet Usage Mining is very useful tool for organizations who wants to keep their customer base. We provided a detailed survey of research in this area. Various softwares and tools are available in market for IUM. We also provided the demonstration of WebLogAnalyzer® by Nihuo™. Though, the survey is short as the area is not very well established. There is immense scope of research in this area for identifying new methods and tools to discover pattern and analyze them.

REFERENCES

[1] J-Han M.Kamber "Data mining: concepts and techniques"2nd edition ,Morgan Kaufman publication, August
[2] Bart Goethals" survey on frequent pattern mining".
[3] The World Wide Web Consortium Web Usage Characterization Activity (WCA). http://w3.org/WCA
[4] Software Inc. Webtrends. http://www.webtrends.com
[5]NetGenesis netAnalysis desktop, http://www.netgen.com
[6] J.Shrivastava, R.Cooley, M.Deshpandey, Pang-Ning Tan, “Web Usage Mining: Discovery and Applications of Usage Patterns from Web Data”, Department of Computer Science and Engineering, University of Minnesota, Minneapolis, MN 55455 USA. http://cs.umn.edu
[7] B.Mobasher, R.Cooley, J.Shrivastava, “Web Mining: Information and Pattern discovery on the World Wide Web”, Department of Computer Science and Engineering, University of Minnesota, Minneapolis, MN 55455, USA http://cs.umn.edu7

Introduction & Features of 4G: A Review

Rishu Bhatia[1]
[1]*Department of Electronics & Communication Engineering, Ganga Institute of Technology and Management, Kablana, Jhajjar, Haryana, INDIA*

Abstract: 4G Wireless Systems or Fourth generation wireless system is a packet switched wireless system with wide area coverage and high throughput. It is designed to be cost effective and to provide high spectral efficiency. Fourth generation (4G) technology will offer many advancement to the wireless market, including downlink data rates well over 100 Mbps, low latency, very efficient spectrum use and low-cost implementations. The move to 4G networks will allow service providers to offer the impressive applications that will drive users to upgrade to the new phones.

I. INTRODUCTION

4G Wireless Systems or Fourth generation wireless system is a packet switched wireless system with wide area coverage and high throughput. It is designed to be cost effective and to provide high spectral efficiency. The 4g wireless uses Orthogonal Frequency Division Multiplexing (OFDM), Ultra Wide Radio Band (UWB), and Millimeter wireless. Data rate of 20mbps is employed. Mobile speed will be up to 200km/hr. The high performance is achieved by the use of long term channel prediction, in both time and frequency, scheduling among users and smart antennas combined with adaptive modulation and power control. Frequency band is 2-8 GHz. it gives the ability for world wide roaming to access cell anywhere. With impressive network capabilities, 4G enhancement promise to bring the wireless experience to an entirely new level with impressive user applications, such as sophisticated graphical user interfaces, high-end gaming, high-definition video and high-performance imaging. Consumer expectations for mobile handsets and similar products are becoming more and more sophisticated. Consumers are demanding a better user experience along with more advanced and useful applications on a more ergonomic device. The current 3G devices are good, but they will have to improve in areas like imaging and processing power to support future 4G applications like three dimensional (3D) and holographic gaming, 16 megapixel smart cameras and high-definition (HD) camcorders. Applications like these will demand more processing power than the current 3G handsets offer, requiring more efficient applications processors.

II. EVOLUTIONS OF WIRELESS TECHNOLOGIES

Wireless mobile communications systems are uniquely identified by "generation designations. Introduced in the early 1980s, first generation (1G) systems were marked by analog frequency modulation and used primarily for voice communications. Second generation (2G) wireless communications systems, which made their appearance in the late 1980s, were also used mainly for voice transmission and reception The wireless system in widespread use today goes by the name of 2.5G-an "in between " service that serves as a stepping stone to 3G. Whereby 2G communications is generally associated with Global System for Mobile (GSM) service, 2.5G is usually identified as being "fueled” by General Packet Radio Services (GPRS) along with GSM. In 3G systems, making their appearance in late 2002 and in 2003, are designed for voice and paging services, as well as interactive media use such as teleconferencing, Internet access, and other services. The problem with 3G wireless systems is bandwidth-these systems provide only WAN coverage ranging from 144 kbps (for vehicle mobility applications) to 2 Mbps (for indoor static applications). Segue to 4G, the "next dimension” of wireless communication. The 4g wireless uses Orthogonal Frequency Division Multiplexing (OFDM), Ultra Wide Radio Band (UWB), and Millimeter wireless and smart antenna. Data rate of 20mbps is employed. Mobile speed will be up to 200km/hr. Frequency band is 2 to 8 GHz. it gives the ability for world wide roaming to access cell anywhere.

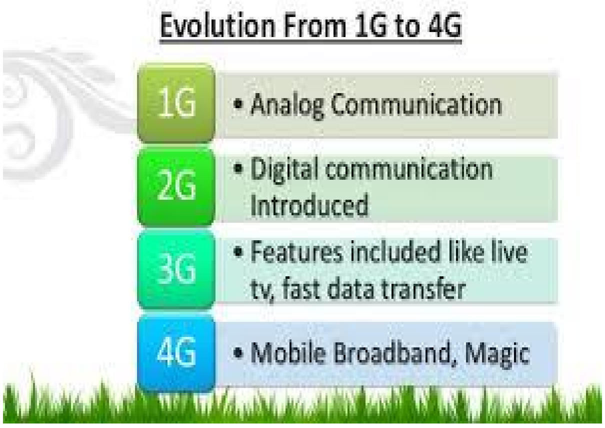

Evolution From 1G to 4G
1G
• Analog Communication
2G
• Digital communication Introduced
3G
• Features included like live tv, fast data transfer
4G
• Mobile Broadband, Magic

Figure 1: Evolution From 1G To 4G

III. LONG TERM EVOLUTION (LTE)

Long Term Evolution (LTE) technology is sometimes called 3.9G or Super 3G and has been developed by the Third Generation Partnership Project (3GPP) as an improvement to the current Universal Mobile Telecommunications System (UMTS). By using Orthogonal Frequency Division Multiple Access (OFDMA), LTE will be able to provide download rates of 150 Mbps for multi-antenna (2x2) multiple-input multiple output (MIMO) for the highest category terminals. For these terminals upload rates in the 50 Mbps range will allow an efficient transfer of data. LTE makes very efficient use of the available spectrum with channel bandwidths from 1.25 Megahertz (MHz) to 20 MHz The flexible “slice” will allow LTE to be more easily implemented in countries where 5 MHz is a commonly allocated amount of spectrum. LTE will also co-exist with legacy systems already rolled out around the world.

IV. RE-CONFIGURABLE TECHNOLOGY

In order to use the large variety of services and wireless networks, multimode user terminals are essential as they can adapt to different wireless networks by reconfiguring themselves. This eliminates the need to use multiple terminals (or multiple hardware components in a terminal).

The most promising way of implementing multimode user terminals is to adopt the software radio approach.

Challenges:

- Regulatory and Standardization issues
- Business models
- User preference profiles
- Inter-system handoff mechanisms and criteria
- Software download mechanisms
- Flexible spectrum allocation and sharing between Operators

Benefits for

- Users
  - Select network depending on service requirements and cost.
  - Connect to any network– Worldwide roaming.
  - Access to new services.
- Operators
  - Respond to variations in traffic demand (load balancing).
  - Incorporate service enhancements and improvements.
  - Correction of software bugs and upgrade of terminals.
  - Rapid development of new personalized and customized services.
- Manufacturers
  - Single platform for all markets.
  - Increased flexible and efficient production.

V. FEATURES OF 4G

- Support for interactive multimedia, voice, streaming video, Internet, and other broadband services
- IP based mobile system
- High speed, high capacity, and low cost per bit
- Global access, service portability, and scalable mobile services
- Seamless switching, and a variety of Quality of Service driven services
- Better scheduling and call admission control techniques
- Ad hoc and multi hop networks (the strict delay requirements of voice make multi hop network service a difficult problem)
- Better spectral efficiency
- Seamless network of multiple protocols and air interfaces (since 4G will be all]IP, look for 4G systems to be compatible with all common network technologies, including802.11, WCDMA, Blue tooth, and Hyper LAN).
- An infrastructure to handle pre existing 3G systems along with other wireless technologies, some of which are currently under development.

VI. APPLICATIONS OF 4G

Applications could include:

• 4G Ultra high speed internet access - E-mail or general web browsing is available.

• 4G Data intensive interactive user services - Services such as online satellite mapping will load instantly.

•4G Multiple User Video conferencing subscribers can see as well as talk to more than one person.

•4G Location-based services - a provider sends wide spread, real time weather or traffic

conditions to the computer or phone, or allows the subscriber to find and view nearby businesses or friends whilst communicating with them.

• 4G Tele-medicine - a medical provider monitors or provides advice to the potentially

CONCLUSION

This paper presented a brief description of 4G and their features. Fourth generation (4G) technology will offer many advancement to the wireless market, including downlink data rates well over 100 Mbps, low latency, very efficient spectrum use and low-cost implementations. The move to 4G networks will allow service providers to offer the impressive applications that will drive users to upgrade to the new phones. 4G seems to be a very promising generation of wireless communication that will change the people’s life in the wireless world.

REFERENCES

[1] B.G. Evans and K. Baughan, “Visions of 4G,”Electronics & Communication Engineering Journal, Vol. 12, No. 6, pp. 293–303, Dec. 2000.

[2] C. R. Casal, F. Schoute, and R. Prasald, “A novel concept for fourth generation mobile multimedia Communication,” in 50th Proc. IEEE Vehicular Technology Conference, Amsterdam, Netherlands, Sep.1999, Vol. 1, pp. 381–385.

[3] Y. Yamao, H. Suda, N. Umeda, and N. Nakajima, “Radio access network design concept for the fourth generation mobile communication system,” in 51st Proc. IEEE Vehicular Technology Conference, Tokyo, Japan, 2000, Vol. 3, pp. 2285–2298.

[4] J. M. Pereira, “Fourth generation: now, it is personal,” in Proc.11th IEEE Int.Symp.Personal, Indoor and Mobile Radio communications, London, UK, Sep. 2000, Vol. 2, pp. 1009–1016.

[5] K. Murota, NTT DoCoMo, “Mobile communications trends in Japan and NTT DoCoMo’s activities towards 21st century,” in ACTS Mobile Summit99, Sorrento, Italy, June 1999.

[6] J. Silva, European Commission, “Beyond IMT-2000,” in ITU-R WP8F workshop, Geneva, Mar. 2000.

[7] F. Williams, Ericsson, “Fourth generation mobile,” in ACTS Mobile Summit99, Sorrento, Italy, June 1999.

[8] H. Huomo, Nokia, “Fourth generation mobile,” in ACTS Mobile Summit99, Sorrento, Italy, June 1999.

Investigation On Properties Of Concrete By Replacing Of Fine Aggregate With Bottom Fly Ash

Manju Hooda[1], Sonam Jhakar[2], Sitender Chhillar[3]

[1,2,3]*Department of Civil Engineering, Ganga Institute of Technology and Management, Kablana, Jhajjar, Haryana, INDIA*

***ABSTRACT*- This paper presents the results of an experimental investigation carried out to evaluate the mechanical properties of concrete mixtures in which fine aggregate (sand) was partially replaced with bottom fly ash. Concrete- a material synonymous with strength and longevity has emerged as the dominant construction material for the infrastructure needs for the Twenty first century. In order to make use of coal ash popular in masonry mortar and structural concrete, research is going on worldwide. In India, research is also going on to utilize huge stocks coal ash in the different zones of the country. The prime objective of the study was to evaluate the structural properties and potential of concrete containing bottom ash vis-à-vis that of concrete containing no bottom ash of corresponding mix proportions and strength. The cubes were tested for the compressive strength and beams specimens were tested for flexural strength. Splitting tensile strength tests were conducted on cylinder specimens. The total numbers of 60 cubes, 40 beams specimens and 40 numbers of cylinders were tested for compressive strength, flexural strength and splitting tensile strength respectively at different ages to study the following aspect. The effect on unit weight of concrete after incorporating varying proportions of bottom ash. The effect of bottom ash on workability (C.F) of fresh concrete. The effect on compressive, flexural and splitting tensile strength using bottom ash in varying percentages as a partial replacement of fine aggregates.**

I. INTRODUCTION

A. GENERAL

Concrete is a material synonymous with strength and longevity has emerged as the dominant construction material for the infrastructure needs for the twenty first century. In addition to being durable, concrete is easily prepared and fabricated from readily available constituents and is therefore widely used in all types of structural systems. The challenge for the civil engineering community in the near future will be to realize projects in harmony with the concept of sustainable development and this involves the use of high performance materials and products manufactured at reasonable cost with the lowest possible environmental impact.

II. GENERATION OF FLY ASH AND BOTTOM ASH

Fly ash is a finely divided residue resulting from the combustion of pulverized coal in boilers. It is transported from the boilers by flue gases and collected by means of electric precipitators and mechanical collectors. It is a pozzolanic material and consists of small spheres of glassy surface of complex chemical composition together with small quantities of quartz, mullica, haematite, magnetite and unburnt carbon. It is finer than Portland cement and varies in color from light grey to dark, depending on carbon content. The greater the carbon content darker is the colour.

A. Disposal of Coal Ash

All this coal ash ejected out of the thermal power stations has to be disposed off to an open area available near the plant. In the wet disposal, which is at present being followed by most of the Thermal Power Stations, both the fly ash and bottom ash are grounded, mixed with water and are pumped into artificial lagoon or dumping yard. This is known as lagoon ash. Sometimes, coal ash mixed with water is conveyed to ponds or to nearby water courses. Disposal of coal ash in such a way no longer remains the answer. Such a huge collection of coal ash tomorrow will be more complex than the ones at present.

III. STRENGTH CHARACTERISTICS OF CONCRETE

It is the most important property of hardened concrete, which represents the ability of concrete to resist forces, in other words, strength of concrete is its resistance to rupture. It is important than other properties of concrete (secondary properties) e.g. durability, density, permeability, dimensional stability, appearance, behaviour of concrete under stresses and creep of concrete etc. Strength or some measure of it, is relatively easy to evaluate, as it is roughly indicative of the quality of concrete in other directions- strength increases, density, permeability, durability etc. generally improves. The present study compression, flexural strength and splitting tensile strength are considered for investigation. splitting .

A. Compressive Strength

It is the strength of concrete against crushing due to the direct compressive load. It is considered as most important property and often taken as the index of overall quality of concrete. Concrete has high compressive stress and it is normally required to resist compressive stresses. Compressive strength at 28 days after casting is taken as the criteria for specifying the quality of concrete. IS: 456-2000 stipulates the gain of strength beyond 28 days.

B. Tensile Strength

Concrete as we know is relatively strong in compression and weak in tension. In reinforced concrete members, little dependence is placed on the tensile strength of concrete since steel reinforcing bars are provide to resist all tensile forces.

IV. NEED FOR THE PRESENT STUDY

The continuous reduction of natural resources and the environmental hazards posed by the disposal of coal ash has reached an alarming proportion. The use of coal ash in normal strength concrete is a new dimension in concrete mix design and if applied on large scale would revolutionize the construction industry, by economizing the construction cost and decreasing the ash content.

V. OBJECTIVE OF THE STUDY

- To design the reference concrete mix of grade M25 using OPC 43 grade cement.

- To investigate the effect of replacing fine aggregate with bottom ash in varying percentages (20-50%) on compressive strength, flexural tensile strength and splitting tensile strength at the moist curing of 7,28, 56 and 90 days.
- To investigate the effect of bottom ash on workability of freshly mixed concrete.
- To investigate the effect the effect the bottom ash on unit weight of concrete.

VI. EXPERIMENTAL PROGRAM

A. GENERAL

The prime objective of the study was to evaluate the structural properties and potential of concrete containing bottom ash vis-à-vis that of concrete containing no bottom ash of corresponding mix proportions and strength.

Since it is an established fact that hydration of pozzolanic material is a delayed process compared to hydration of plain cement concrete, the main emphasis was to compare the relative structural properties of two types of the concrete at later ages. Moreover bottom ash used in this study was obtained from 'Tau Devi Lal Thermal Power Plant, Panipat'.

To investigate the strength considerations the following tests were conducted:

- Compressive strength test
- Flexural strength test
- Split tensile strength test

Along with this test for workability was also conducted. The compression test was carried out on 150mm X 150mm X 150mm cubes, flexural strength tests was carried on 100mm X 100mm X 500mm prisms and split tensile strength test was carried out on 150mm X 300 mm cylinders.

VII. MATERIAL TESTING

The following materials were used in the experimental work.

- Cement
- Fine aggregates
- Coarse aggregates
- Bottom ash
- Super plastisizer

A. *Cement*

In the present investigation ordinary Portland cement 43 grade with brand name 'Jaypee Cement' conforming to IS:8112-1989 was used. The cement was tested in accordance with the test methods specified in IS:4031-1988 and results obtained.

B. *Fine Aggregates*

TABLE I

TABLE III

SPECIFICATIONS OF SUPERPLASTICIZER

Basis	**Aqueous solution of modified polycarboxylate**
Appearance	Brown liquid
Density	Approx. 1.10
Ph	Approx. 5.0

Specific gravity	2.65

The sand used conforms to zone III. Sieve analysis for the sand was performed and result were obtained.

C. *Coarse Aggregates*

TABLE II

Maximum size of aggregates	20mm
Specific Gravity	2.6
Fineness modulus	6.9
Bottom Ash	
Specific Gravity	1.68

D. Water

Portable water available in the laboratory extracted from the ground was used for casting and curing.

E. *Super Plasticizer*

Super plastisizer of the make 'SIKA VISCOCRETE-10 (H1)' was used for the concrete.

VIII. CONCRETE MIX DESIGN

In the present investigation the existing method as per IS: 10262 (1982)[8] has been used for selecting the referenced mix (M25), however new information given in IS:456 (2000) have been incorporated. In order to get the final mix proportions for the reference mix design three trails had been prepared earlier and tested at 7 days and 28 days.

IX. CASTING OF SPECIMENS

The moulds were filled in three equal layers of concrete. Bottom layer was compacted with a 16mm dia. temping rod with bullet nose to provide a proper formation of corners and base. Then second and third layers were placed and temped. After this the moulds were placed on the table vibrator for the compaction. Proper compaction is attained when the slurry of cement appears on the surface. The vibrator was stopped and some amount of concrete was poured to fill it. The mould was again vibrated and top surface was finished with a trowel. Casting for specimens was done for each test of plain cement concrete and bottom ash concrete. The specimens were kept in a clean water tank just after removal from the mould and kept continuously moist till the time of testing.

X. PROPERTIES OF CONCRETE TO BE TESTED

- Properties Of Fresh Concrete
- Properties Of Hardend Concrete

A. *Properties of Fresh Concrete*

The diver's requirements mixibility, stability, transportability,

placability, modility, compactability and finishability of fresh concrete collectively refer to as workability.

1) *Measurement Of Workability:*A number of different tests are available for the measuring the workability of fresh concrete, but none of them is wholly satisfactory. Each test measures only particular aspect of it.

The different tests used for measuring workability are:

- The slump test
- The compaction factor test
- The Vee Bee consistency test
- The flow

B. Properties Of Hardend Concrete

1) *Compressive Strength Test:* Compressive strength tests were carried on 150mm*150mm*150mmm cubes with compression testing machine of 1000KN capacity. The compressive strength was found after 7, 28, 56 and 90 days in order to compare the strength of different concrete mixes.

2) *Flexural Strength Test:*Although the concrete is not normally designed to resist tension, the knowledge of tensile strength is of value in estimating the load under which crack will develop.. In the present study, the flexural test was conducted on 100mm*100mm*500mm specimens under two point loading pattern. The supports were placed at 400mm apart and loading was placed at 133mm apart.

3) *Splitting Tensile Strength:* Part from flexural test, the other method used to determine the tensile strength of concrete is splitting tensile strength test. In this test, in general a compressive force is applied to a concrete specimen in such a way that the specimen fails due to tensile stresses induced in the specimen.The splitting tensile strength was found at 7, 28, 56, and 90 days after casting of specimens.

XI. RESULTS AND DISCUSSION

A. GENERAL

The results of the tests conducted on plain and bottom ash concrete. The cubes were tested for the compressive strength and beams specimens were tested for flexural strength. Splitting tensile strength tests were conducted on cylinder specimens. The total numbers of 60 cubes, 40 beams specimens and 40 numbers of cylinders were tested for compressive strength, flexural strength and splitting tensile strength respectively at different ages to study the following aspects:

1) The effect on unit weight of concrete after incorporating varying proportions of bottom ash.
2) The effect of bottom ash on workability (C.F) of fresh concrete.
3) The effect on compressive, flexural and splitting tensile strength using bottom ash in varying percentages as a partial replacement of fine aggregates.

REFERENCES

[1] T. U. Ganiron Jr, "Scrap Waste Tire as an Additive in Asphalt Pavement for Road Construction",
[2] International Journal of Advances in Applied Sciences, vol. 1, no. 2, (2012), pp. 31-37.
[3] 2.T. U. Ganiron Jr, "Concrete Debris a Fine Aggregate for Architectural Finishing Mortar", Architectural
[4] Journal, vol. 2, no. 5, (2012).
[5] 3.R. L. Davison, "Trace Elements in Fly Ash, Dependence of Concentration on Particle Size", Environmental
[6] Science & Technology, vol. 8, no. 13, (1974), pp. 1107-1113.
[7] 4.T. U. Ganiron Jr, "Effects of Rice Hush as Substitute for Fine Aggregate in Concrete Mixture", International
[8] Journal of Advanced Science and Technology", vol. 58, (2013).
[9] 5.T. U. Ganiron Jr, "Technical Specification of Concrete Hollow Blocks with Coconut Shells and Fiber as
[10] Aggregate", Proceedings of the 1st International Concrete Sustainability, (2013) May 27, Tokyo, Japan.
[11] 6.H. Vogg and L. Stieglitz, "Thermal behavior of PCDD/PCDF in Fly Ash from Municipal Incinerators",
[12] Chemosphere, vol. 15, no. 9, (1986), pp. 1373-1378.
[13] 7.Akthem A.Av-Manaseeer, Moir D.Hang and Karum W.Nasser 'Compressive strength of concrete containing fly ash, Brine and Admixture' ACI Material J. March-April 1988, pp 109-116.
[14] 8.Chai Jaturapitakkul & Raungrut Cheerarot 'Development of Bottom Ash as pozzolainic material' J. of materials in Civil Engineering Jan-Feb 2003, pp48-53.
[15] 9.Gambhir M.L. 'Concrete Technology', Publisher Tata McGraw Hill.
[16] 10.IS:383-1970. 'Specifications for Coarse and Fine Aggregates from Natural sources for Concrete' Bureau of Indian Standards, New Delhi, India.
[17] 11.IS:516-1959. 'Indian Standard Code of Practice Methods of Test for Strength of Concrete' Bureau of Indian Standards, New Delhi, India.
[18] 12.IS:1199-1959. 'Indian Standard Methods of Sampling and analysis of Concrete, Bureau of Indian Standards, New Delhi, India.
[19] 13.IS:8112-1989. Specifications for 43 Grade Portland Cement, Bureau of Indian Standards, New Delhi, India.
[20] 14.IS:10262-1982. 'Recommended guidelines for Concrete Mix Design' Bureau of Indian Standards, New Delhi, India.
[21] 15.J.Pera, L.Coutaxz, J.Ambroise, M Chababbet ' Use of incinerator Bottom Ash in concrete' Cement and Concrete Research volume 27, 1997, pp 1-5.

Author Profile: Manju Hooda,B.Tech., M. Tech. Scholar in Civil Engineering (Structural Design) from Ganga Institute of Technology and Management, Kablana, Jhajjar, Haryana (India) affiliated to Maharshi Dayanand University, Rohtak, Haryana (India).

Investigation On Properties Of Concrete By Replacing Of Fine Aggregate With Bottom Fly Ash

Manju Hooda[1], Sonam Jhakar[2], Sitender[3]
[1,2,3] Department of Civil Engineering, Ganga Institute of Technology and Management, Kablana, Jhajjar, Haryana, INDIA

Abstract: This paper presents the results of an experimental investigation carried out to evaluate the mechanical properties of concrete mixtures in which fine aggregate (sand) was partially replaced with bottom fly ash. Concrete- a material synonymous with strength and longevity has emerged as the dominant construction material for the infrastructure needs for the Twenty first century. In order to make use of coal ash popular in masonry mortar and structural concrete, research is going on worldwide. In India, research is also going on to utilize huge stocks coal ash in the different zones of the country. The prime objective of the study was to evaluate the structural properties and potential of concrete containing bottom ash vis-à-vis that of concrete containing no bottom ash of corresponding mix proportions and strength. The cubes were tested for the compressive strength and beams specimens were tested for flexural strength. Splitting tensile strength tests were conducted on cylinder specimens. The total numbers of 60 cubes, 40 beams specimens and 40 numbers of cylinders were tested for compressive strength, flexural strength and splitting tensile strength respectively at different ages to study the following aspect. The effect on unit weight of concrete after incorporating varying proportions of bottom ash. The effect of bottom ash on workability (C.F) of fresh concrete. The effect on compressive, flexural and splitting tensile strength using bottom ash in varying percentages as a partial replacement of fine aggregates.

I. INTRODUCTION

Concrete is a material synonymous with strength and longevity has emerged as the dominant construction material for the infrastructure needs for the twenty first century. In addition to being durable, concrete is easily prepared and fabricated from readily available constituents and is therefore widely used in all types of structural systems. The challenge for the civil engineering community in the near future will be to realize projects in harmony with the concept of sustainable development and this involves the use of high performance materials and products manufactured at reasonable cost with the lowest possible environmental impact.

GENERATION OF FLY ASH AND BOTTOM ASH

Fly ash is a finely divided residue resulting from the combustion of pulverized coal in boilers. It is transported from the boilers by flue gases and collected by means of electric precipitators and mechanical collectors. It is a pozzolanic material and consists of small spheres of glassy surface of complex chemical composition together with small quantities of quartz, mullica, haematite, magnetite and unburnt carbon. It is finer than Portland cement and varies in color from light grey to dark, depending on carbon content. The greater the carbon content darker is the colour.

DISPOSAL OF COAL ASH

All this coal ash ejected out of the thermal power stations has to be disposed off to an open area available near the plant. In the wet disposal, which is at present being followed by most of the Thermal Power Stations, both the fly ash and bottom ash are grounded, mixed with water and are pumped into artificial lagoon or dumping yard. This is known as lagoon ash. Sometimes, coal ash mixed with water is conveyed to ponds or to nearby water courses. Disposal of coal ash in such a way no longer remains the answer. Such a huge collection of coal ash tomorrow will be more complex than the ones at present.

STRENGTH CHARACTERISTICS OF CONCRETE

It is the most important property of hardened concrete, which represents the ability of concrete to resist forces, in other words, strength of concrete is its resistance to rupture. It is important than other properties of concrete (secondary properties) e.g. durability, density, permeability, dimensional stability, appearance, behaviour of concrete under stresses and creep of concrete etc. Strength or some measure of it, is relatively easy to evaluate, as it is roughly indicative of the quality of concrete in other directions- strength increases, density, permeability, durability etc. generally improves. The present study compression, flexural strength and splitting tensile strength are considered for investigation. splitting

COMPRESSIVE STRENGTH

It is the strength of concrete against crushing due to the direct compressive load. It is considered as most important property and often taken as the index of over all quality of concrete. Concrete has high compressive stress and it is normally required to resist compressive stresses. Compressive strength at 28 days after casting is taken as the criteria for specifying the quality of concrete. IS: 456-2000 stipulates the gain of strength beyond 28 days.

TENSILE STRENGTH

Concrete as we know is relatively strong in compression and weak in tension. In reinforced concrete members, little dependence is placed on the tensile strength of concrete since steel reinforcing bars are provide to resist all tensile forces.

NEED FOR THE PRESENT STUDY

The continuous reduction of natural resources and the environmental hazards posed by the disposal of coal ash has reached an alarming proportion. The use of coal ash in normal strength concrete is a new dimension in concrete mix design and if applied on large scale would revolutionize the construction industry, by economizing the construction cost and decreasing the ash content.

OBJECTIVE OF THE STUDY

1. To design the reference concrete mix of grade M25 using OPC 43 grade cement.

2. To investigate the effect of replacing fine aggregate with bottom ash in varying percentages (20-50%) on compressive strength, flexural tensile strength and splitting tensile strength at the moist curing of 7,28, 56 and 90 days.
3. To investigate the effect of bottom ash on workability of freshly mixed concrete.
4. To investigate the effect the effect the bottom ash on unit weight of concrete.

II. EXPERIMENTAL PROGRAM

The prime objective of the study was to evaluate the structural properties and potential of concrete containing bottom ash vis-à-vis that of concrete containing no bottom ash of corresponding mix proportions and strength.

Since it is an established fact that hydration of pozzolanic material is a delayed process compared to hydration of plain cement concrete, the main emphasis was to compare the relative structural properties of two types of the concrete at later ages. Moreover bottom ash used in this study was obtained from 'Tau Devi Lal Thermal Power Plant, Panipat'.

To investigate the strength considerations the following tests were conducted:

1. Compressive strength test
2. Flexural strength test
3. Split tensile strength test

Along with this test for workability was also conducted. The compression test was carried out on 150mm X 150mm X 150mm cubes, flexural strength tests was carried on 100mm X 100mm X 500mm prisms and split tensile strength test was carried out on 150mm X 300 mm cylinders.

MATERIAL TESTING

The following materials were used in the experimental work.

1. Cement
2. Fine aggregates
3. Coarse aggregates
4. Bottom ash
5. Super plastisizer

Cement

In the present investigation ordinary Portland cement 43 grade with brand name 'Jaypee Cement' conforming to IS:8112-1989 was used. The cement was tested in accordance with the test methods specified in IS:4031-1988 and results obtained.

Fine Aggregates

Specific gravity	2.65

The sand used conforms to zone III. Sieve analysis for the sand was performed and result were obtained.

Coarse Aggregates

Maximum size of aggregates	20mm
Specific Gravity	2.6
Fineness modulus	6.9
Bottom Ash	
Specific Gravity	1.68

Table Specifications of Superplasticizer

Basis	Aqueous solution of modified polycarboxylate
Appearance	Brown liquid
Density	Approx. 1.10
Ph	Approx. 5.0

Water

Portable water available in the laboratory extracted form the ground was used for casting and curing.

Super Plasticizer

Super plastisizer of the make 'SIKA VISCOCRETE-10 (H1)' was used for the concrete.

III. CONCRETE MIX DESIGN

In the present investigation the existing method as per IS: 10262 (1982)[8] has been used for selecting the referenced mix (M25), however new information given in IS:456 (2000) have been incorporated. In order to get the final mix proportions for the reference mix design three trails had been prepared earlier and tested at 7 days and 28 days.

CASTING OF SPECIMENS

The moulds were filled in three equal layers of concrete. Bottom layer was compacted with a 16mm dia. temping rod with bullet nose to provide a proper formation of corners and base. Then second and third layers were placed and temped. After this the moulds were placed on the table vibrator for the compaction. Proper compaction is attained when the slurry of cement appears on the surface. The vibrator was stopped and some amount of concrete was poured to fill it. The mould was again vibrated and top surface was finished with a trowel. Casting for specimens was done for each test of plain cement concrete and bottom ash concrete. The specimens were kept in a clean water tank just after removal from the mould and kept continuously moist till the time of testing.

PROPERTIES OF CONCRETE TO BE TESTED

- Properties Of Fresh Concrete
- Properties Of Hardend Concrete

Properties of Fresh Concrete

The diver's requirements mixibility, stability, transportability, placability, modility, compactability and finishability of fresh concrete collectively refer to as workability.

Measurement Of Workability

A number of different tests are available for the measuring the workability of fresh concrete, but none of them is wholly satisfactory. Each test measures only particular aspect of it.

The different tests used for measuring workability are:

(i) The slump test

(iii) The compaction factor test

(iii) The Vee Bee consistency test

(iv) The flow

Properties Of Hardend Concrete

Compressive Strength Test

Compressive strength tests were carried on 150mm*150mm*150mmm cubes with compression testing machine of 1000KN capacity. The compressive strength was found after 7, 28, 56 and 90 days in order to compare the strength of different concrete mixes.

Flexural Strength Test

Although the concrete is not normally designed to resist tension, the knowledge of tensile strength is of value in estimating the load under which crack will develop.. In the present study, the flexural test was conducted on 100mm*100mm*500mm specimens under two point loading pattern. The supports were placed at 400mm apart and loading was placed at 133mm apart.

Splitting Tensile Strength

Part from flexural test, the other method used to determine the tensile strength of concrete is splitting tensile strength test. In this test, in general a compressive force is applied to a concrete specimen in such a way that the specimen fails due to tensile stresses induced in the specimen.The splitting tensile strength was found at 7, 28, 56, and 90 days after casting of specimens.

IV. RESULTS AND DISCUSSION

The results of the tests conducted on plain and bottom ash concrete. The cubes were tested for the compressive strength and beams specimens were tested for flexural strength. Splitting tensile strength tests were conducted on cylinder specimens. The total numbers of 60 cubes, 40 beams specimens and 40 numbers of cylinders were tested for compressive strength, flexural strength and splitting tensile strength respectively at different ages to study the following aspects:

1. The effect on unit weight of concrete after incorporating varying proportions of bottom ash.
2. The effect of bottom ash on workability (C.F) of fresh concrete.
3. The effect on compressive, flexural and splitting tensile strength using bottom ash in varying percentages as a partial replacement of fine aggregates.

REFERENCES

[1] T. U. Ganiron Jr, “Scrap Waste Tire as an Additive in Asphalt Pavement for Road Construction”,
[2] International Journal of Advances in Applied Sciences, vol. 1, no. 2, (2012), pp. 31-37.
[3] 2.T. U. Ganiron Jr, “Concrete Debris a Fine Aggregate for Architectural Finishing Mortar”, Architectural
[4] Journal, vol. 2, no. 5, (2012).
[5] 3.R. L. Davison, “Trace Elements in Fly Ash, Dependence of Concentration on Particle Size”, Environmental
[6] Science & Technology, vol. 8, no. 13, (1974), pp. 1107-1113.
[7] 4.T. U. Ganiron Jr, “Effects of Rice Hush as Substitute for Fine Aggregate in Concrete Mixture”, International
[8] Journal of Advanced Science and Technology”, vol. 58, (2013).
[9] 5.T. U. Ganiron Jr, “Technical Specification of Concrete Hollow Blocks with Coconut Shells and Fiber as
[10] Aggregate”, Proceedings of the 1st International Concrete Sustainability, (2013) May 27, Tokyo, Japan.
[11] 6.H. Vogg and L. Stieglitz, “Thermal behavior of PCDD/PCDF in Fly Ash from Municipal Incinerators”,
[12] Chemosphere, vol. 15, no. 9, (1986), pp. 1373-1378.
[13] 7.Akthem A.Av-Manaseeer, Moir D.Hang and Karum W.Nasser ‘Compressive strength of concrete containing fly ash, Brine and Admixture’ ACI Material J. March-April 1988, pp 109-116.
[14] 8.Chai Jaturapitakkul & Raungrut Cheerarot ‘Development of Bottom Ash as pozzolainic material’ J. of materials in Civil Engineering Jan-Feb 2003, pp48-53.
[15] 9.Gambhir M.L. ‘Concrete Technology’, Publisher Tata McGraw Hill.
[16] 10.IS:383-1970. ‘Specifications for Coarse and Fine Aggregates from Natural sources for Concrete’ Bureau of Indian Standards, New Delhi, India.
[17] 11.IS:516-1959. ‘Indian Standard Code of Practice Methods of Test for Strength of Concrete’ Bureau of Indian Standards, New Delhi, India.
[18] 12.IS:1199-1959. ‘Indian Standard Methods of Sampling and analysis of Concrete, Bureau of Indian Standards, New Delhi, India.
[19] 13.IS:8112-1989. Specifications for 43 Grade Portland Cement, Bureau of Indian Standards, New Delhi, India.
[20] 14.IS:10262-1982. ‘Recommended guidelines for Concrete Mix Design’ Bureau of Indian Standards, New Delhi, India.
[21] 15.J.Pera, L.Coutaxz, J.Ambroise, M Chababbet ‘ Use of incinerator Bottom Ash in concrete’ Cement and Concrete Research volume 27, 1997, pp 1-5.

Author Profile: Manju Hooda,B.Tech., M. Tech. Scholar in Civil Engineering (Structural Design) from Ganga Institute of Technology and Management, Kablana, Jhajjar, Haryana (India) affiliated to Maharshi Dayanand University, Rohtak, Haryana (India).

JAVA RING

Sakshi Bhardwaj[1] Sonia Tomer[2]
[1,2]*Department of Computer Science &Engineering, Ganga Institute of Technology and Management, Kablana, Jhajjar, Haryana, INDIA*

***Abstract:* Java ring is a finger ring in which a small microprocessor was contained with some built-in capabilities for the user, it is a sort of smart card that is easily wearable on the finger. Sun microsystem's java ring was introduced at their java one conference in 1998 and it contained an inexpensive microprocessor built in built in a stainless steel ibutton that was running a java virtual machine (jvm)and was preloaded with applets (little applications programs). It was not an ordinary ring that contains the gemstones instead of gem stones it contained the inexpensive microprocessor. It was built by Dallas semiconductor.**

Keywords:* *Rapid zeroization, Personalization, Wearable, Cryptographic iButton, Java virtual machine, Applets, etc.

1. INTRODUCTION

The java ring was an extremely secure java-powered electronic token that has a continuously running, the unalterable real time clock and rugged packaging that was suitable for many applications. The most precious stone or we can say the jewel of the java ring is the java i-button that is a one million transistor, with a single chip trusted micro computer that has a powerful java virtual machine(JVM) that is housed in a rugged and secure stainless steel case. That was designed to be a fully compatible with the java card 2.0 standard. The packaged module has only a single electrical contact and a ground return, confirming to the specifications of the Dallas semiconductor I-Wire bus. In this the Lithium-backed non-volatile SRAM the static random access memory offers the high read and write speed and an unparallel tamper resistance. Through near-instances clearing of all memory when tempring is detected, a feature known as rapid zeroization . The data integrity and the clock function are maintained for more than 10 years. The 16 mili meter diameter stainless steel enclosure accommodates larger chip sizes needed for up to 128 kilobytes of high speed non-volatile static ram. The small and extremely rugged packaging of the module allows it to attach to the accessoryof your choice to match individual lifestyles, such as a key job, wallet , watch, necklace, braclet or finger ring.

Figure 1

II. BACKGROUND

In the summer of 1989, Dallas semiconductor corporation produced the first stainless steel encapsulated memory devices utilizing the Dallas semiconductor i-wire communication protocol. By 1990, the protocol had been refined and employed in a variety of self contained memory devices. Originally called "touch memory" device they were later renamed "i-buttons" packaged like batteries, i-buttons have only a single active electrical contact on the top surface, with the stainless steel shell serving as ground.

Data can be read from or written to the memory serially through a simple and inexpensive RS232C serial port adapter, which also supplies the power required to perform the I/O. The i-button memory can be read or written with a momentary contact to the "blue dot" receptor provided by the adapter. When not connected to the serial port adapted memory data is maintained in non-volatile random access memory (NVRAM) by a lifetime lithium energy suppkly that will maintain the memory content for at least 10 yearas. Unlike electrically erasable programmable read only memory (EEPROM), the NVRAM i-button memory can be erased and rewritten as often as necessary without wearing out. It can also be erased or rewritten at the high speeds typical of complementary metal oxide (CMOS) memory, without requiring time-consuming programming of EEPROM.

Figure 2

III. JAVA VIRTUAL MACHINE

The java virtual machine is the piece of the software that recognizes the java language and translates the byte code.It supports java card 2.0 specification. It allows the java ring to navigate through java operating environment. It provides automatic garbage collection for efficient reuse of memory space.

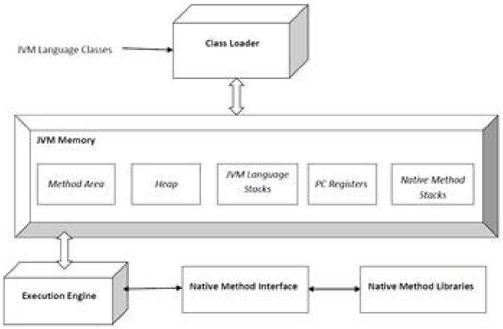


Figure 3

IV. iBUTTON

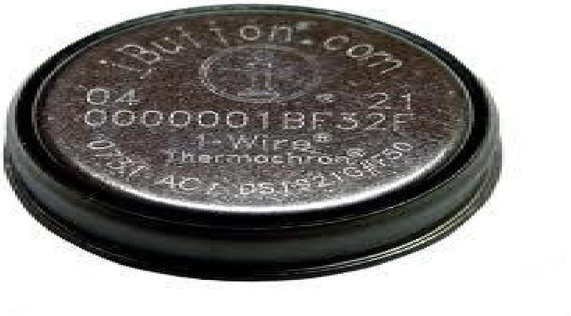
The i-button device is a micro chip similar to those used in a smart card but housed in a round stainless steel button of 17.35mm. The ibutton is a computer chip that is enclosed in a

16mm thick stainless steel can. Because of this unique and durable container, up-to-date information can travel with a person or object any where they go. It is designed to be fully compatible with the java card 2.0 standard. It is small and portable enough to attach to a key fob, ring, watch, or other personal items.

Types of i-button:-

- Memory iButton.
- Java powered cryptographic iButton.
- Thermochron iButton.

Figure 4



V. JAVA CONNECTION

The java connection is with the experience designing the E-Commerce operating system and VM for the Crypto iButtom hardware platform. With a java iButton, a vast number of existing java programmers could easily learn to write applets that could be compiled with the standard tools available from sun Microsystems, loaded into the java iButton, and run on demand to support a wide variety of financial applications. The java card 2.0 specifications provided the opportunity to implement a useful version of the JVM and runtime environment with the limited resources available to a small process.

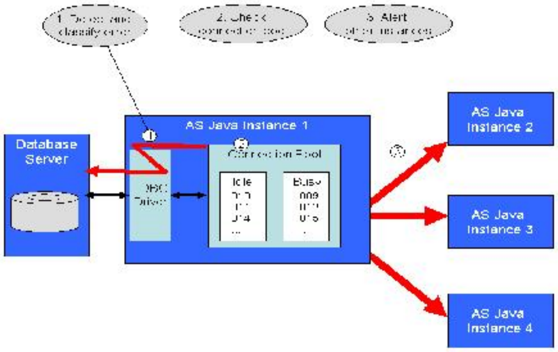
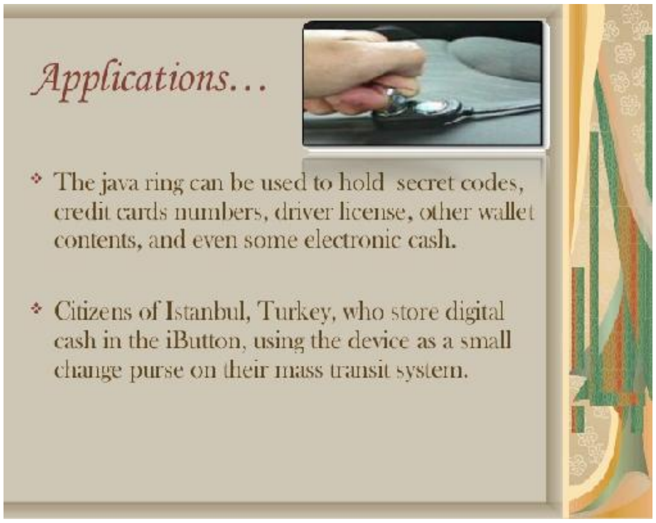


Figure 5

VI. APPLICATIONS/USES OF JAVA RING

Access control to buildings and equipments. It secure the network login using challenge/response authentication. Storage vault for user names and passwords. It is the user profile for rapid internet form-filling. It proides the digital signature gor the E-Commerce. United states postal service postal security device for PC postage downlodable over the internet. Digital photo ID and fingerprint biometrics.



Applications…

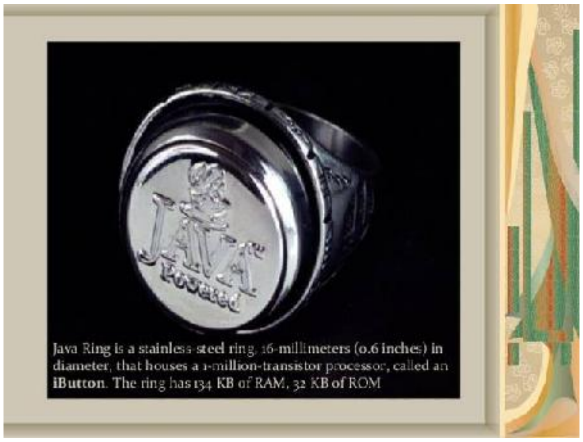
- The java ring can be used to hold secret codes, credit cards numbers, driver license, other wallet contents, and even some electronic cash.
- Citizens of Istanbul, Turkey, who store digital cash in the iButton, using the device as a small change purse on their mass transit system.

Figure 6

VII. INSIGHT OF JAVA RING

The todays world is the hunt for the new technology, and has contributed miracles to the world of science, the ever ending stream. The one such contribution is the JAVA RING the finger ring that contains a small microprocessor with a built in caoabilities for the user, a sort of smart card that is wearable on the finger. Well it's something new to the world. Since it has not been very popular these days, it's really a new opening for sure.

Introducing more of it we can say that, it contained an inexpensive microprocessor in a stainless steel iButton , this particular is running on a java virtual machine and it is preloaded with applets.



Java Ring is a stainless-steel ring, 16-millimeters (0.6 inches) in diameter, that houses a 1-million-transistor processor, called an **iButton**. The ring has 134 KB of RAM, 32 KB of ROM

Figure 7

VIII. OPERATING SYSTEM IN JAVA RING

A special operating system was designed and stored in the ROM of crypto iButton to support cryptography and general purpose financial transaction- such as those required by postal service program. While not a java virtual machine the E-Commerce firmware designed for the application have several points of similarity with java, including an object oriented design and a byte code interpreter to interpret and execute the Dallas semiconductor custom designed E-Commerce script language.

The compiler was also written to compile the high level language representation of script language to a byte code form that could be interpreted by the E-Commerce VM.

Although the E-Commerce firmware was intented primarily through the USPS application, the firmware supports a variety of general electronic commerce models that are suitable for many different applications.

IX. SECURITY

National institute of Standards and technology (NIST) and the Canadian security establishment (CSE) have validated the DS1954 cryptographic iButton as meeting federal information processing publications (FIPS 140-I).

The crypto iButton includes the highest level of physical security ever validated by the FIPS 140-1 program and it does this in an extremely small and durable package. There is no other hardware token like this meeting government and federal requirements and providing rich functionality at a fraction of the cost of similar devices.

The crypto iButton provides hardware cryptographic services such as long term safe storage of private keys , a high speed math accelarater for 1024- bit public key cryptography and secure message digest.

Figure 7

X. ADVANTAGES

The java ring is a very easy and convinent way for the users. The users are more sure than using the passwords as since the passwords are short or they can be guessed. The java ring provides the authentication to users which is crucial for the many applications. As it is very easier for administrator to maintain the security infrastructure and it will provide the real memory, more power and a capacity for dynamic programming. The java ring was used widely all around the world for the several applications such as the access control, asset management, e-cash and for many other purpose.

ASSET MANAGEMENT: The java ring provides us the very simple and a secure way of identifying any person or the asset. It will serve us an electronic serial number that can never be duplicated. With an memory up to 32k bytes the java ring can also the give the asset their own personalized database. As the each asset will have the ability to store the unique information permanently fixed to the asset This makes the java ring perfect for the various assets management and data collection function such as equipment maintainance and record and inventory management. By connecting our java ring to a ring receptor to a car and the car knows based on your profile what you are allowed to do.

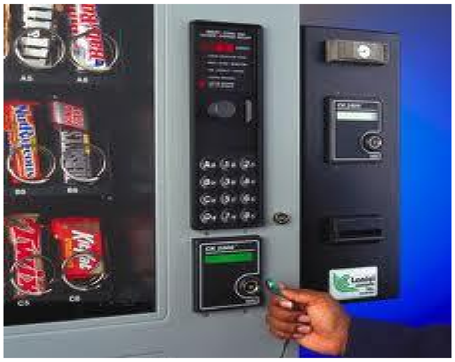


Figure 8

Access Control: The java ring becomes a personalized key to protected assets and information. By touching the correct key to an iButton reader, the desired event such as opening a lock is enabled. Java ring are perfect for various access control functions like access to buildings, computers, vechicles and equipments.

Figure 9

E-Cash: The Java ring can be an personalized token and acts like a small change for one or multiple applications. It enables to complete the transactions, like dispencing a candy bar or metering a prepaid volume of water. By using the java ring it eliminate to carry the small amounts of cash and it can service multiple, independent applications.

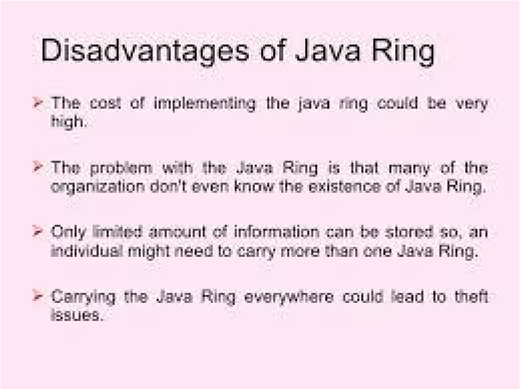
Figure 10

XI. DISADVANTAGES

Although the java ring can be the most secure storage medium for many industries the cost of implementing the system could be very high. Even though the iButton can be purchased for cheaper price in order to function it needs a receiver such as blue dot receptor which could be very expensive. Also it needs a

high level tools and method in order to program applications effectively, reliably and securely.

As such a java ring based system does not automatically allow user mobility. The problems with the java ring that many organization does not even know the existence of java ring. User mobility is only possible if every machine that the user accesses has a iButton.



Disadvantages of Java Ring

- The cost of implementing the java ring could be very high.
- The problem with the Java Ring is that many of the organization don't even know the existence of Java Ring.
- Only limited amount of information can be stored so, an individual might need to carry more than one Java Ring.
- Carrying the Java Ring everywhere could lead to theft issues.

Figure 11

XII. CONCLUSION

Java has significant advantages not only as a commercial language but also as a teaching language. It allows to learn the object oriented programming to the students without exposing them to the complexity of C++. Java might well be a language that most computer science departments could agree to use as an introductory language. This paper address one of the areas where more power is needed. It extends java with a mechanism for parametric polymorphism which allows the definition and implementation of generic abstractions.

REFERENCES

[1] http://www.maxim-ic.com/products/ibutton/ibuttons

[2] http://www.maxim-ic.com/products/1-wire/flash/overview/index.cfm

[3] http://www.javaworld.com/javaworld/jw-04-1998/jw-04-javadev.html

[4] http://electronics.howstuffworks.com/gadgets/home/digital-jewelry4.htm

[5] http://www.123eng.com/forum/viewtopic.php?p=158456

[6] pdfserv.maxim-ic.com/en/an/AN937.pdf

[7] http://findarticles.com/p/articles/mi m0EIN/is 1998 July 21/ai 20924045/?tag=content;col1

[8] http://en.wikipedia.org/wiki/1-Wire

[9] http://javaring.blogspot.com/

[10] http://www.maxim-ic.com/products/ibutton/software/crypto/fips140-1l3.pdf.

Knowledge Discovery in Data-Mining

Shivali[1], Joni Birla[2], Gurpreet[3]

[1,2,3]*Department of Computer Science &Engineering, Ganga Institute of Technology and Management, Kablana, Jhajjar, Haryana, INDIA*

Abstract- **Data mining (the analysis step of the "Knowledge Discovery in Databases" process, or KDD) an interdisciplinary subfield of computer science, is the computational process of discovering patterns in large data sets involving methods at the intersection of artificial intelligence, machine learning, statistics, and database systems. The overall goal of the data mining process is to extract information from a data set and transform it into an understandable structure for further use.**

A warehouse is a commercial building for storage of goods. It is manufacturers, importers, exporters, wholesalers,transport businesses, customs, etc. They are usually large plain buildings in industrial areas of cities and towns and villages.

I. INTRODUCTION

Advances in data gathering storage and distribution have created a need for computational tools and techniques to aid in data analysis. Data Mining and Knowledge Discovery in Databases (KDD) is a rapidly growing area of research and application that builds on techniques and theories from many fields including statistics databases pattern recognition and learning data visualization uncertainty modelling data warehousing and OLAP optimization and high performance computing. KDD is concerned with issues of scalability the multi-step knowledge discovery process for extracting useful patterns and models from raw data stores (including data cleaning and noise modelling) and issues of making discovered patterns understandable. Data Mining and Knowledge Discovery is intended to be the premier technical publication in the field providing a resource collecting relevant common methods and techniques and a forum for unifying the diverse constituent research communities. The journal publishes original technical papers in both the research and practice of DMKD surveys and tutorials of important areas and techniques and detailed descriptions of significant applications. Short application summaries are published in a special section. The journal accepts paper submissions of any work relevant to DMKD. A summary of the scope *of* Data Mining and Knowledge Discovery includes Theory and Foundational Issues: Data and knowledge representation; modelling of structured textual and multimedia data; uncertainty management; metrics of interestingness and utility of discovered knowledge; algorithmic complexity efficiency and scalability issues in data mining; statistics over massive data sets. Data Mining Methods: including classification clustering probabilistic modelling prediction and estimation dependency analysis search and optimization. Algorithms for data mining including spatial textual and multimedia data (e.g. the Web) scalability to large databases parallel and distributed data mining techniques and automated discovery agents. Knowledge Discovery Process: Data pre-processing for data mining including data cleaning selection efficient sampling and data reduction methods; evaluating consolidating and explaining discovered knowledge; data and knowledge visualization; interactive data exploration and discovery. Application Issues: Application case studies; data mining systems and tools; details of successes and failures of KDD; resource/knowledge discovery on the Web; privacy and security issues.

II. WHAT DOES KNOWLEDGE DISCOVERY IN DATABASES (KDD) MEAN?

Knowledge discovery in databases (KDD) is the process of discovering useful knowledge from a collection of data. This widely used data mining technique is a process that includes data preparation and selection, data cleansing, incorporating prior knowledge on data sets and interpreting accurate solutions from the observed results. Major KDD application areas include marketing, fraud detection, telecommunication and manufacturing.

III. ADVANCES IN KNOWLEDGE DISCOVERY AND DATA MINING

It brings together the latest research—in statistics, databases, machine learning, and artificial intelligence —that are part of the exciting and rapidly growing field of Knowledge Discovery and Data Mining. Topics covered include fundamental issues, classification and clustering, trend and deviation analysis, dependency modeling, integrated discovery systems, next generation database systems, and application case studies. The contributors include leading researchers and practitioners from academia, government laboratories, and private industry.

The last decade has seen an explosive growth in the generation and collection of data. Advances in data collection, widespread use of bar codes for most commercial products, and the computerization of many business and government transactions have flooded us with data and generated an urgent need for new techniques and tools that can intelligently and automatically assist in transforming this data into useful knowledge. This book is a timely and comprehensive overview of the new generation of techniques and tools for knowledge discovery in data.

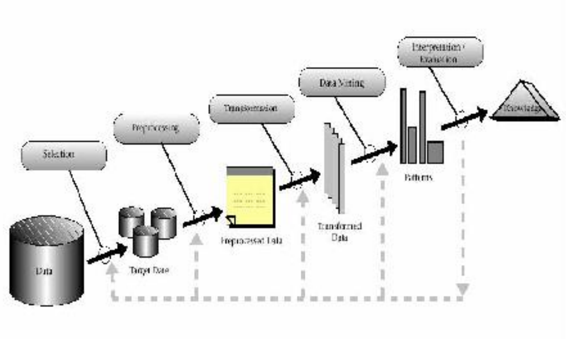


Fig 1. Knowledge Discovery Process

IV. WHAT IS THE KNOWLEDGE DISCOVERY PROCESS?

There is some confusion about the terms data mining, knowledge discovery, and knowledge discovery in databases, we first define them. Note, however, that many researchers and practitioners use

DM as a synonym for knowledge discovery; DM is also just one step of the KDP.

Data miningwas defined in just add here that DM is also known under many other names, including knowledge extraction, information discovery, information harvesting, data archeology, and data pattern processing.

The knowledge discovery process(KDP), also called knowledge discovery in databases, seeks new knowledge in some application domain. It is defined as the nontrivial process of identifying valid, novel, potentially useful, and ultimately understandable patterns in data. The process generalizes to non database sources of data, although it emphasizes databases as a primary source of data. It consists of many steps (one of them is DM), each attempting to complete a particular discovery task and each accomplished by the application of a discovery method. Knowledge discovery concerns the entire knowledge extraction process, including how data are stored and accessed, how to use efficient and scalable algorithms to analyze massive datasets, how to interpret and visualize the results, and how to model and support the interaction between human and machine. It also concerns support for learning and analyzing the application domain.

This defines the term knowledge extractionin a narrow sense. While the acknowledge that extracting knowledge from data can be accomplished through a variety of methods — some not even requiring the use of a computer —uses the term to refer to knowledge obtained from a database or from textual data via the knowledge discovery process.

V. STEPS OF THE KNOWLEDGE DISCOVERY IN DATABASES PROCESS

Data mining is actually the core step in Knowledge Discovery in Databases (KDD) process. Though KDD is used synonymously to represent data mining, both these are actually different. Some preprocessing steps before data mining and post processing steps after data mining are to be completed to transform the raw data as useful knowledge. Thus, data mining alone might not give you what you actually look for.

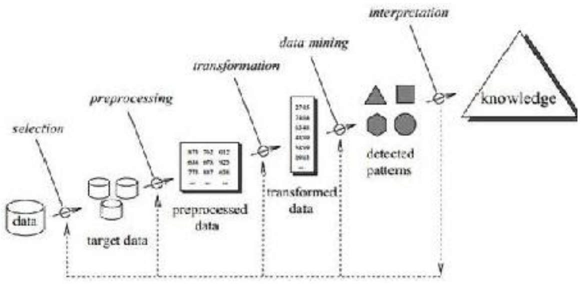


Fig 2. Data Mining process

KDD is an iterative process that transforms raw data into useful information. Different steps of Knowledge Discovery in Databases are:Understanding: The first step is understanding the requirements. We need to have a clear understanding about the application domain and your objectives, whether it is to improve your sales, predict stock market etc. It should also know whether you are going to describe your data or predict information.Selection of data set: Data mining is done on yourcurrent or past records. Thus, you should select a data set or subset of data, in other words data samples, on which you need to perform data analysis and get useful knowledge. We should have enough quantity of data to perform data mining.

A. *Data cleaning*

Data cleaning is the step where noise and irrelevant data are removed from the large data set. This is a very important preprocessing step because your outcome would be dependent on the quality of selected data. As part of data cleaning, you might have to remove duplicate records, enter logically correct values for missing records, remove unnecessary data fields, standardize data format, update data in a timely manner and so on.

B. *Data transformation*

With the help of dimensionality reduction or transformation methods, the number of effective variables is reduced and only useful features are selected to depict data more efficiently based on the goal of the task. In short, data is transformed into appropriate form making it ready for data mining step.

C. *Selection of data mining task*

Based on the objective of data mining, appropriate task is selected. Some common data mining tasks are classification, clustering, association rule discovery, sequential pattern discovery, regression and deviation detection. We can choose any of these tasks based on whether we need to predict information or describe information.

D. *Selection of data mining algorithm*

Appropriate method(s) is to be selected for looking for patterns from the data. You need to decide the model and parameters that might be appropriate for the method. Some popular data mining methods are decision trees and rules, relational learning models, example based methods etc.

E. *Data mining*

Data mining is the actual search for patterns from the data available using the selected data mining method.

F. *Pattern evaluation*

This is a post processing step in KDD which interprets mined patterns and relationships. If the pattern evaluated is not useful, then the process might again start from any of the previous steps, thus making KDD an iterative process.

G. *Knowledge consolidation:*

This is the final step in Knowledge Discovery in Databases (KDD). The knowledge discovered is consolidated and represented to the user in a simple and easy to understand format. Mostly, visualization techniques are being used to make users understand and interpret information.

Though these are the main steps in any KDD process, some of the steps could be done combined during the actual process. For example, considering the convenience, data selection and data transformation can be combined together. Even after presenting knowledge to the user, new data can be added to the data set or mining can be further refined or a different data mining method can be chosen to get more accurate results. Thus, KDD is completely an iterative process.

When we analyze different steps of KDD process, we could understand that we are mining data to get useful information or knowledge. Thus, knowledge mining would be the more appropriate term rather than data mining.

VI. KNOWLEDGE DISCOVERY PROCESS MODELS

Although the models usually emphasize independence from specific applications and tools, theycan be broadly divided into those that take into account industrial issues and those that do not.However, the academic models, which usually are not concerned with industrial issues, can bemade applicable relatively easily in the industrial setting and vice versa. We restrict our discussion to those models that have been popularized in the literature and have been used in real knowledgediscovery projects.

VII. ACADEMIC RESEARCH MODELS

The efforts to establish a KDP model were initiated in academia. In the mid-1990s, when the DMfield was being shaped, researchers started defining multistep procedures to guide users of DMtools in the complex knowledge discovery world. The main emphasis was to provide a sequenceof activities that would help to execute a KDP in an arbitrary domain. The two process modelsdeveloped in 1996 and 1998 are the nine-step model by Fayyad et al. and the eight-step modelby Anand and Buchner. Below we introduce the first of these, which is perceived as the leadingresearch model. The second model is summarized

VIII. KNOWLEDGE DISCOVERY PROCESS MODELS

The Fayyad et al. KDP model consists of nine steps, which are outlined as follows:

- Developing and understanding the application domain. This step includes learning the relevantprior knowledge and the goals of the end user of the discovered knowledge.
- Creating a target data set. Here the data miner selects a subset of variables (attributes) anddata points (examples) that will be used to perform discovery tasks. This step usually includesquerying the existing data to select the desired subset.
- Data cleaning and preprocessing. This step consists of removing outliers, dealing with noiseand missing values in the data, and accounting for time sequence information and knownchanges.
- Data reduction and projection. This step consists of finding useful attributes by applyingdimension reduction and transformation methods, and finding invariant representation ofthe data.
- Choosing the data mining task. Here the data miner matches the goals defined in Step 1 witha particular DM method, such as classification, regression, clustering, etc.
- Choosing the data mining algorithm. The data miner selects methods to search for patterns inthe data and decides which models and parameters of the methods used may be appropriate.
- Data mining. This step generates patterns in a particular representational form, such as classificationrules, decision trees, regression models, trends, etc.
- Interpreting mined patterns. Here the analyst performs visualization of the extracted patternsand models, and visualization of the data based on the extracted models.
- Consolidating discovered knowledge. The final step consists of incorporating the discoveredknowledge into the performance system, and documenting and reporting it to the interestedparties. This step may also include checking and resolving potential conflicts with previouslybelieved knowledge.

Notes: This process is iterative. The authors of this model declare that a number of loops betweenany two steps are usually executed, but they give no specific details. The model provides a detailed

technical description with respect to data analysis but lacks a description of business aspects. Thismodel has become a cornerstone of later models.

Major Applications: The nine-step model has been incorporated into a commercialknowledge discovery system called MineSet(for details, see Purple Insight Ltd)The model has been used in a number of different domains,including engineering, medicine, production, e-business, and software development.

IX. INDUSTRIAL MODELS

Industrial models quickly followed academic efforts. Several different approaches were undertaken,ranging from models proposed by individuals with extensive industrial experience tomodels proposed by large industrial consortiums. Two representative industrial models are thefive-step model by Cabena et al., with support from IBM and the industrialsix-step CRISP-DM model, developed by a large consortium of European companies. The latterhas become the leading industrial model, and is described in detail next.

The CRISP-DM (Cross-Industry Standard Process for Data Mining) was first established inthe late 1990s by four companies: Integral Solutions Ltd. (a provider of commercial data miningsolutions), NCR (a database provider), DaimlerChrysler (an automobile manufacturer), and OHRA(an insurance company). The last two companies served as data and case study sources.

The development of this process model enjoys strong industrial support. It has also beensupported by the ESPRIT program funded by the European Commission. The CRISP-DM SpecialInterest Group was created with the goal of supporting the developed process model. Currently,it includes over 300 users and tool and service providers.

X. THE KNOWLEDGE DISCOVERY PROCESS

The CRISP-DM KDP model consists of six steps, which are summarizedbelow:

- Business understanding. This step focuses on the understanding of objectives and requirementsfrom a business perspective. It also converts these into a DM problem definition, and designsa preliminary project plan to achieve the objectives. It is further broken into several substeps,namely,
    1) determination of business objectives,
    2) assessment of the situation,
    3) determination of DM goals, and
    4) generation of a project plan.
- Data understanding. This step starts with initial data collection and familiarization with thedata. Specific aims include identification of data quality problems, initial insights into the data, and detection of interesting data subsets. Data understanding is further broken down into– collection of initial data,

1) description of data,
2) exploration of data, and
3) verification of data quality.

- Data preparation. This step covers all activities needed to construct the final dataset, whichconstitutes the data that will be fed into DM tool(s) in the next step. It includes Table, record,and attribute selection; data cleaning; construction of new attributes; and transformation ofdata. It is divided into
    1) selection of data,
    2) cleansing of data,
    3) BusinessUnderstanding
    4) DataUnderstanding
    5) DataPreparation
    6) ModelingEvaluation
    7) DeploymentData
    8) construction of data,
    9) integration of data, and
    10) formatting of data substeps.
- Modeling. At this point, various modeling techniques are selected and applied. Modeling usuallyinvolves the use of several methods for the same DM problem type and the calibration of their parameters to optimal values. Since some methods may require a specific format for input data,often reiteration into the previous step is necessary. This step is subdivided into– selection of modeling technique(s),
    1) generation of test design,
    2) creation of models, and
    3) assessment of generated models.
- Evaluation. After one or more models have been built that have high quality from a dataanalysis perspective, the model is evaluated from a business objective perspective. A reviewof the steps executed to construct the model is also performed. A key objective is to determinewhether any important business issues have not been sufficiently considered. At the end of thisphase, a decision about the use of the DM results should be reached. The key substeps in thisstep include
    1) evaluation of the results,
    2) process review, and
    3) determination of the next step.
- Deployment. Now the discovered knowledge must be organized and presented in a way thatthe customer can use. Depending on the requirements, this step can be as simple as generatinga report or as complex as implementing a repeatable KDP. This step is further divided into– plan deployment,
    1) plan monitoring and maintenance,
    2) generation of final report, and
    3) review of the process substeps.

XI. CONCLUSION

In this paper,the characteristics ofData Mining of knowledge iswere studied. We have concentrated here on different angles of KDD mean, KDD process, Academic Research Models, Steps of Knowledge Discovery in Database, Knowledge Discover Process,Industrial Model, Knowledge discovery process.

REFERENCES

[1] RDB2RDF Working Group, Website: http://www.w3.org/2001/sw/rdb2rdf/ , charter: http://www.w3.org/2009/08/rdb2rdf-charter, R2RML: RDB to RDF Mapping Language:http://www.w3.org/TR/r2rml/

[2] LOD2 EU Deliverable 3.1.1 Knowledge Extraction from Structured Sources http://static.lod2.eu/Deliverables/deliverable-3.1.1.pdf

[3] "Life in the Linked Data Cloud". www.opencalais.com. Retrieved 2009-11-10. Wikipedia has a Linked Data twin called DBpedia. DBpedia has the same structured information as Wikipedia – but translated into a machine-readable format.

[4] Tim Berners-Lee (1998), "Relational Databases on the Semantic Web". Retrieved: February 20, 2011.

[6] Hu et al. (2007), “Discovering Simple Mappings Between Relational Database Schemas and Ontologies”, In Proc. of 6th International Semantic Web Conference (ISWC 2007), 2nd Asian Semantic Web Conference (ASWC 2007), LNCS 4825, pages 225-238, Busan, Korea, 11-15 November 2007. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.97.6934&rep=rep1&type=pdf

[7] R. Ghawi and N. Cullot (2007), "Database-to-Ontology Mapping Generation for Semantic Interoperability". In Third International Workshop on Database Interoperability (InterDB 2007).http://le2i.cnrs.fr/IMG/publications/InterDB07-Ghawi.pdf

[8] Li et al. (2005) "A Semi-automatic Ontology Acquisition Method for the Semantic Web", WAIM, volume 3739 of Lecture Notes in Computer Science, page 209-220. Springer.http://dx.doi.org/10.1007/11563952_19 .

LIFI – Light Fidelity – Feel The Speed

Sonia Tomer[1], Sonia Choudhary[2]

[1,2]*Department of Computer Science &Engineering, Ganga Institute of Technology and Management, Kablana, Jhajjar, Haryana, INDIA*

***Abstract*: Li-Fi Technology deals with large amount of speed of internet which is upto 10gbps. It is fast and cheap optical version of Wi-Fi. Li-Fi is a technology that uses the technology the light emitting diodes (LED) to transmit the data wirelessly . The data rate of Li-Fi can be compared with size and numbers of LED bulb used in it. In Li-Fi data rate can be increased by increasing number of LEDs. In this we also discussed its literature review and its working phenomenon. What the need for the development of the technology and drawbacks of the technology which is overcome by this technology. This paper include the review of the brief description of Li-fi and its advantages and future scope .**

***Keywords*— Li-Fi , Wi-Fi, Emitter, RF Driver , Data rate**

I. INTRODUCTION

Li-Fi means “Light Fidelity”. Li-Fi is fast and cheap optical version of Wi-Fi. Li-Fi is a technology that uses the technology the light emitting diodes (LED) to transmit the data wirelessly . The idea of Li-Fi was introduced by a German physicist, Harald Hass. The term Li-Fi was first used by Haas in his TED Global talk on Visible Light Communication. Li-fi based on visible light communication (VLC).VLC is a data communication medium ,Which uses the visible light between 400 Thz and 800 THz as optical carrier for data transmission. Li-Fi uses visible light communication in the range of 100Mbps.

Li-Fi can be thought of as a light-based Wi-Fi. That is, it uses light instead of radio waves to transmit information. And instead of Wi-Fi modems, Li-Fi would use transceiver-fitted LED lamps that can light a room as well as transmit and receive information. Since simple light bulbs are used, there can technically be any number of access points. Li-Fi can be the technology for the future where data will be transmitted through the light in a room. In this paper, the comparison is made between Wi-Fi and Li-Fi technology.

II. HISTORY

Professor Harald Haas, from the University of Edinburgh in the UK, is widely recognised as the original founder of Li-Fi. He is Chair man of Mobile Communications at the University of Edinburgh and co-founder of pure LiFi. The general term visible light communication (VLC), includes any use of the visible light portion of the electromagnetic spectrum to transmit information. The D-Light project at Edinburgh's Institute for Digital Communications was funded from January 2010 to January 2012. Mr. Haas promoted this technology in his 2011 TED Global talk and helped start a company to market it. In October 2011, companies and industry groups formed the Li-Fi Consortium, to promote high-speed optical wireless systems. VLC technology was exhibited in 2012 using Li-Fi. By August 2013, data rates of over 1.6 Gbit/s were demonstrated over a single colour LED. In September 2013, a press release said that Li-Fi or VLC systems in general, do not require line-of-sight conditions.

In October 2013, it was reported Chinese manufacturers were working on Li-Fi development kits. Philips lighting company has developed a VLC system for shoppers at stores. They have to download an app on their smartphone and then their smartphone works with the LEDs in the store. The LEDs can pinpoint where they are at in the store and give them corresponding coupons and information based on path where they are on and what they are looking at.

III. LIFI CONSTRUCTION AND WORKING

The Li-Fi product consists of three primary sub-assemblies:

- Emitter (including bulb).
- RF Driver (Radio Frequency)
- Power supply

3.1 FUNCTION OF THE BULB ASSEMBLY

At the heart of LIFI is the bulb sub-assembly where a sealed bulb is embedded in a dielectric material. The dielectric material serves two purposes: Waveguide, Electric field

3.2 RF DRIVER

Power amplifier (PA) assembly that uses an LDMOS (Laterally Diffused Metal Oxide Semiconductor)device. Converts electrical energy into RF power. The PA is designed for hardness and efficiency. The RF driver also contains controls circuit for digital and analog lighting controls.

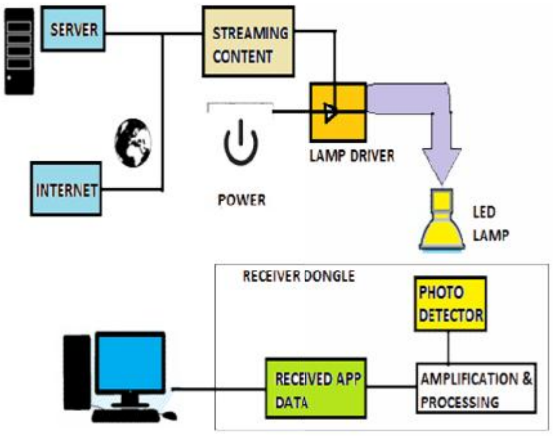


FIG. 1. ARCHITECTURE OF LI-FI

3.3 WORKING

Li-Fi offers an integrated light source that is straight forward to integrate into a projector. In this example LIFI consists of 5 primary sub-assemblies: Printed circuit board (PCB), RF power amplifier (PA), Bulb, Optics, Enclosure. The operational procedure of LIFI is very simple.If the LED is ON, you transmit a digital 1’s , if its OFF you transmit a 0’s. The LEDs can be switched ON and OFF very quickly, which gives nice opportunities for transmitting data.

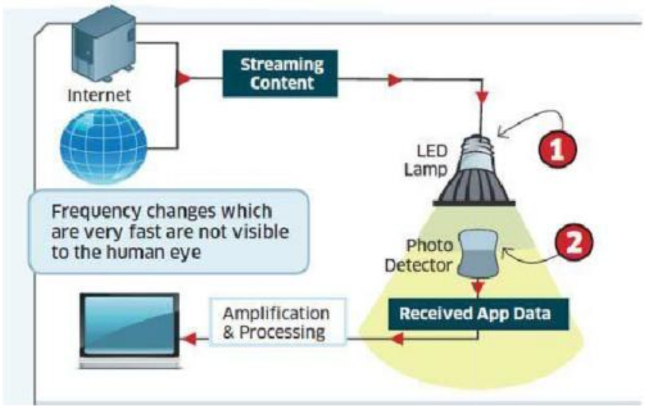

Internet
Streaming Content
LED Lamp
1
Frequency changes which are very fast are not visible to the human eye
Photo Detector
2
Amplification & Processing
Received App Data

Fig. - 2 Block diagram of Li-Fi system

IV. ISSUES REGARDING RADIO SPECTRUM

7.1 EFFICIENCY

There are 1.4 millions cellular radio base stations. Efficiecy of each base station is just 5%.

7.2 SECURITY

Radio waves can penetrate through walls and hence can be intercepted. Anyone with knowledge and bad intention can misuse it.

7.3 AVALILABLITY

We have to switch off mobiles in aircrafts.

It is also not advisable to use mobiles at petrol pumps.

7.4 CAPACITY

With the advent of new technologies like 3g ,4g we are running out of spectrum. That’s why radio waves are now becoming expensive.

V. WHY ONLY VLC

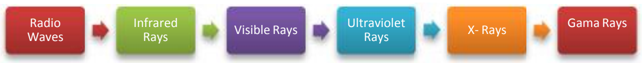


Fig 3

Gama rays cant be used as they could be dangerous.

X-rays have similar health issues. Ultraviolet light is good for place without people, but other wise dangerous for the human body. Infrared, due to eye safety regulation, can only bse used with low power. *HENCE WE LEFT WITH THE ONLY THE VISIBLE - LIGHT SPECTRUM.*

VI. COMPARISON BETWEEN LI-FI &WI-FI

Technology	Speed
Wi-Fi	150 Mbps
Bluetooth	3 Mbps
Li-fi	1 Gbps

Table I :Comparison of transfer speed of various wireless technologies.

VII. ADVANTAGES OF LI-FI

***Capacity**:*

10000 times more spectrum than RADIO WAVES. Light boxes are already present, so infrastructure is available already and installed.

Availability:

Light is present everywhere.

Data is present where light is present

Efficiency:

Highly efficient because LED consumes less energy

VIII. FUTURE DEVELOPMENTS AND FUTURE APPLICATIONS

The concept of Li-Fi is currently attracting a great deal of interest.It is Efficient alternative to radio-based wireless.

Li-Fi is an emerging technology which is quick and reliable. Air waves are clogged so let’s use light waves.

So lets proceed to LI FI for a brighter and greener future.

Some Future Applications of Li-Fi are:-

8.1 Education systems:

Li-Fi is the latest technology that can provide fastest

speed internet access.

So, it can replace Wi-Fi at educational institutions and at companies so that all the people can make use of Li-Fi with the same speed intended in a particular area.

8.2 Medical Applications: Operation theatres do not allow Wi-Fi due to radiation concerns. Usage of

Wi-Fi at hospitals blocks the signals for monitoring equipments. So, it may be hazardous to the patient's health. To overcome from this problem , Li-Fi can be used to accessing internet and to control medical equipments. This can even be beneficial for robotic surgeries and other automated procedures.

*8.3 In Aircrafts***:** Li-Fi can easily provide high speed internet via every light source. The passengers travelling in aircrafts get access to low speed internet at a very high rate. In aircrafts Li-Fi can be used for data transmission.

*8.4 Disaster management***:** Li-Fi can be used as a

powerful means of communication in times of disaster such as earthquake

VALUES OF LI-FI

- CHEAPER THAN WI-FI.
- No more monthly broadband bills.
- Theoretical speed up to 1 gb per second.
- A free band that does not need license.
- less time & energy consumption

IX. CONCLUSION

- The possibilities are numerous and can be explored further.
- If this technology can be put into practical use, every bulb can be used something like a Wi-Fi hotspot.

- we will proceed toward the cleaner, greener, safer and brighter future.
- This may solve issues such as the shortage of radio-frequency bandwidth.
- Allows internet where traditional radio based wireless isn't allowed such as aircraft or hospitals.
- This concept promises to solve issues such as the shortage of radio-frequency bandwidth.

REFERENCES

[1]. http://en.wikipedia.org/wiki/Li-Fi
[2]. seminarprojects.com/s/seminar-report-on-Li-Fi
[3]. http://teleinfobd.blogspot.in/2012/01/what-is-lifi.html
[4]. technopits.blogspot.comtechnology.cgap.org/2012/01/a-lifi-world
[5]. www.lificonsortium.org
[6]. the-gadgeteer.com/2011/08/LI-FI

Linux Network Security Access & Monitoring Service Tools

Mahesh Kumar [1]

[1] *Department of Computer Science & Engineering, Ganga Institute of Technology and Management, Kablana, Jhajjar, Haryana, INDIA*

Abstract--It has been recognized that securing applications is only half of the battle: a computer system must also employ security policies at the OS level, and the current model of user vs. administrator that we find in standard Unix is insufficient. For the basic security features, Linux has password authentication, file system discretionary access control, and security auditing. These three fundamental features are necessary to achieve a security evaluation at the C2 level [4]. Most commercial server-level operating systems, including AIX (IBM), Windows NT, and Solaris, have been certified to this C2 level. Generally speaking workstations/servers are used by people that don't really care about the underlying technology, they just want to get their work done and retrieve their email in a timely fashion. There are however many users that will have the ability to modify their workstation, for better or worse (install packet sniffers, warez ftp sites, www servers, irc bots, etc). To add to this most users have physical access to their workstations, meaning you really have to lock them down if you want to do it right.

***Keywords*:- *Security, Linux OS*, Server, Security, monitoring tool**

I. INTRODUCTION

By expanding the basic standard security features we have:

- User and group separation
- File system security
- Audit trails
- PAM authentication

A. User and Group Separation

User accounts are used to verify the identity of the person using a computer system. By checking the identity of a user through username and password credentials, the system is able to determine if the user is permitted to log into the system and, if so, which resources the user is allowed to access.

Groups are logical constructs that can be used to group user accounts together for a particular purpose. For example, if a company has a group of system administrators, they can all be placed in a system administrator group with permission to access key resources of the OS. In addition, through group creation and assignment of privileges, access to restricted resources can be controlled for those who need them and denied to others.

The ability for a user to access a machine is determined by whether or not that user's account exists. Access to an application or file is granted based on the permission settings for the file. This helps to ensure the integrity of sensitive information and key resources against accidental or purposeful damage by users.

After a normal user account is created, the user can log into the system and access any applications or files they are permitted to access. Linux determines whether or not a user or group can access these resources based on the permissions assigned to them.

There are three permissions for files, directories, and applications. Table 1 lists the symbols used to indicate each of them. Each of the three permissions is assigned to three defined categories of users. The categories are listed in Table 2.

TABLE 1.

Permission character symbols

Symbol	**Description**
r	Indicates that a given category of user can **read** a file.
w	Indicates that a given category of user can **write** to a file.
x	Indicates that a given category of user can **execute** the file.
-	A fourth symbol indicates that no access is permitted.

TABLE 2.

PERMISSION CATEGORIES

Category	**Description**
Owner	The owner of the file or application.
Group	The group that owns the file or application.
Everyone	All users with access to the system.

One can easily view the permissions for a file by invoking a long format listing using the command ls -l. For instance, if the user kambing creates an executable file named foo, the output of the command ls -l foo would look something like this:

```
-rwxrwxr-x 1 kambing kambing 0 Sep 2 12:25 foo
```

The permissions for this file are listed at the start of the line, starting with set of rwx.

- This first set of symbols defines owner access.
- The next set of rwx symbols define group access,
- The last set of symbols defining access permitted for all other users.

This listing indicates that the file is readable, writable, and executable by the user who owns the file (user kambing) as well as the group owning the file (which is a group named kambing). The file is also world-readable and world-executable, but not world-writable.

II. FILE SYSTEM SECURITY

A very true statement of a UNIX/Linux system, everything is a file; if something is not a file, it is a process. Most files are just files, called regular files; they contain normal data, for example text files, executable files or programs, input to or output from a program and so on. While it is practically safe to say that everything you encounter on a Linux system is a file, there are some exceptions as listed below:

- Directories: files that are lists of other files.
- Special files: the mechanism used for input and output. Most special files are in /dev for example USB and CD-ROM.
- Links: a system to make a file or directory visible in multiple parts of the system's file tree. It is a shortcut.
- (Domain) sockets: a special file type, similar to TCP/IP sockets, providing inter-process networking protected by the file system's access control.
- Named pipes: act more or less like sockets and form a way for processes to communicate with each other, without using network socket semantics.

e following table gives an overview of the characters ermining the file type:

TABLE 3.

FILE TYPES CHARACTER SYMBOLS

Symbol	Meaning
-	Regular file
d	Directory
l	Link
c	Special file
s	Socket
p	Named pipe
b	Block device

On Linux system, every file is owned by a user and a group user. There is also a third category of users, those that are not the user owner and don't belong to the group owning the file. For each category of users, read, write and execute permissions can be granted or denied.

The long option to list files using the ls -l command, also displays file permissions for these three user categories; they are indicated by the nine characters that follow the first character, which is the file type indicator at the beginning of the file properties line. As seen in the following examples, the first three characters in this series of nine display access rights for the actual user that owns the file.

```
 ls -l Mine
-rw-rw-r-- 1 mike users  5 Jul 15 12:39 Mine
ls -l /bin/ls
-rwxr-xr-x 1 root root 45948 Aug 10 15:01 /bin/ls*
```

The next three are for the group owner of the file, the last three for other users. The permissions are always in the same order: read, write, execute for the user, the group and the others. The first file is a regular file (first dash). Users with user name mike or users belonging to the group users can read and write (change/move/delete) the file, but they can't execute it (second and third dash). All other users are only allowed to read this file, but they can't write or execute it (fourth and fifth dash).

The second example is an executable file, the difference is everybody can run this program, but you need to be root to change it.

For easy use with commands, both access rights or modes and user groups have a code shown in Table 4 and 5.

TABLE 4.

ACCESS MODE CODES

Code	Meaning
0 or -	The access right that is supposed to be on this place is not granted.
4 or r	read access is granted to the user category defined in this place
2 or w	write permission is granted to the user category defined in this place
1 or x	execute permission is granted to the user category defined in this place

TABLE 5.

USER GROUP CODES

Code	Meaning
u	user permissions
g	group permissions
o	permissions for others

This straight forward scheme is applied very strictly, which allows a high level of security even without network security. Among other functions, the security scheme takes care of user access to programs; it can serve files on a need-to-know basis or least privilege and protect sensitive data such as home directories and system configuration files. We can use the chmod command to modify the file permission, changing of the access mode of a file. The chmod command can be used with alphanumeric or numeric options, whatever you like best. The following shows the examples.

```
>/hello
bash: ./hello: bad interpreter: Permission denied
>cat hello
```

```
#!/bin/bash
echo "Hello, World"
>ls -l hello
-rw-rw-r-- 1 mike  mike 32 Jul 1 16:29 hello
>chmod u+x hello
>./hello
Hello, World
>ls -l hello
-rwxrw-r-- 1 mike mike 32 Jul 1 16:29 hello*
```

The + and - operators are used to grant or deny a given right to a given group. Combinations separated by commas are allowed. The following is another example, which makes the file from the previous example a private file to user mike:

```
>chmod u+rwx,go-rwx hello
>ls -l hello
-rwx------ 1 mike mike 32 Jan 15 16:29 hello*
```

If you encounter problems resulting in an error message saying that permission is denied, it is usually a problem with access rights in most cases.

When using chmod with numeric arguments, the values for each granted access right have to be counted together per group. Thus we get a 3-digit number, which is the symbolic value for the settings chmod has to make. The following table lists the most common combinations:

TABLE 5.

FILE PROTECTION WITH CHMOD

Command	**Meaning**
chmod 400 file	To protect a file against accidental overwriting.
chmod 500 directory	To protect you from accidentally removing, renaming or moving files from this directory.
Chmod 600 file	A private file only changeable by the user who entered this command.
chmod 644 file	A publicly readable file that can only be changed by the issuing user.
chmod 660 file	Users belonging to your group can change this file; others don't have any access to it at all.
chmod 700 file	Protects a file against any access from other users, while the issuing user still has full access.
chmod 755 directory	For files that should be readable and executable by others, but only changeable by the issuing user.
chmod 775 file	Standard file sharing mode for a group.
chmod 777 file	Everybody can do everything to this file.

If you enter a number with less than three digits as an argument to chmod, omitted characters are replaced with zeros starting from the left. There is actually a fourth digit on Linux systems that precedes the first three and sets special access modes.

A. The File Mask

When a new file is saved somewhere, it is first subjected to the standard security procedure. Files without permissions don't exist on Linux. The standard file permission is determined by the mask for new file creation. The value of this mask can be displayed using the umask command:

```
>umask
0002
```

Instead of adding the symbolic values to each other, as with chmod, for calculating the permission on a new file they need to be subtracted from the total possible access rights. In the example above, however, we see 4 digits displayed, yet there are only 3 permission categories: user, group and other. The first zero is part of the special file attributes settings. It might just as well be that this first zero is not displayed on your system when entering the umask command and that you only see 3 numbers representing the default file creation mask.

Each UNIX-like system has a system function for creating new files, which is called each time a user uses a program that creates new files, for instance, when downloading a file from the Internet, when saving a new text document. This function creates both new files and new directories. Full read, write and execute permission is granted to everybody when creating a new directory. When creating a new file, this function will grant read and write permissions for everybody, but set execute permissions to none for all user categories. In this case, before the mask is applied, a directory has permissions 777 or rwxrwxrwx, a plain file 666 or rw-rw-rw-.

The umask value is subtracted from these default permissions after the function has created the new file or directory. Thus, a directory will have permissions of 775 by default, a file 664, if the mask value is (0)002. This is demonstrated in the following examples:

```
>mkdir newdir
>ls -ld newdir
drwxrwxr-x 2 mike mike 2096 Jul 28 13:45 newdir/
>touch newfile
>ls -l newfile
-rw-rw-r-- 1 mike mike 0 Jul 28 13:52 newfile
```

A directory gets more permission by default, it always has the execute permission. If it wouldn't have that, it would not be accessible.

If you log in to another group using the newgrp command, the mask remains unchanged. Thus, if it is set to 002, files and directories that you create while being in the new group will also be accessible to the other members of that group; you don't have to use chmod. The root user usually has stricter default file creation permissions as shown below:

```
[root@tenouk root]# umask 022
```

These defaults are set system-wide in the shell resource configuration files, for instance /etc/bashrc or /etc/profile. You can change them in your own shell configuration file.

III. AUDIT TRAILS

Linux kernel 2.6 comes with auditd daemon. It's responsible for writing audit records to the disk. During startup, the rules in /etc/audit.rules are read by this daemon. You can open /etc/audit.rules file and make changes such as setup audit file log location and other option. The default file is good enough to get started with auditd. In order to use audit facility you need to use following utilities:

TABLE 6.

AUDIT UTILITY

Utility	Description
auditctl	A command to assist controlling the kernel's audit system. You can get status, and add or delete rules into kernel audit system
ausearch	A command that can query the audit daemon logs based for events based on different search criteria.
aureport	A tool that produces summary reports of the audit system logs.

IV. Pluggable Authentication Modules authentication (PAM)

PAM [5] was invented by SUN Microsystems. Linux-PAM provides a flexible mechanism for authenticating users. It consists of a set of libraries that handle the authentication tasks of applications on the system. The library provides a stable general interface to which privilege-granting programs (such as login) defer to perform standard authentication tasks.

Historically, authentication of Linux users relied on the input of a password which was checked with the one stored in /etc/passwd. At each improvement (e.g. /etc/shadow, one-time passwords) each program (e.g. login, ftp) had to be rewritten. PAM is a more flexible user authentication mechanism. Programs supporting PAM must dynamically link themselves to the modules in charge of authentication. The administrator is in charge of the configuration and the attachment order of modules. All applications using PAM must have a configuration file in /etc/pam.d. Each file is composed of four columns:

TABLE 7.

PAM'S PAM.D CONTENT

Column	Description
Module type	▪ auth: user authentication ▪ account: user restriction (e.g.: hour restriction) ▪ session: tasks to perform at login and logout e.g.: mounting directories ▪ password: update of the user authentication token
success control	▪ required: a least one of the required modules ▪ requisite: all the requisite modules ▪ sufficient: only one sufficient module ▪ optional: a least one of the required modules is necessary if no other has succeeded
path to the module	Usually /lib/security.
optional arguments	-

Other PAM functionalities are listed in the following Table.

TABLE 8.

OTHER PAM FUNCTIONALITY

Functionality	Description
/etc/pam.d/other file	Provides default configuration for all modules not specified in the configuration file of the application.
pam_cracklib	Uses the cracklib library to check the "strength" of a password and to check it was not built based on the old one.
pam_limits	This module can restrict, depending on the user and/or group, the number of simultaneous processes, CPU time, the number of files simultaneously opened, their size, and the maximum number of simultaneous connections. The configuration file is: /etc/security/limits.conf
pam_rootok	Enables root to access a service without using his password. To be used with chfn or chsh and not with login.
pam_time	Control the access time. The configuration file is: /etc/security/time.conf.
pam_wheel	Allow access to root only to users of the wheel group. For use with su.
pam_cap	This module can force all privileges to a user.

Keep in mind that PAM however does not itself have an authenticated access to the kernel.

LINUX SECURITY EXTENSIONS

The Linux family of products has provided a highly secure environment since its original delivery in early 2002. The features discussed in the following sections have been added to the Linux OS. For example, the Red Hat Enterprise Linux Update 3, shipped in September 2004 contains:

- ExecShield [6] – With the **N**o e**X**ecute (NX) [7], [8], or e**X**ecute **D**isable (XD) and Segmentation features.
- Position Independent Executables (PIE) [9]

Then, in Red Hat Enterprise Linux v.4, shipped in February 2005 contains the following security features:

- SecurityEnhanced Linux (SELinux) [10]
- Compiler and library enhancements [11]
- Advanced glibc memory corruption checker [11]
- Secure version of the printf and other string manipulation functions. [11]
- gcc buffer bound checking [11]

In term of the Linux OS security breaches, most of the problems originated from the buffer overflow issue. The buffer overflow exploits unprotected and or unchecked fixed sized buffers, overwriting the area beyond it. The overwritten area may be filled with the malicious codes, containing code that pointing to the customized return address. There are many buffer locations in the memory area. It is used to temporarily store data.

A. *ExecShield*

The ExecShield supports two technologies that protect application from being compromised by most of the buffer exploit types. The goal of these features is to prevent code that is maliciously written in the data areas of an application from being executed. These NX/XD and Segmentation features use different techniques but to achieve the similar result. PAX [12], [13], [14] is similar, earlier technology that will not be discussed here.

1) *The NX/XD:*

The NX term is used by AMD for its Opteron/Athlon64 processors, while the XD is used by Intel for its Itanium2 and the x86/EM64T processors. These capabilities provides a new memory management feature that that allows individual pages of an application's memory to be marked as non executable. The problem is, previously the only level of control over memory pages was read and write. However, a page that was enabled for read could also be executed.

This meant that data areas such as the stack, heap and I/O buffers, which are typically only used for read/write could also be used to execute codes. It is a common form of exploit that involves writing code in a stack buffer and then executing it. So the ability to disable execution enhances the application and system security. The NX/XD support is available for most new processors including the recent model Intel x86 CPUs.

V. ADMINISTRATIVE MONITORING TOOLS ACCESS

A. *Telnet*

Telnet is by far the oldest and well known remote access tool, virtually ever Unix ships with it, and even systems such as NT support it. Telnet is really only useful if you can administer the system from a command prompt (something NT isn't so great at), which makes it perfect for Unix. Telnet is incredibly insecure, passwords and usernames as well as the session data flies around as plain text and is a favourite target for sniffers. Telnet comes with all Linux distributions. You should never ever use stock telnet to remotely administer a system.

B. *SSL Telnet*

SSL Telnet is telnet with the addition of SSL encryption which makes it much safer and far more secure. Using X.509 certificates (also referred to as personal certificates) you can easily administer remote systems. Unlike systems such as SSH, SSL Telnet is completely GNU and free for all use. You can get SSL Telnet server and client from: ftp://ftp.replay.com/.

C. *SSH*

SSH was originally free but is now under a commercial license, it does however have many features that make it worthwhile. It supports several forms of authentication (password, rhosts based, RSA keys), allows you to redirect ports, and easily configure which users are allowed to login using it. SSH is available from: ftp://ftp.replay.com/. If you are going to use it commercially, or want the latest version you should head over to: http://www.ssh.fi/.

D. *LSH*

LSH is a free implementation of the SSH protocol, LSH is GNU licensed and is starting to look like the alternative (commercially speaking) to SSH (which is not free anymore). You can download it from: http://www.net.lut.ac.uk/psst/, please note it is under development.

E. *REXEC*

REXEC is one of the older remote UNIX utilities, it allows you to execute commands on a remote system, however it is seriously flawed in that it has no real security model. Security is achieved via the use of "rhosts" files, which specify which hosts/etc may run commands, this however is prone to spoofing and other forms of exploitation. You should never ever use stock REXEC to remotely administer a system.

F. *Slush*

Slush is based on OpenSSL and supports X.509 certificates currently, which for a large organization is a much better (and saner) bet then trying to remember several dozen passwords on various servers. Slush is GPL, but not finished yet (it implements most of the required functionality to be useful, but has limits). On the other hand it is based completely in open source software making the possibilities of backdoors/etc remote. Ultimately it could replace SSH with something much nicer. You can get it from: http://violet.ibs.com.au/slush/.

G. *NSH*

NSH is a commercial product with all the bells and whistles (and I do mean all). It’s got built in support for encryption, so it’s relatively safe to use (I cannot really verify this as it isn’t open source). Ease of use is high, you cd //computername and that ‘logs’ you into that computer, you can then easily copy/modify/etc. files, run ps and get the process listing for that computer, etc. NSH also has a Perl module available, making scripting of commands pretty simple, and is ideal for administering many like systems (such as workstations). In addition to this NSH is available on multiple platforms (Linux, BSD, Irix, etc.). NSH is available from:

http://www.networkshell.com/, and 30 day evaluation versions are easily downloaded.

H. *Fsh*

Fsh is stands for “Fast remote command execution” and is similar in concept to rsh/rcp. It avoids the expense of constantly creating encrypted sessions by bring up an encrypted tunnel using ssh or lsh, and running all the commands over it. You can get it from:

http://www.lysator.liu.se/fsh/.

I. secsh

secsh (Secure Shell) provides another layer of login security, once you have logged in via ssh or SSL telnet you are prompted for another password, if you get it wrong secsh kills off the login attempt. You can get secsh at: http://www.leenux.com/scripts/.

J. *YaST*

YaST (Yet Another Setup Tool) is a rather nice command line graphical interface (very similar to scoadmin) that provides an easy interface to most administrative tasks. It does not however have any provisions for giving users limited access, so it is really only useful for cutting down on errors, and allowing new users to administer their systems. Another problem is unlike Linuxconf it is not network aware, meaning you must log into each system you want to manipulate.

K. *sudo*

Sudo gives a user setuid access to a program(s), and you can specify which host(s) they are allowed to login from (or not) and have sudo access (thus if someone breaks into an account, but you have it locked down damage is minimized). You can specify what user a command will run as, giving you a relatively fine degree of control. If granting users access be sure to specify the hosts they are allowed to log in from and execute sudo, as well give the full pathnames to binaries, it can save you significant grief in the long run (i.e. if I give a user setuid access to "adduser", there is nothing to stop them editing their path statement, and copying "bash" into /tmp). This tool is very similar to super but with slightly less fine control.

Sudo is available for most distributions as a core package or a contributed package. Sudo is available at: http://www.courtesan.com/sudo/ just in case your distribution doesn’t ship with it Sudo allows you to define groups of hosts, groups of commands, and groups of users, making long term administration simpler. Several /etc/sudoers examples:

Give the user ‘seifried’ full access seifried ALL=(ALL) ALL

Create a group of users, a group of hosts, and allow then to shutdown the server as root Host_Alias WORKSTATIONS=localhost, station1, station2

User_Alias SHUTDOWNUSERS=bob, mary, jane

Cmnd_Alias REBOOT=halt, reboot, sync

Runas_Alias REBOOTUSER=admin

SHUTDOWNUSERS WORKSTATIONS=(REBOOTUSER) REBOOT

L. *Super*

Super is one of the very few tools that can actually be used to give certain users (and groups) varied levels of access to system administration. In addition to this you can specify times and allow access to scripts, giving setuid access to even ordinary commands could have unexpected consequences (any editor, any file manipulation tools like chown, chmod, even tools like lp could compromise parts of the system). Debian ships with super, and there are rpm's available in the contrib directory (buildhost is listed as "localhost", you might want to find the source and compile it yourself). This is a very powerful tool (it puts sudo to shame), but requires a significant amount of effort to implement properly, I think it is worth the effort though. The head end distribution site for super is at: ftp://ftp.ucolick.org/pub/users/will/.

M. *Remote*

Webmin

Webmin is a (currently) a non commercial web based administrative tool. It’s a set of perl scripts with a self contained www server that you access using a www browser, it has modules for most system administration functions, although some are a bit temperamental. One of my favourite features is the fact is that it holds it’s own username and passwords for access to webmin, and you can customize what each user gets access to (i.e. user1 can administer users, user2 can reboot the server, and user3 can fiddle with the apache settings). Webmin is available at: http://www.webmin.com/.

N. *Linuxconf*

Linuxconf is a general purpose Linux administration tool that is usable from the command line, from within X, or via it's built in www server. It is my preferred tool for automated system administration (I primarily use it for doing strange network configurations), as it is relatively light from the command line (it is actually split up into several modules). From within X it provides an overall view of everything that can be configured (PPP, users, disks, etc.). To use it via a www browser you must first run Linuxconf on the machine and add the host(s) or network(s) you want to allow to connect (Conf > Misc > Linuxconf network access), save changes and quit, then when you connect to the machine (by default Linuxconf runs on port 98) you must enter a username and password, it only accepts root as the account, and Linuxconf doesn't support any encryption, so I would have to recommend very strongly against using this feature across public networks. Linuxconf ships with RedHat Linux and is available at: http://www.solucorp.qc.ca/linuxconf/.

Linuxconf also doesn't seem to ship with any man pages/etc, the help is contained internally which is slightly irritating.

O. *COAS*

The COAS project (Caldera Open Administration System) is a very ambitious project to

provide an open framework for administering systems, from a command line (with semi

graphical interface), from within X (using the qt widget set) to the web. It abstracts the actual

configuration data by providing a middle layer, thus making it suitable for use on disparate Linux platforms. Version 1.0 was just released, so it looks like Caldera is finally pushing ahead with it. The COAS site is at: http://www.coas.org/.

P. *Log files and other forms of monitoring*

One integral part of any UNIX system are the logging facilities. The majority of logging in Linux is provided by two main programs, sysklogd and klogd, the first providing logging services to programs and applications, the second providing logging capability to the Linux kernel. Klogd actually sends most messages to the syslogd facility but will on occasion pop up messages at the console (i.e. kernel panics). Sysklogd actually handles the task of processing most messages and sending them to the appropriate file or device, this is configured from within /etc/syslog.conf. By default most logging to files takes place in /var/log/, and generally speaking programs that handle their own logging (such as apache) log to /var/log/progname/, this centralizes the log files and makes it easier to place them on a separate partition (some attacks can fill your logs quite quickly, and a full / partition is no fun). Additionally there are programs that handle their own interval logging, one of the more interesting being the bash command shell. By default bash keeps a history file of commands executed in ~username/.bash_history, this file can make for extremely interesting reading, as oftentimes many admins will accidentally type their passwords in at the command line. Apache handles all of it's logging internally, configurable from httpd.conf and extremely

flexible with the release of Apache 1.3.6 (it supports conditional logging). Sendmail handles it's logging requirements via syslogd but also has the option (via the command line -X switch) of logging all SMTP transactions straight to a file. This is highly inadvisable as the file will grow enormous in a short span of time, but is useful for debugging. See the sections in network security on apache and sendmail for more information.

Q. *sysklogd / klogd*

In a nutshell klogd handles kernel messages, depending on your setup this can range from almost none to a great deal if for example you turn on process accounting. It then passes most messages to syslogd for actual handling, i.e. placement in a logfile. the man pages for sysklogd, klogd and syslog.conf are pretty good with clear examples. One exceedingly powerful and often overlooked ability of syslog is to log messages to a remote host running syslog. Since you can define multiple locations for syslog messages (i.e. send all kern messages to the /var/log/messages file, and to console, and to a remote host or multiple remote hosts) this allows you to centralize logging to a single host and easily check log files for security violations and other strangeness. There are several problems with syslogd and klogd however, the primary ones being the ease of which once an attacker has gained root access to deleting/modifying log files, there is no authentication built into the standard logging facilities.

The standard log files that are usually defined in syslog.conf are:

/var/log/messages

/var/log/secure

/var/log/maillog

/var/log/spooler

The first one (messages) gets the majority of information typically, user login's, TCP_WRAPPERS dumps information here, IP firewall packet logging typically dumps information here and so on. The second typically records entries for events like users

changing their UID/GID (via su, sudo, etc.), failed attempts when passwords are required and so on. The maillog file typically holds entries for every pop/imap connection (user login and 30 logout), and the header of each piece of email that goes in or out of the system (from whom, to where, msgid, status, and so on). The spooler file is not often used anymore as the number

of people running usenet or uucp has plummeted, uucp has been basically replaced with ftp and email, and most usenet servers are typically extremely powerful machines to handle a full, or even partial newsfeed, meaning there aren't many of them (typically one per ISP or more depending on size). Most home users and small/medium sized business will not (and should not in my opinion) run a usenet server, the amount of bandwidth and machine power required is phenomenal, let alone the security risks.

You can also define additional log files, for example you could add:

```
kern.* /var/log/kernel-log
```

And/or you can log to a separate log host:

```
*.emerg @syslog-host
mail.* @mail-log-host
```

Which would result in all kernel messages being logged to /var/log/kernel-log, this is useful on headless servers since by default kernel messages go to /dev/console (i.e. someone logged in at the machines). In the second case all emergency messages would be logged to the host “syslog-host”, and all the mail log files would be sent to the “mail-log-host” server, allowing you to easily maintain centralized log files of various services.

R. *secure-syslog*

The major problem with syslog however is that tampering with log files is trivial. There is however a secure versions of syslogd, available at http://www.core-sdi.com/ssyslog/ (these

guys generally make good tools and have a good reputation, in any case it is open source

software for those of you truly paranoid). This allows you to cyrptographically sign logs and other ensure they haven’t been tampered with, ultimately however an attacker can still delete the log files so it is a good idea to send them to another host, especially in the case of a firewall to prevent the hard drive being filled up.

next generation syslog Another alternative is "syslog-ng" (Next Generation Syslog), which seems much more customizable then either syslog or secure syslog, it supports digital signatures to prevent log tampering, and can filter based on content of the message, not just the facility it comes from or priority (something that is very useful for cutting down on volume). Syslog-ng is available at: http://www.balabit.hu/products/syslog-ng.html.

S. *Log monitoring*

1) *Logcheck:*

logcheck will go through the messages file (and others) on a regular basis (invoked via crontab usually) and email out a report of any suspicious activity. It is easily configurable with several 'classes' of items, active penetration attempts which is screams about immediately, bad activity, and activity to be ignored (for example DNS server statistics or SSH rekeying). Logcheck is available from: http://www.psionic.com/abacus/logcheck/.

2) *Colorlogs:*

colorlogs will color code log lines allowing you to easily spot bad activity. It is of somewhat questionable value however as I know very few people that stare at log files on an on-going basis. You can get it at: http://www.resentment.org/projects/colorlogs/.

3) *WOTS*

WOTS collects log files from multiple sources and will generate reports or take action based on what you tell it to do. WOTS looks for regular expressions you define and then executes the commands you list (mail a report, sound an alert, etc.). WOTS requires you have perl installed and is available from: http://www.vcpc.univie.ac.at/~tc/tools/.

4) *Swatch:*

swatch is very similar to WOTS, and the log files configuration is very similar. You can download swatch from: ftp://ftp.stanford.edu/general/security-tools/swatch/.

T. *Kernel logging*

1) *Auditd:*

auditd allows you to use the kernel logging facilities (a very powerful tool). You can log mail messages, system events and the normal items that syslog would cover, but in addition to this you can cover events such as specific users opening files, the execution of programs, of setuid programs, and so on. If you need a solid audit trail then this is the tool for you, you can get it at: ftp://ftp.hert.org/pub/linux/auditd/.

U. *Shell logging*

1) *bash*

I will also cover bash since it is the default shell in most Linux installations, and thus it's logging facilities are generally used. bash has a large number of variables you can configure at or during run time that modify how it behaves, everything from the command prompt style to how many lines to keep in the log file.

2) HISTFILE

name of the history file, by default it is ~username/.bash_history

3) HISTFILESIZE

maximum number of commands to keep in the file, it rotates them as needed.

4) HISTSIZE

the number of commands to remember (i.e. when you use the up arrow key).

The variables are typically set in /etc/profile, which configures bash globally for all users, the values can however be over-ridden by users with the ~username/.bash_profile file, and/or by manually using the export command to set variables such as export EDITOR=emacs. This is one of the reasons user directories should not be world readable, as the bash_history file can contain a lot of valuable information to a hostile party. You can also set the file itself non world readable, set your .bash_profile not to log, set the file non writeable (thus denying bash the ability to write and log to it) or link it to /dev/null (this is almost always a sure sign of suspicious user activity, or a paranoid user). For the root account I would highly

VI. CONCLUSION

The fundamental Linux securities not change so much however there are many Linux security and monitoring extensions enhancement tools. These extensions and tools seem overlapped in many aspects. There should be an independent body that coordinates Linux security framework or tools development and adoption.

We can appreciate that although without starting from scratch in designing new secure kernel, the approaches to provide a secure OS start from designing compiler and using new safer C/C++ libraries.

In dealing with the current vulnerabilities we need to face many new challenges from time to time.

REFERENCES

[1] The Linux Kernel Archives site, "The primary site for the Linux kernel source", http://kernel.org/

[2] The Linux Distributions information site, http://distrowatch.com/

[3] Buffer overflows tutorial, http://www.tenouk.com/Bufferoverflowc/Bufferoverflow1.html

[4] USDA's C2 LEVEL OF TRUST information, http://www.ocio.usda.gov/directives/doc/DM3535-001.htm

[5] The Linux-PAM Guides, http://www.kernel.org/pub/linux/libs/pam/Linux-PAM-html/

[6] The first patch was released by Ingo Molnar of Red Hat and first released in May 2003, ExecShield information, http://people.redhat.com/mingo/exec-shield/

[7] NX/XD bit information at Wikipedia, http://en.wikipedia.org/wiki/NX_bit

[8] Geek.com, "Desktop NX/XD-enabled Intel processors already available", http://www.geek.com/desktop-nxxd-enabled-intel-processors-already-available/?rfp=dta

[9] linuxfromscratch.org, Position Independent Executables (PIE) information, http://www.linuxfromscratch.org/hlfs/view/unstable/glibc-2.6/chapter02/pie.html

[10] Security-Enhanced Linux homepage at National Security Agency (NSA)/Central Security Service (CSS), http://www.nsa.gov/selinux/

[11] Proceedings of the GCC Developers Summit, Ottawa, Ontario Canada, May 25–27, 2003, gccsummit-2003-proceedings.pdf

[12] Homepage of The PaX Team, http://pax.grsecurity.net/

[13] kerneltrap.org, "Linux: PaX vs. ExecShield, An ExecShield Perspective", January 20, 2005 - 6:40pm, by Jeremy, http://kerneltrap.org/node/4590

[14] kerneltrap.org, "Pax vs. ExecShield: Blowing away the smoke", July 9, 2005 - 5:59am, by bluefoxicy on July 9, 2005 - 5:59am, http://kerneltrap.org/node/5396

[15] Rationale for TR 24731 Extensions to the C Library Part I: Bounds-checking interfaces, www.open-std.org/JTC1/SC22/WG14/www/docs/TR24731-Rationale.pdf

[16] ISO/IEC WDTR 24731-2, Specification for Safer C Library Functions — Part II: Dynamic Allocation Functions, www.open-std.org/jtc1/sc22/wg14/www/docs/n1193.pdf

[17] Specification for Safer, More Secure C Library Functions, ISO/IEC draft Technical Report, www.open-std.org/jtc1/sc22/wg14/www/docs/n1135.pdf

[18] The LOCK project, O. S. Saydjari, J. M. Beckman, and J. R. Leaman. LOCK Trek: Navigating Uncharted Space. In *Proceedings of the 1989 IEEE Symposium on Security and Privacy*, pages 167-175, 1989.

[19] Distributed Trusted Mach (DTMach), T. Fine and S. E. Minear. Assuring Distributed Trusted Mach. In *Proceedings IEEE Computer Society Symposium on Research in Security and Privacy*, pages 206-218, May 1993.

[20] The Distributed Trusted Operating System (DTOS) project, S. E. Minear. Providing Policy Control Over Object Operations in a Mach Based System. In *Proceedings of the Fifth USENIX UNIX Security Symposium*, pages 141-156, June 1995.

[21] The Distributed Trusted Operating System (DTOS) Home Page http://www.cs.utah.edu/flux/fluke/html/dtos/HTML/dtos.html

[22] University of Utah, The Flux Research Group, http://www.cs.utah.edu/flux/

[23] University of Utah, Fluke: Flux µ-kernel Environment, http://www.cs.utah.edu/flux/fluke/html/index.html

[24] Flask: Flux Advanced Security Kernel, http://www.cs.utah.edu/flux/fluke/html/flask.html

[25] Role Set Based Access Control, RSBAC, MAC kernel security enhancement project for Linux. http://www.rsbac.org/why

[26] Multi Level security (MLS), “SELinux and MLS: Putting the Pieces Together”, by Chad Hanson, Trusted Computer Solutions, Inc.

[27] Trusted Computing Platform Alliance (TCPA), an initiative led by Intel, http://www.trustedpc.org/

[28] Trusted Computing FAQ, “TC / TCG / LaGrande / NGSCB / Longhorn / Palladium / TCPA”, Version 1.1, August 2003, by Ross Anderson, http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html

[29] IBM PCI Cryptographic Coprocessor, http://www-03.ibm.com/security/cryptocards/pcicc/overview.shtml

[30] The Bastille Linux homepage, http://www.bastille-linux.org/

Low Leakage Cell for Ternary Content Addressable Memory: A Tutorial and Review

Ankaj Gupta[1]

[1]*Department of Electronics& Communication Engineering, Ganga Institute of Technology and Management, Kablana, Jhajjar, Haryana, INDIA*

***Abstract*- Ternary Content addressable Memory (TCAM) has been an emerging technology for packet forwarding in Network Router. New architecture innovations are reducing power and leakage in TCAM. Beside power, leakages also constitute a major part in TCAM performance. In this paper we review various schemes for low leakage TCAM. The circuits have been implemented in 0.35-µm CMOS technology. The minimum power supply is 1.5 V and the maximum supply current is 11.5 µA for a temperature range of 25°C to 30°C.**

***Index Terms*- TCAM Cell, Leakage Current, Power Dissipation**

I. INTRODUCTION

A Content Addressable Memory (CAM) is an outgrowth of random access memory (RAM) technology. Unlike RAMs which access a word based on its address, CAMs access a word based on its contents. A CAM compares an incoming key with all the words in parallel and returns the address of the best match in the array [1]. Therefore CAM is an application specific memory that allows its entire contents to be searched within a single clock cycle. TCAM applications include parametric curve extraction [2], Hough transformation [3], Huffman coding/decoding [4], [5], Lempel–Ziv compression [6]-[9], and image coding [10].Techniques are described to reduce leakage. Fig.1 gives general view of TCAM architecture. The input to the system is the *search word* that is broadcast onto the search lines to the table of stored data. Each stored word has a matchline that indicates whether the search word and stored word are identical (the match or are different (a mismatch case, or miss).

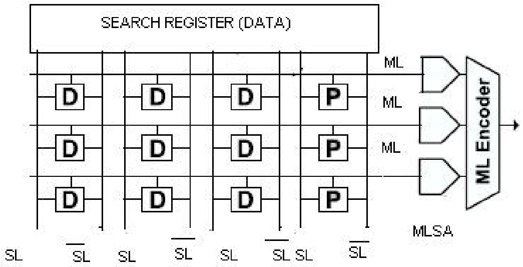


Fig. 1. Schematic of TCAM

II . TCAM CELL

1.1 Leakage Current Component

The leakage current of a deep sub micrometer CMOS transistor consists of three major components: junction tunneling current, subthreshold current and tunneling gate current [11]. In this section, each of these three components is briefly described

1.1.1 Subthreshold Leakage Current: Subthreshold leakage is the drain-source current of a transistor when the gate-source voltage is lower than the threshold voltage. The subthreshold leakage is modeled as [11].

$$I_{sub} = A_{sub}\exp\Big(\frac{q}{n'kT}(V_{GS}-V_{to}-\text{ª}'V_{SB}+\text{¦}V_{DS})\Big)\times\Big(1-\exp(-\frac{q}{kT}V_{DS})\Big) \quad (1)$$

Where

C_{OX} = Gate oxide capacitance per unit area

W = Width of the Transistor

L = Effective Length of the transistor

K = Boltzman’s Constant

T = Absolute Temperature

$\text{ª}'$ = Linearized body effect cofficient

¦ = Drain induced barrier Lowering (DIBL)

$\text{¦}'$ = Subthreshold Swing coefficient of the transistor

1.1.2 Tunneling Gate Leakage Current: Electron tunneling from the conduction band, which is only significant in the accumulation region, results in direct tunneling gate leakage current in nMOS transistors. In pMOS transistors, hole tunneling from the valence band results in the tunneling gate leakage current. If is used for the gate oxide, pMOS transistors will have about one order of magnitude smaller gate leakage than nMOS transistors Therefore, one may conclude that the major source of tunneling gate leakage in CMOS circuits is the gate-to channel tunneling current of the ON nMOS transistors which can be modeled as [12]

$$J_{tunnel} = \frac{4\text{®}m^{*}q}{h^{3}}(kT)2\Big(1+\frac{\text{¥}kT}{2\sqrt{E_B}}\Big)\times\exp\Big(\frac{E_F}{KT}-\text{¥}\sqrt{E_B}\Big) \quad (2)$$

Where $m^*(=0.19M_o)$ = Electron transfer mass

M_o = Electron Rest Mass

h= plank’s Constant

E_F = Fermi Level at the Si/SiO_2 interface

E_B = Height of Barrier

$$\text{¥} = \frac{4\text{®}T_{OX}\sqrt{2m_{ox}}}{h} \quad (3)$$

Where m_{ox} (= $0.32M_o$) = Effective Electron Mass in the Oxide

The major contributor to the tunneling gate leakage current in a 6T SRAM cell is the gate-to-channel leakage of the ON pull-down transistor. To weaken this leakage path, one needs to increase the gate-oxide thickness of the pull-down transistors. To reduce other (minor) tunneling gate leakage currents in the SRAM cell, one only needs to increase the gate oxide thickness of the pass transistors, because from the previous discussion, it can be concluded that the gate leakage saving achieved by increasing the oxide thickness of the pMOS transistors would be quite small. Increasing the oxide thickness of a transistor not only increases the threshold voltage, but also reduces the drive current of the transistor. So, the effect of applying this technique to an SRAM cell is an increase in the read/write delay of the cell. This is general equation for leakage in SRAM cell that govern all leakage in TCAM memory.

1.2 Conventional Cell16T TCAM

Fig. 2. shows the leakage paths in a 6T-SRAM-based TCAM cell when the BLs are charged to the 'mask' state (BL1 = BL2 = '0'), and minimum-size transistors are used. I_{SN} and I_{SP} are NMOS and PMOS subthreshold leakages respectively. NMOS gate leakages are specified by I_{GON} and I_{GOFF} for 'ON' and 'OFF' transistors, respectively. Similarly I_{GONP} and I_{GOFFP} are PMOS gate leakages. Assuming random data, a TCAM column with shared BLs has the same probability of storing '0', '1' and 'mask' states. Hence, one-third of the bits will be masked and setting the BLs to the 'mask' state minimizes the subthreshold leakage. For example, if the BLs are set to '0' (BL1 = '0', BL2 = '1'), the subthreshold leakage through the access transistors will be $2I_{SN}$ when the stored value is 'mask'. Typically, the driver transistors (NMOS in the cross-coupled inverters) are sized nearly 2 to 2.5 times larger than the access transistors to perform fast READ operation without disturbing the stored data.

Leakage Current	Measured Current	Modified Value (fA)
$2I_{SN}$	2(-4.9087 n+ 802.77f)	-9.815 e6 f
$2I_{SP}$	2(6.0318 u + 3.6117 u)	19.287 e9 f
$2I_{GON}$	2(-1.8082 f + 4.998 e-16 A)	-2.6168 f
$6I_{GOFF}$	6(1.3378 e-17 A+ -2.934 e -17A)	-9.5772 e-2 f
$2I_{GONP}$	2(3.20 f + -1.089 e -16 A)	6.1822 f
$2I_{GOFFP}$K	2(-9.2001 e-16A + 3.6729 e-16A)	-5.5272 e-1 f

$$I_{6T\_Mask}/_{BLs} = Mask = 2I_{SN} + 2I_{SP} + 2I_{GON} + 6I_{GOFF} + 2I_{GONP} + 2I_{GOFFPK} \quad (4)$$

Larger transistors result in greater leakages. Since the READ speed is not critical in a TCAM, minimum size transistors can be USED.

This choice also reduces the cell area. Conventional SRAMs also precharge BLs to VDD in order to perform fast READ operation.

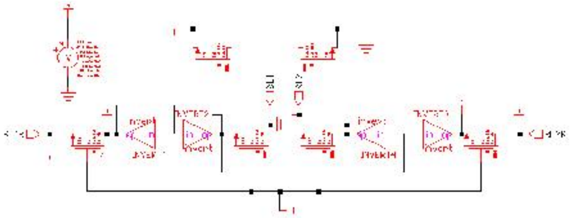


Fig. 2. Conventional TCAM Cell

Leakage Current	Measured Current	Modified Value (fA)
$2I_{SN}$	2(-4.9087 n+ 802.77f)	-9.815 e6 f
$2I_{SP}$	2(6.0318 u + 3.6117 u)	19.287 e9 f
$2I_{GON}$	2(-1.8082 f + 4.998 e-16 A)	-2.6168 f
$6I_{GOFF}$	6(1.3378 e-17 A+ -2.934 e -17A)	-9.5772 e-2 f
$2I_{GONP}$	2(3.20 f + -1.089 e -16 A)	6.1822 f
$2I_{GOFFP}$K	2(-9.2001 e-16A + 3.6729 e-16A)	-5.5272 e-1 f

TABLE I

LEAKAGE CURRENT OF CONVENTIONALJ TCAM

Table I gives leakage current of different transistor of 16 T TCAM Cell. In TCAMs, BLs can be precharged to the state, which results in the minimum leakage. Figure 1 can be used to calculate the leakage current for a 6T-SRAM-based TCAM cell as given by equation (3) for different storage conditions. Below table shows abbreviations

1.3 NMOS-Coupled TCAM Cell

Till this point we have studied conventional TCAM cell. In 2006, Nitin and Manoj [13] presented a novel ternary storage cell. In this paper we have review this NMOS and Next PMOS technique .Each TCAM cell contains two SRAM cells to store the ternary value. These SRAM cells can have four combinations: '00', '01', '10', and '11'. Table II shows leakage current of NMOS coupled TCAM cell

Leakage Current	Measured Current	Modified Value (fA)
$2I_{SN}$	2(-4.9087 n+ 802.77f)	-9.815 e6 f
$2I_{SP}$	2(6.0318 u + 3.6117 u)	19.287 e9 f
$2I_{GON}$	2(-1.8082 f + 4.998 e-16 A)	-2.6168 f
$6I_{GOFF}$	6(1.3378 e-17 A+ -2.934 e -17A)	-9.5772 e-2 f
$2I_{GONP}$	2(3.20 f + -1.089 e -16 A)	6.1822 f
$2I_{GOFFP}$K	2(-9.2001 e-16A + 3.6729 e-16A)	-5.5272 e-1 f

TABLE II

LEAKAGE AT NMOS COUPLED TCAM

. However, only three out of them are used for the ternary value, and the "unused" state (typically '11') is forbidden. This ternary storage cell trades this "unused" state for a smaller leakage by coupling two 5T-SRAM cells and eliminating a subthreshold leakage path [13]. Fig. 3 shows the leakage paths of the NMOS-coupled (NC) ternary storage cell that connects two 5T-SRAM cells . For storing a ternary ‘0’ or ‘1’, one of the storage nodes (connected to the access transistors) is held at logic ‘0’through the coupling NMOS transistor. Likely when the ‘mask’ state is stored, both coupling NMOS transistors are ‘OFF’. Note that when both coupling NMOS transistors are ‘ON’, the cell is not stable. Hence, this cell can store only three states. It can be noticed in Figure 3. that the proposed cell can store only three states because the coupling does not allow the “unused” state. The total leakage current for an NC-TCAM cell (with BLs = ‘mask’) can be given by equation (5)

$$I_{NC\_MASK}/_{BLs=Mask} = 2I_{SN} + 2I_{SP} + 2I_{GON} + 6I_{GOFF} + 2I_{GONP} + 2I_{GOFFP} \quad (6)$$

Thus, it will exhibit less leakage than the 5TSRAM- based cell only if condition (7) is satisfied:

$$0.67I_{SN} > 3.33I_{GOF\ F} \rightarrow I_{SN} > 5I_{GOFF} \quad (7)$$

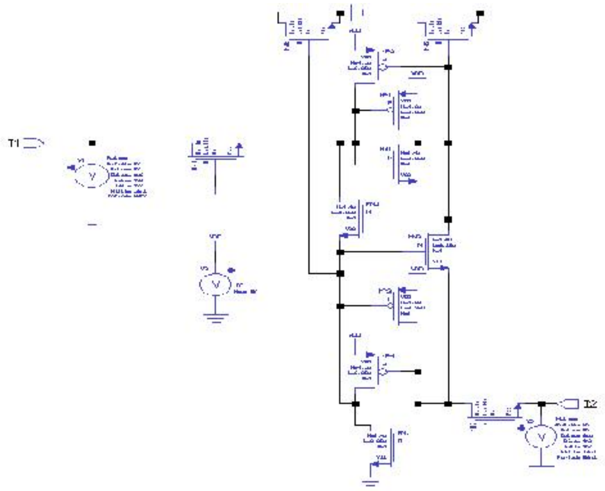


Fig. 3. NMOS Coupled TCAM Cell

1.4 P-MOS Coupled TCAM Cell

The coupling between the two 5T-SRAM cells can also be obtained by PMOS transistors. Fig. 4. shows the leakage paths of the PMOS-coupled (PC) TCAM cell. Similar to the NC-TCAM cell, one of the coupling PMOS transistors does not consume subthreshold leakage under ‘0’ and ‘1’ conditions. Thus, it will also exhibit smaller leakage than the 5T-SRAM-based cell if the subthreshold leakage is more than the gate leakage. The total leakage current for a PC-TCAM cell (with BLs set to the ‘mask’ condition) can be given by equation (6).

$$I_{PC\_MASK}/_{BLs=Mask} = 2I_{SN} + 2I_{SP} + 2I_{GON} + 2I_{GOFF} + 2I_{GONP} + 2I_{GOFFP} \quad (8)$$

Similar to the 5T-SRAM-based cell, this BL precharge condition reduces both subthreshold and gate leakages. The PC-TCAM cell will consume less leakage than the 6T-SRAM-based cell only if condition (9) is satisfied.

$$0.67I_{SP} > 0.67I_{GOFFP} \rightarrow I_{SP} > I_{GOFFP} \quad (9)$$

Similarly, the PC-TCAM cell will consume less leakage than the NC-TCAM cell (when BLs = ‘mask’) only if condition (10) is satisfied.

$$0.67I_{SP} + 3.33I_{GOFF} > 0.67I_{SN} + 0.67I_{GOFFP} \rightarrow I_{SP} + 5I_{GOFF} > I_{SN} + I_{GOFFP} \quad (10)$$

Table III gives leakage current of PMOS coupled TCAM cell

Leakage Current	Measured Current	Modified Value (fA)
$2I_{SN}$	2(0 + 91.328 n)	182.64 e6 f
$2I_{SP}$	2(-526.3173 f + -9.481 e-18 A)	-1.052 e-3 f
$2I_{GON}$	2(0 + 2.20803 e-17A)	4.41606 e-2 f
$2I_{GOFF}$	2(0 + 1.4698 e-18A)	2.9392 e-3 f
$2I_{GONP}$	2(0 + -2.4130 e-18A)	4.82 e-3 f
$2I_{GOFFP}$K	2(-5.9084 e-17 A + 5.1861 e-17A	-14.4 e-3 f

TABLE III
LEAKAGE AT PMOS COUPLED TCAM

If the gate leakage is comparable to the subthreshold leakage (ISN < 3IGOFF) and BLs of NCTCAM are at GND, the PC-TCAM cell will consume less leakage than the NC-TCAM cell if condition (10) is satisfied.

$$0.67_{ISP} + 1.33I_{GOFF} > 0.67I_{GOFFP} \rightarrow \quad I_{SP} + 2I_{GOFF} > I_{GOFFP} \quad (11)$$

Most CMOS processes will satisfy condition (8) because the PMOS subthreshold leakage and the NMOS gate leakage both are typically larger than the PMOS gate leakage.

The leakages of the above cells (when BLs = ‘mask’) are summarized in Table IV. It can be shown that that the 6T-SRAM-based cell always consumes more leakage than the other three cells

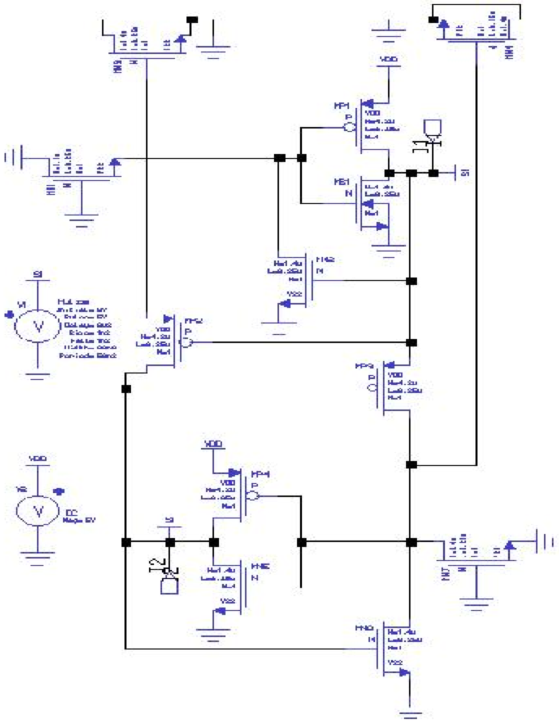


Fig . 4. PMOS Coupled TCAM Cell

.

Cell	Stored Value	Subthreshold Leakage	NMOS Gate Leakage	PMOS Gate Leakage
6T	×	$2I_{SN}+2I_{SP}$	$2I_{GON}+6I_{GOFF}$	$2I_{GONP}+2I_{GOFFP}$
PC	×	$2I_{SN}+2I_{SP}$	$2I_{GON}+2I_{GOFF}$	$2I_{GONP}+2I_{GOFFP}$
NC	×	$2I_{SN}+2I_{SP}$	$2I_{GON}+6I_{GOFF}$	$2I_{GONP}+2I_{GOFFP}$

TABLE IV
LEAKAGE CURRENT OF TCAM WHEN BITLINE=MASK

III SIMULATION RESULT

We simulated the above TCAM cells using 0.35 µm technology. Figure 5 shows the leakage of different TCAM cells at 0.35µm CMOS technologies. It can be noticed that the magnitudes of different leakage components are related as follows:

ISN > ISP >> IGON > IGOFF >> IGONP > IGOFFP

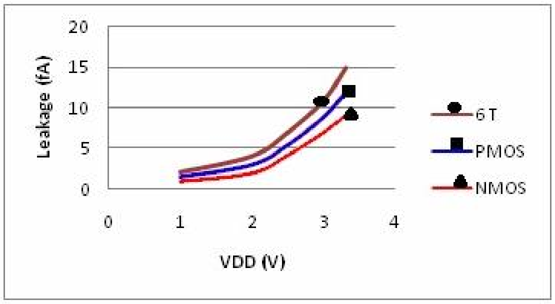


Fig. 5. TCAM Cell Leakage for 35 nm CMOS technology

In this writing 1 was more difficult than writing 0 as it is tough to transfer 1 from NMOS transistor. The conventional 16 transistor TCAM area consume most area and hence most power dissipation. Newer approach like NMOS and PMOS use less area as number of transistor is less as well less power dissipation.

IV CONCLUSION

In this work we have studied and analyzed TCAM circuits with an emphasis on high capacity RAM. We have simulated conventional 16 transistor TCAM cell, NMOS coupled TCAM cell and PMOS coupled TCAM cell for low leakage and less area. Simulation results shows a reduction of up to 38% leakage reduction in NMOS and PMOS coupled TCAM cell as compared to conventional TCAM cell. The efficiency of PMOS coupled TCAM cell is best in all category

ACKNOWLEDGMENT

This work has been performed on Mentor-Graphics Tools at VLSI Design Lab, Department of Electronics and Communication Engineering, Guru Jambheswar University of Science and Technology, Hisar-125001

REFERENCES

[1] T. Kohonen, *Content-Addressable Memories*, 2nd ed. New York: Springer-Verlag, 1987.

[2] M. Meribout, T. Ogura, and M. Nakanishi, "On using the CAM concept for parametric curve extraction," *IEEE Trans. Image Process.*, vol. 9, no. 12, pp. 2126–2130, Dec. 2000.

[3] M. Nakanishi and T. Ogura, "Real-time CAM-based Hough transform and its performance evaluation," *Machine Vision Appl.*, vol. 12, no. 2, pp. 59–68, Aug. 2000.

[4] E. Komoto, T. Homma, and T Nakamura, "A high-speed and compactsize JPEG Huffman decoder using CAM," in *Symp. VLSI Circuits Dig. Tech. Papers*, pp. 37–38,1993.

[5] L.-Y. Liu, J.-F.Wang, R.-J.Wang, and J.-Y. Lee, "CAM-based VLSI architectures for dynamic Huffman coding," *IEEE Trans. Consumer Electron.*, vol. 40, no. 3, pp. 282–289, Aug. 1994.

[6] B. W. Wei, R. Tarver, J.-S. Kim, and K. Ng, "A single chip Lempel-Ziv data compressor," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, vol. 3, pp. 1953–1955, 1993.

[7] R.-Y. Yang and C.-Y. Lee, "High-throughput data compressor designs using content addressable memory," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, vol. 4, pp. 147–150, 1994..

[8] C.-Y. Lee and R.-Y. Yang, "High-throughput data compressor designs using content addressable memory," *IEE Proc.—Circuits, Devices and Syst.*, vol. 142, no. 1, pp. 69–73, Feb. 1995.

[9] D. J. Craft, "A fast hardware data compression algorithm and some algorithmic extansions," *IBM J. Res. Devel.*, vol. 42, no. 6, pp. 733–745, Nov. 1998.

[10] S. Panchanathan and M. Goldberg, "A content-addressable memory architecture for image coding using vector quantization," *IEEE Trans. Signal Process.*, vol. 39, no. 9, pp. 2066–2078, Sep. 1991.

[11] B. Amelifard, F. Fallah, and M. Pedram, "Low-leakage SRAM design with dual Vt transistors," in *Proc. Int. Symp. Quality Electron. Dec.*, pp. 729–734, 2006.

[12] F. Hamzaoglu, Y. Te, A. Keshavarzi, and K. Zhang, "Dual V–SRAM cells with full-swing single-ended bit line sensing for high-performance on-chip cache in 0.13 _m technology generation," in *Proc. Int. Symp. Low Power Electron. Des.*, pp. 15–19, 2006.

[13] N. Mohan, and M. Sachdev, "Novel ternary storage cells and techniques for leakage reduction in ternary CAM, "Proceedimgs of *the IEEE Iinternational SOC conference (SOCC),* Austin, Texas, Sep. 24-27, 2006.

MCML:Design and analysis of CMOS Invertor and MCML Invertor

Shankar Kumar Vijay [1]

[1] *Department of Electronics & Communication Engineering, Ganga Institute of Technology and Management, Kablana, Jhajjar, Haryana, INDIA*

Abstract—In this paper, a new D-latch topology has been implemented in MOS Current Mode Logic (MCML) that works on lower supply voltage than the D-latch topology already implemented in MCML. The already implemented D-latch topology is called Traditional D-Latch Topology and the new D-latch topology that works on lower voltage is called low-voltage D-Latch Topology. Power consumed by MCML circuit is directly related to the supply voltage given to the circuit. For a particular amount of current drawn from the power supply, if supply voltage increases then power consumption of the circuit also increases and vice versa. Thus, the low-voltage D-latch topology consumes lesser power than the traditional D-latch topology.

Keywords- MCML, D-latch, VLSI, Low Power, MOSFET, Ttraditional D-latch.

I. INTRODUCTION

The demand for electronic circuits with extremely low supply voltages and power consumption is important in development of microelectronic technologies. In many applications, additional requirements appear, particularly the extreme speed or the accuracy of signal processing. Simultaneous fulfilment of the above demands is problematic. In the last two decades, the evolution of modern applications of analog signal processing has followed the trends of so-called current mode, where signals, representing the information, are in the form of electric currents. In contrast to the conventional voltage mode, which utilizes electric voltages, the current mode circuits can exhibit under certain conditions among other things higher bandwidth and better signal linearity. The current mode approach for analog signal processing circuits and systems has emerged as an alternate method besides the traditional voltage mode circuits due to their potential performance features like wide bandwidth, less circuit complexity, wide dynamic range, low power consumption and high operating speed [1].The continued growth of market of mobile and satellite communication as well as multiple optical fiber system, demands for the implementation of high performance MCML circuit. In many applications, the D-latch gate is the basic circuit used to implement a number of fundamental blocks, whose performance strongly depends on D-latch gate performance.

The traditional implementation of MCML D-latch is based on stacked source-coupled pairs of MOSFETs. To keep its speed performance as high as possible, transistor operation in the saturation region has to be ensured by using a high enough supply voltage according to the number of stacked MOSFET. In addition, a high bias current must be used to improve the speed performance, thereby determining a high static power dissipation that reduces the battery life time in portable devices and limits the feasibility of complex circuits [2].

MCML D-latch topology has been developed to reduce the supply voltage by decreasing the number of stacked MOSFET. This topology will be accordingly referred as the low voltage topology. The interest in MOS current-mode logic (MCML) is increasing because of its ability to dissipate less power than conventional CMOS circuits at high frequencies, while providing an analog friendly environment. It is used as a technique for obtaining low power mobile wireless systems operating in GHz range. MCML is a logic style for high speed, low power circuits. This type of logic was 1st implemented using bipolar transistors and extended for application with MOS transistors. MCML circuits with constant bias current are intended for accurate high-speed mixed signal application [3]. MCML dissipates constant static power and requires techniques more analogous to analog design. However, MCML requires smaller dynamic power than that of the conventional logic because of the smaller output swings. MCML seems to be promising in both reducing power consumption and providing an analog friendly environment. The reduced output swing and a faster switching makes MCML a promising candidate for certain mixed-signal applications. The constant supply currents, lower cross talk between analog and digital circuits of MCML improve the accuracy of mixed-mode systems.

II. BASIC CONCEPT OF MCML

MCML in general consists of three main components, as shown in the Fig 2.1, which includes the pull-up load, the pull-down network (PDN) and a constant current source.

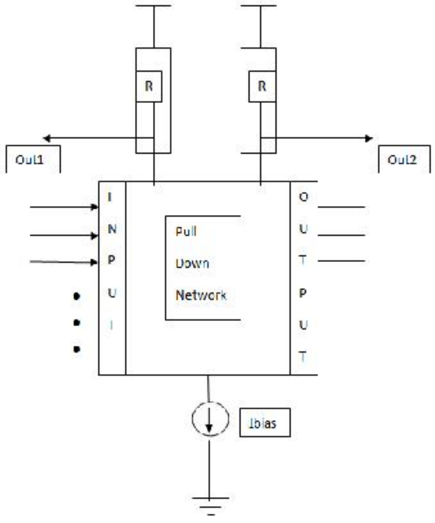


Fig. 1: Basic blocks of MCML

MCML is a completely differential logic, i.e. all signals and their complements are required. Depending on the logic implemented by PDN, all the current flows through one of the two branches, providing complementary output signals. Voltage at the output of branch with no current reaches VDD, whereas for the other branch some voltage drops across the load. resistor and the output voltage becomes VDD - Ibias*RL. Due to the reduced swing, it has smaller dynamic power dissipation.

MCML circuits are faster than other logic families, because it uses NMOS transistors only. Due to its differential nature, it is highly immune to common mode noise. It has almost flat power curve over a wide range of frequency as opposed to other logic styles where power consumption increases directly with frequency. Therefore at very high frequencies its power consumption is comparable or lower than other logic styles. This makes it a good choice for high speed and low power integrated circuit design

III.COMPARISON BETWEEN CMOS AND MCML CODE

Till recently, CMOS technology was being used extensively to implement digital circuits. CMOS has the advantage that its static power consumption is extremely less. It uses power only when charging and discharging. That is, dynamic power consumption of CMOS logic is considerable.

Now a day's frequency of operation of the digital circuit is increasing day by day. With the increase in frequency, dynamic power consumption of CMOS circuit increases considerably. Hence at higher frequency of operation, power consumption of CMOS circuits is substantial. Another problem with CMOS logic is that its operation is relatively slow

IV. INVERTERS OF THE CMOS LOGIC

The data plotted there was obtained by SPICE simulations using the parameters of 0.18µm CMOS transistors with a 1.8-V supply voltage. The MCML is faster than CMOS logic because of its smaller input capacitance and smaller signal amplitude. Because the CMOS logic uses power only when charging and discharging, its power consumption is generally than that of the MCML. The power consumption of this CMOS logic is the product of the operation frequency and the charging and discharging power unit switching.

On the other hand, the power consumption of the MCML is the sum of the penetration currents of MN1 and MN2 in the figure, which is the same as the drain current of the current source transistor MC1. Since MC1 operates at saturation region, this drain current is mainly determined by the gate bias and the contribution of the voltage at the common- source node NC is small. Moreover, the operation frequency has little effect on the voltage at NC because of the power consumption of the MCML is nearly independent of the operation frequency. In the Fig.4.1and Fig. 5.1, there are two MOSFETs in the CMOS logic and five in the MCML.

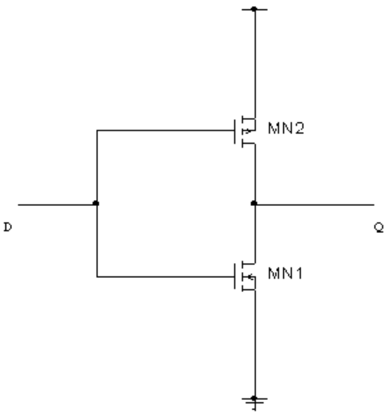


Fig.2
CMOS Inverter

V. CONVENTIONAL MCML

In addition, the MCML requires two lines for each signal. Therefore, a chip area with a given function is about two to four times larger in the MCML than in the CMOS logic.

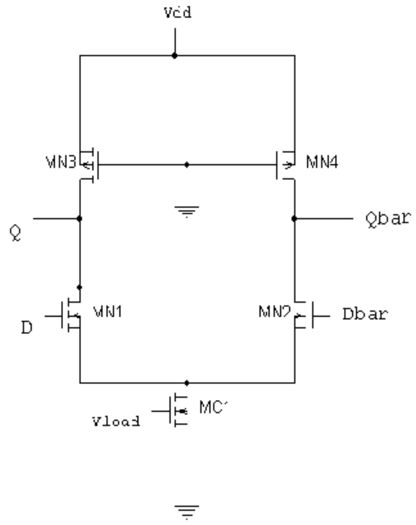


Fig.3 MCML Inverter

VI.TRADITIONAL D-LATCH

A MOS current mode logic (MCML) D-Latch consists of a source-coupled pair driven by the input CLK, that alternatively activates the transistor pair M3-M4 or M5-M6. When CLK is high, M2 is OFF, hence the bias current Is flow through M1 and is then steered by transistors M3-M4 according to the value of input D. Being the output set by input D, the latch is said to be in the transparent state. When CLK is low, the bias current is flow through transistor M2 and cross-coupled transistors M5-M6, that store the previous out value by virtue of their positive feedback connection, and the is in hold mode which is shown in fig.6.1

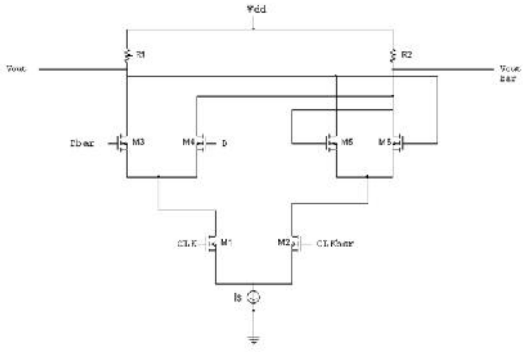


Fig. 4 Traditional D-Latch

VI.RESULT AND ANALYSIS

A. Inverters of the CMOS logic

The CMOS logic has the advantage of low power consumption, but its operation is relatively slow. For example, the maximum toggle frequency of a conventional 0.18µm CMOS inverter is only about 3.5 GHz. Simulated inverter delay time as a function of fan-out and power consumption is a function of a operation frequency for the CMOS logic and the MCML are shown in the Fig.7.1.

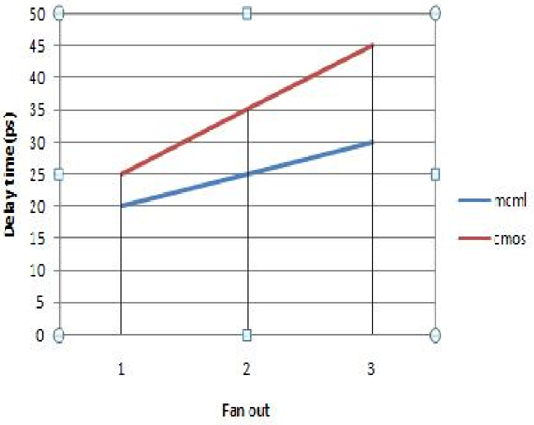


Fig 5 Delay Vs Fan out of MCML and CMOS inverter

The data plotted there was obtained by SPICE simulations using the parameters of 0.18μm CMOS transistors with a 1.8-V supply voltage. The MCML is faster than CMOS logic because of its smaller input capacitance and smaller signal amplitude. The data plotted there was obtained by SPICE simulations using the parameters of 0.18μm CMOS transistors with a 1.8-V supply voltage.

B.Conventional MCML

Spice simulations were performed using the parameters of 0.18-μm CMOS transistors. However, in the gigahertz frequency range, the power consumption of the CMOS logic

becomes larger than that of the MCML, as shown in the Fig7.1[b].From the graph it is clear that the MCML is suitable for low-power operation in the gigahertz frequency range

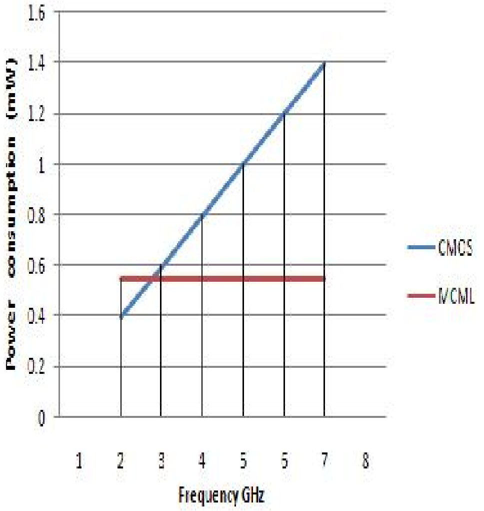
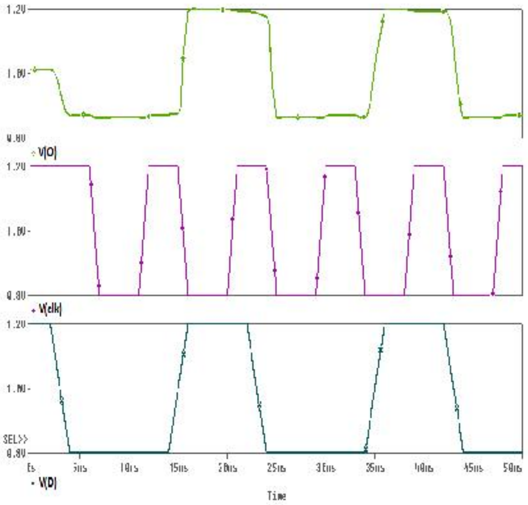


Fig. 6 Power dissipation Vs Frequency for CMOS and MCML

C. Simulation result for D-Latch

When data is high all the current passes through one branch, as a result the voltage at the drain of that transistor drops to a voltage level (VDD - IsRL). As the other transistor is in cut off and no current is flowing through it, the voltage at the drain of that transistor becomes high (VDD). When clock goes low, the hold pair is activated.



.

Fig. 7. Simulation result for D-Latch

VII.CONCLUSIONS

The concept of MOS current mode logic is explained in. CML logic is very useful for high frequency application because power consumption of CMOS based circuit increase in high frequency. MCML based Low Voltage D-latch topology has been developed and compared to the traditional implementation of MCML D-Latch in terms of supply voltage. It allows for a supply voltage reduction by a factor of 25 % with respect to the traditional topology, which could be exploited to achieve power savings.

REFERENCES

[1] M. Sumathi, Kartheek, “Performance and analysis of CML Logic gates and latches” IEEE 2007 International Symposium on Microwave, Antenna, Propagation, and EMCTechnologies for Wireless Communications

[2] FERRI, G., GUERRINI, N. C. Low-voltage low-power CMOS current conveyors. London: Kluwer Academic Publishers.2003.

[3] B. Razavi, Y. Ota, and R. G. Swartz, “Design techniques for low-voltage high-speed digital bipolar circuits,” IEEE J. Solid-State Circuits, vol. 29, pp. 332–339, Mar. 1994.

[4] Hassan, Mohab Anis, Mohamed Elmasry, “MOS Current Mode Circuits Analysis, Design” IEEE transactions on very large scale integration (vlsi) systems, vol. 13, no. 8, august 2005.

[5] K.Kishine, Y.Kobayashi, H.Ichno, “A high speed low power by polar digital circuit for Gb/LSI: current mirror control logic”,IEEE solid state ckt(1997).

[6] M. Alioto, R. Mita, G. Palurnbo, “Analysis and Comparison of Low-Voltage by CML D- Latch” 0-7803-7596-3/02,2002 IEEE

[7] TOUMAZOU, C., LIDGEY, F.J., HAIGH, D.G. Analogue IC Design: The current mode approach. IEE Circuits and Systems Series 2, Peter Peregrinus Ltd., 1990.

[8] M. Yamashina and H. Yamada, “An MOS current mode logic (MCML) circuit for low- power sub-GHz processors,” IEICE Trans. Electron., vol. E75-C, no. 10, pp. 1181–1187, Oct. 1992.

[9] J. Musicer and J. Rabaey, “MOS current mode logic for low power, low noise CORDIC computation in mixed-signal environments,” in Proc. Int. Symp. Low Power Electronic Design (ISLPED’00), Jul. 2000, pp. 102–107.

[10] M. Alioto and G. Palumbo, “Design strategies for source coupled logic gates,” IEEE Trans. Circuits Syst. I, vol. 50, pp. 640–654, May 2003.

[11] B. Razavi, Design of Analog CMOS Integrated Devices. New York: McGraw-Hill, 2001.

[12] M. Alioto - G. Palumbo, "Modeling and optimized design of current mode MUX/XOR and D Flip-Flop," IEEE Trans. on CASpart I I , V. 47, No.5, pp.452-461, May2004

Mechanically Reinforced Earth Walls

Naveen Kumar[1], Manoj Lakra[2], Pankaj Yadav[3]

[1,2,3]*Department of Civil Engineering, Ganga Institute Of Technology & Management, Kablana, Jhajjar, Haryana, INDIA*

Abstract: this paper will investigate the basic principles of the reinforced erath and gravity wall. At present, the mechanically stabilized earth and gravity walls are probably the most used-particularly for roadwork where deep cuts or hill side road locations require retaining walls to hold the earth in place. These walls eliminate the need for using natural slopes and result in savings in both right of way costs and fill requirements. Most retaining structures are vertical or nearly so; however, if the ‘α’ angle in the coulomb earth-pressure coefficient is larger than 90°, there is a reduction in lateral pressure that can be of substantial importance where the wall is high and a wall tilt into the backfill is acceptable.

I. INTRODUCTION:

The mechanically reinforced earth wall of Fig. 1-1 uses the principle of placing reinforcing into the backfill using devices such as metal strips and rods, geotextile strips and sheets and grids, or wire grids. There is little conceptual difference in reinforcing soil or concrete masses—reinforcement carries the tension stresses developed by the applied loads for either material. Bond stresses resist rebar pullout in concrete: soil relies on friction stresses developed based on the angle of friction δ between soil and reinforcement or a combination of friction and passive resistance with geo- and wire grids.

The principle of reinforced earth is not new. Straw, bamboo rods, and similar alternative materials have long been used in technologically unsophisticated cultures to reinforce mud bricks and mud walls. Nevertheless, in spite of this long usage French Architect H. Vidal was able to obtain a patent (ca. mid- 1960s) on the general configuration of Fig. 1-1, which he termed “reinforced earth.”

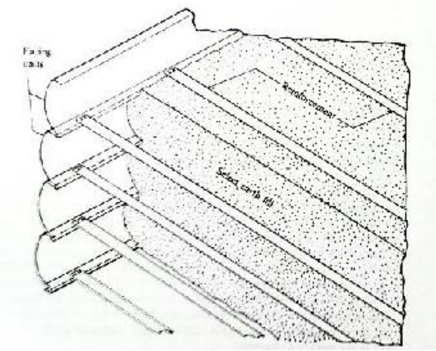


Figure 1 The Reinforced Earth Concept

We see three basic components in this figure:

1. The earth fill---usually select granular material with less than 1 percent passing the No. 200 sieve.

2. Reinforcement---strips or rods of metal, strips or sheets of geotextiles, wire grids, or chain link fencing or geo grids (grids made from plastic) fastened to the fencing unit and extending into the backfill some distance. Vidal used only metal strips.

3. Facing unit---not necessary but usually used to maintain appearance and to avoid soil erosion between the reinforcements.

These three components are combined to form a wall whose side view is shown in fig.1-2 the facing units may be curved or flat metal plates or precast concrete strips or plates .where geotextiles are used the sheet may lap,fig. 1-3, to produce the facing unit When wire mesh or other reinforcement with discontinuities (grid voids) is used ,a portion may be bent, similar to the sheet of fig.1-3, to form a facing unit. Grid type reinforcements strengthen the soil through a combination of friction and passive pressure pullout resistance. The bent-up portion used as a facing piece provides some erosion control until the wall is completed.

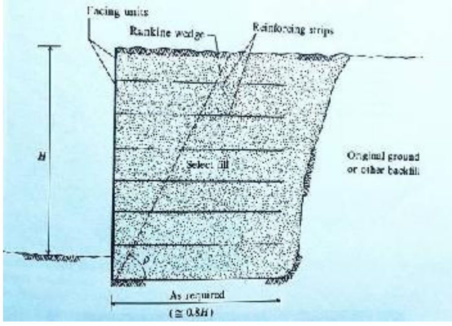


Fig 2 reinforced earth walls

The exposed reinforcements are usually sprayed with concrete mortar or gunite (material similar to mortar) in lifts to produce a thickness on the order of 150 to 200mm. This is both to improve the appearance and to control erosion. For metals this covering also helps control rust, and for geotextiles it provides protection from the ultraviolet rays in sunlight and discourages vandalism.

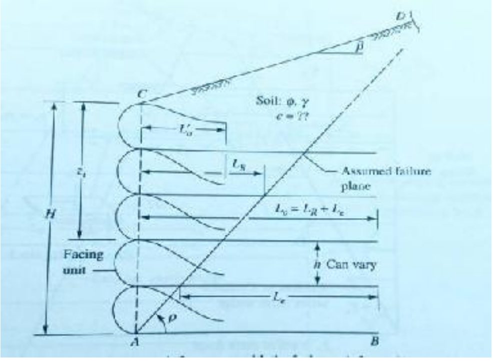


Figure 3; Using Geotextile sheets for reinforcement with the facing unit formed by lapping the sheet as shown. Critical Dimensions are L_e, L_0. Distances L_e and L_0 are variable but for this wall produce a constant length $L_{con} = L_0 + L_e$. The Rankine p not equal to $45^\circ + \varphi/2$ for backfill β as shown.

The basic principle of reinforced earth is shown in fig 1.4 where we see a wall acted on by either the Rankine or Coulomb active earth wedge. Full-scale tests have verified that the earth force developed from the active earth wedge at any depth z is carried by reinforcing strip tension.

Strip tension is developed in the zone outside the active earth wedge from the friction angle δ between strip and soil and the vertical earth pressure left to be carried by the wall facings they can be quite thin and flexible with the principal functions of erosion control and appearance.

II. DESIGN CONSIDERATION

The following several factors enter into the design of reinforced earth wall:

1. Backfill soil is usually specified to be granular; however, recent research indicates that we can use cohesive soil if a porous geotextile is used for reinforcement to allow backfill drainage. This allows one to use the drained friction angle φ' to calculate friction between the soil and reinforcing.
2. Backfill soil should be compacted, taking care not to get component too close to the facing unit, so that it is not pulled from the reinforcement.

   It is also necessary to exercise care with geotextile fabrics not to tear the fabric in the direction parallel to the wall. A partial tear of this type would reduce the amount of tension the fabric can carry.
3. Tests with experimental walls indicate that the ranking wedge adequetly defines the "soil wedge" this angle should be routinely checked using the trial wedges method for large backfill angles.
4. The wall should be sufficiently flexible that the active earth pressure wedge forms and any settlement/subsidence do not tear the facing unit from the reinforcement.
5. It is usually the assume all the tension stress are in the reinforcement outside the assumed soil wedge zone – typically the distance L of fig 1-5.

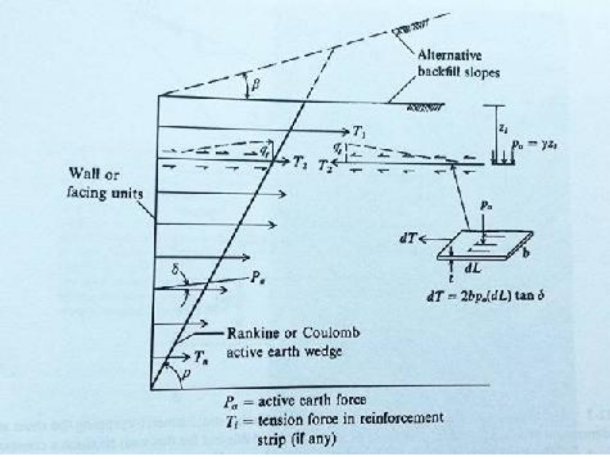


Figure 1.4; The General Concept of reinforced earth is that $\Sigma T_i = P_a Cos\delta$, so the earth force against the wall =0

6. The wall failure will occur in one of three ways

a. Tension in the reinforcements.
b. Bearing capacity failure of the base soil supporting the wall along the base line AB of fig 1-3 and 1-6.
c. Sliding of the full block (ABCD of fig 1-6) along base AB.

7. Surcharges (as in fig 1-6) are allowed on the backfill. These requires analysis to ascertain whether they are permanent (such as a roadway) or temporary and where located for example

   a. Temporary surcharges within the reinforcement zone will increase the lateral pressure which in turn increases the tension in the reinforcements but does not contribute reinforcement stability.
   b. Permanent surcharges within the reinforcement zone will increase the lateral pressure and tension in the reinforcements and will contribute additional vertical pressure for the reinforcement friction.
   c. Temporary or permanent surcharges outside the reinforcement zone contribute a lateral pressure, which overturn the wall.

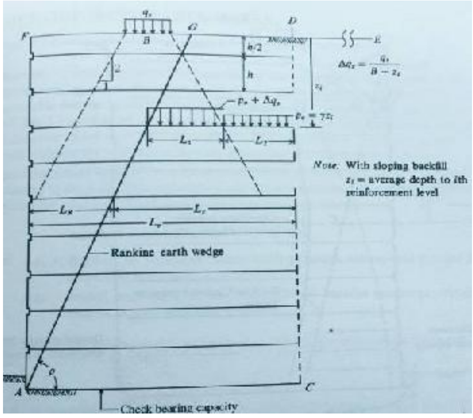


Figure 1.5; Length of Reinforcements L0 = Lr +Le as required bus must extend beyond Rankine/Coulomb Earth-Pressure wedge

In most cases the lateral pressure from the backfill surcharge can be estimated using the Theory of Elasticity equation [Eq. (11-20)]. One can also use the Bossiness equation for vertical pressure, but it will may be sufficiently accurate to use the 2:1 method [Eq.(5-2)] adjusted for plane strain to give $q_v = Q/B+Z$

Where Q=Bqo for the strip width(side view) and average contact pressure produced by the surcharge ; for point loads use either a unit width(0.3m or 1 ft) or Eq. (5-3). Since these two methods give greatly differing vertical pressures (the 2:1 is the high and Eq (5-3) is very low) yo may have to use some judgement in what to use –perhaps an average of two methods.

B= strip width; you implicitly using L=1 unit of width.

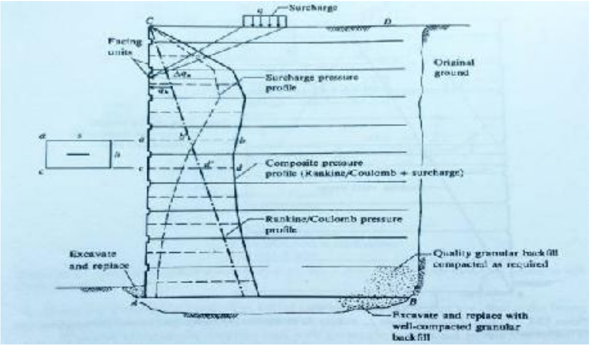


Figure 1.6; General wall case with surcharge on backfill as from a road or other construction.

Linearizing the surcharge pressure profile as shown is sufficiently accurate, Laba and Kennedy (1986) used the 2:1 vertical pressure method [Eq. (5.2)] as shown in Fig. 1-5 with reasonably good results. In this figure Eq. (5.2) is being used to get a pressure increase in the zone L_1 so that the friction resistance F_R for the effective lengths ($L_e = L_1 + L_2$) is

$$Fr = \tan\delta\,[(\gamma z + \Delta q)\,L_1 + \gamma z L_2]$$

Where terms are identified in Fig. 1.5

8. Corrosion may be a factor where metal reinforcements are used. It is common to increase the theoretical strip thickness somewhat to allow for possible corrosion within the design period, which may be on the order of 50 to 100 years.
9. Where aesthetics is critical, a number of concrete facing unit configurations are available in a wide range of architecturally pleasing facades, which can either outline the wall or blend it into the landscape
10. There will be two safety factors SF involved. One SF is used to reduce the ultimate strength of the reinforcements to a "design" value. The other SF is used to increase the computed length L_e required to allow for any uncertainty in the backfill properties and soil-to-reinforcement friction angle δ.

DESIGN OF REINFORCED EARTH WALLS:

The design of a reinforced earth wall proceeds basically as follows:

1. Estimate the vertical and horizontal spacing of the reinforcement strips as in Fig. 1-7. Horizontal spacing *s* is meaningless for both wire grids and geotextile sheets but one must find a suitable vertical spacing *h* for those materials. The vertical spacing may range from about 0.2 to 1.5 (8 to 60in.). The lateral-earth-pressure diagram is based on a unit width of the wall but is directly proportional to horizontal spacing *s*.
2. Compute the tensile loads of the several reinforcements as the area of the pressure diagram contributing to the strip. This calculation can usually be done with sufficient accuracy by computing the total lateral pressure at the strip (see Fig. 1-6) level,

$$q_{h,I} = q_h + \Delta q_h \quad (1\text{-}1)$$

q_h = Rankine or Coulomb lateral earth pressure, taking into account backfill slope and any uniform surcharge

Δq_h = lateral pressure from any concentrated backfill surcharge; obtain using your computer program SMBLP1

With the average pressure obtained from Eq. (1-1), the strip tensile force can be computed as

$$T_i = Acq_{h,I} \quad (1\text{-}1a)$$

Where A_c = contributory area, computed (Including the Horizontal spacing s) as

$$A_c = (h_1 + h_1 + 1)s/2$$

Only should routinely make a computational check:

$$\sum T_i = S \text{ X } (P_{ah} + \text{area of } \Delta q \text{ diagram})$$

That is the sum of the several tensile reinforcement forces should equal the lateral-earth-pressure diagram rationed from a unit width to the actual reinforcement spacing s.

3. Compute the strip lengths L_e of fig 1.5 that are required to develop a friction resistance
$F_r = T_i$ X SF (or $L_{e,\text{ Computed}}$ X SF). From these lengths and the Rankine wedge zone we can then determine the overall strip length L_o to use. It is common to use a single length for the full wall height so that the assembly crew does not have to be concerned with using an incorrect length is based on soil to strip friction of f= tanδ, where δ = some fraction of φ such as 1.0, 0.8, 0.6φ. What to use depends on the roughness of the strip. For rough materials use δ =φ; for smooth metal strips use δ = 20̊ to 25̊.

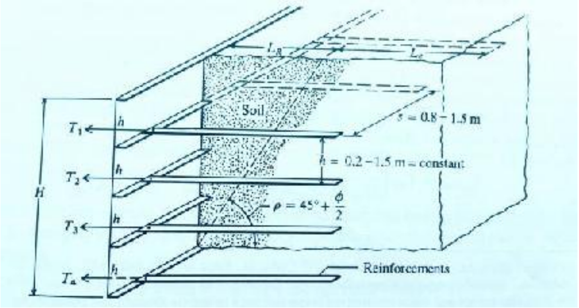


Figure 1.7; Typical range in reinforcement spacing for reinforced earth walls.

For strips of b x L_e geotextile sheets of base width L_e, both sides resist in friction. For round bars the perimeter resists friction. In both cases friction is the product of X normal pressure on the reinforcement. Using consistent units, this approach gives the following reinforcements:

Strip: $F_r = 2(yz_i)\,(b \text{ X } L_e) \tan\delta > T_i \text{ X SF}$
Rod : $F_r = 2\pi\,(yz_i)\,L_e \tan\delta > T_i \text{ X SF}$
Sheet : $F_r = 2(yz_i)\,(1 \text{ X } L_e) \tan\delta > T_i \text{ X SF}$

Where b= strip width, D = Rod diameter, and 1= unit sheet width

4. Next compute the reinforcement area for strips b X t and for rods with bar diameter D. for wire and geotextile grids, obtain the tension force per some unit of width. For geotextile sheets look in the manufacturer's catalog to find a fabric with a suitable strength.
For these materials a suitable SF must be used to reduce the ultimate tensile strength of metal strips and bars to a design value or the geotextile strength. To a design value, for metals it is common to use some SF such as 1.5 to 1.67; however, for both metals and geotextiles we can compute an SF based on partial safety factors as follows:

$$T_{allow} = T_{ult}\left(\frac{1}{SF_{id} \text{ X } SF_{cr} \text{ X } SF_{cd} \text{ X } SF_{bd} \text{ X } SF_{if} \text{ X } SF_{\varphi}}\right) \quad (1.3)$$

Where T_{allow} = Allowable Tensile Stress
T_{ult} = Ultimate Tensile Stress
SF_{id} = Installation damage factor, 1.1 to 1.5 for geotextiles; 1 for metal
SF_{cr} = Creep Factor (1.0 to 3.0 for geotextiles; 1 for metal)
SF_{cd} = Factor for chemical damage or corrosion (1.0 to 1.5 for Geotextiles; 1.0 to 1.2 for metal)
SF_{bd} = Factor for biological degradation (1.0 to 1.3 for Geotextiles; 1.0 to 1.2 for metal)
SF_{if} = Imprtance factor (1.0 to 1.5)
SF_{φ} = Genral Factor; (1.0 for Geotextiles; 1.3 to 1.4 for metal)

Let us compute an allowable tensile stress fa for steel strip based on 350 MPa steel (factors not shown are 1.0) as

Fa = (350x1)/ (1.1x1.2x1.3) = 350/ 1.716 = 204 ~ 200MPa

Let us now consider a geotextile example. From the 1995 specifier's guide we find an Amoco 2044 woven (W) geotextile with a wide-width tensile strength, using the ASTMD 4595 method, of 70.05 kN/M in both the MD (along the roll) directions. The Allowable tensile strength is computed using Eq.(1.3). Substituting some estimated values, we obtain

$$T_{allow} = (70.05x1)/(1.5x2.0x1.2x1.1x1.1x1.0) = 70.05/4.356 = 16.08 \sim 16.0 \text{ kN/m}$$

III. GENERAL COMMENTS

1. Between manufacturers.
2. With fabric type and grade. For Example, woven fabric is usually stronger than film fabric and additionally has a larger coefficient of friction.
3. With direction. The MD direction (Machine Direction, also warp; that is, with the roll) is stronger than (or as strong as) the XD direction (cross-machine, or fill; that is, across the roll-transverse to the the roll length). Sometimes the strength difference is on the order of XD~ 0.5MD. This means that attention to th strength direction during placing may be Critical.

REFERANCES

1. Foundation Analysis and Design (Fifth Edition) by Joseph E. Bowles

Mobile Ad Hoc Network

Monika Suhag[1], Sonia Choudhary[2]

[1,2]*Department of Computer Science & Engineering, Ganga Institute of Technology and Management, Kablana, Jhajjar, Haryana, INDIA*

ABSTRACT: Mobile Ad hoc Networks have been highly vunerable to attacks due to the dynamic nature of its network infrastructure. Among these attacks ,routing attacks have received considerable attention since it could cause the most devastating damage to Manet even though there exist several intrusion responsr techniques to mitigate such critical attacks ,exixting solutions typically attempt to isolate malicious nodes based on binary or naïve fuzzy response decision . however ,binary responses may result in the unexpected network partition ,causing additional damages to the network infrastructure and naïve fuzzy responses could lead to uncertainty in countering routing attacks in Manet .In this paper we propose a risk_aware response mechanism to systematically cope with the identified routing attacks.our risk aware approach is based on an extended dempster _shafer mathematically theory of evidence introducing a notion of importance factors .

I. INTRODUCTION

A mobile ad hoc network (MANET) is a collection of mobile devices that can communicate with each other without the use of a predefined infrastructure or centralized administration. In addition to freedom of mobility, a MANET can be constructed quickly at a low cost, as it does not rely on existing network infrastructure. Due to this flexibility, a MANET is attractive for applications such as disaster relief, emergency operations, military service, maritime communications, vehicle networks, casual meetings, campus networks, robot networks, and so on.

Unlike the conventional network, a MANET is characterized by having a dynamic, continuously changing network topology due to mobility of nodes [1]. This feature makes it difficult to perform routing in a MANET compared with a conventional wired network.

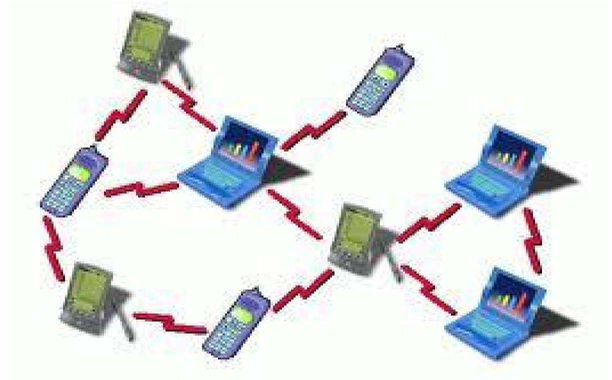


Fig.1.1 Mobile Ad-Hoc Network

Another characteristic of a MANET is its resource constraints, that is, limited bandwidth and limited battery power. This characteristic makes routing in a MANET an even more challenging task. Therefore, early work in MANET research focused on providing routing service with minimum cost in terms of bandwidth and battery power.

Currently, several efficient routing protocols have been proposed. These protocols can be classified into two categories: reactive routing protocols and proactive routing protocols. In reactive routing protocols, such as the Ad hoc On Demand Distance Vector (AODV) protocol [2], nodes find routes only when required. In proactive routing protocols, such as the Optimized Link State Routing (OLSR) protocol [3], nodes obtain routes by periodic exchange of topology information. Most of these routing protocols rely on cooperation between nodes due to the lack of a centralized administration and assume that all nodes are trustworthy and well-behaved.

Fig.1.2 Example of MANET

The survey has been done on the current state of the art of attacks on the network layer, that is, routing attacks such as link spoofing, wormhole attacks, and colluding misrelay attacks, as well as countermeasures in a MANET. Then, an overview of countermeasures for each attack and an overview of routing protocols in a MANET.

1.1 MANET'S FEATURES AND THEIR IMPACT ON SECURITY

The features of MANETs make them more vulnerable to attacks and misbehavior than traditional networks, and impose the security solution to be different from those used in other networks. These features are:

- **Infrastructure-less**: Central servers, specialized hardware, and fixed infrastructures are necessarily absent. The lack of infrastructure precludes the deployment of hierarchical host relationships; instead, nodes uphold egalitarian relationships.

That is, they assume contributory collaborative roles in the network rather than ones of dependence. i.e any security solution should rely on cooperative scheme instead of centralized one.

- **Wireless links use**: The use of wireless links renders a wireless ad hoc network susceptible to attacks. Unlike wired networks where an adversary must gain physical access to the network wires or pass through several lines of defense at firewalls and gateways, attacks on a wireless ad-hoc network can come from all directions and target at any node. Hence, a wireless ad hoc network will not have a clear line of defense, and every node must be prepared to threats. Moreover, since the channel is widely accessible, the MAC protocols used in ad hoc networks, such IEEE802.11, rely on trusted cooperation in a neighborhood to ensure channel access, which presents vulnerability.
- **Multi-hop**: Because the lack of central routers and gateways, hosts are themselves routers, then packets follow multi-hop routes and pass through different mobile nodes before arriving to the destination. Because of the possible untrustworthy of such nodes, this feature presents a serious vulnerability.
- **Nodes movement autonomy**: mobile nodes are autonomous units that are capable of roaming independently. This means that tracking down a particular mobile node in a large scale ad hoc network cannot be done easily.
- **Amorphous**: Nodes mobility and wireless connectivity allow nodes to enter and leave the network spontaneously. Therefore, the network topology has no form regarding both the size and the shape. Hence, any security solution must take this feature into account.
- **Power limitation**: Ad hoc enabled mobile nodes are small and lightweight; therefore, they are often supplied with limited power resources, small batteries, to ensure portability. The security solution should take this restraint into account. Furthermore, this limitation causes vulnerability since a node powering-on can cause its break-down. Thereby, attackers may targets some nodes batteries to disconnect them, even to make network partition. This is called energy starvation attack or sleep deprivation torture attack [10].
- **Memory and computation power limitation**: Ad hoc enabled mobile nodes have limited storage devices and weak computational capabilities. High complexity security solutions employed, as cryptography, should take these constraints into consideration.
- **Dynamic topologies**: Nodes are free to move arbitrarily; thus, the network topology--which is typically multihop may change randomly and rapidly at unpredictable times, and may consist of both bidirectional and unidirectional links.
- **Limited physical security**: Mobile wireless networks are generally more prone to physical security threats than are fixed- cable nets. The increased possibility of eavesdropping, spoofing, and denial-of-service attacks should be carefully considered. Existing link security techniques are often applied within wireless networks to reduce security threats. As a benefit, the decentralized nature of network control in MANETs provides additional robustness against the single points of failure of more centralized approaches.

II. ESSENTIALS AND VULNERABILITIES OF AD-HOC NETWORKS

To ensure proper operation, several attributes of these networks have to be protected against defects and more importantly against malicious intent. [1, 4]

- **Availability**

Availability is the most basic requirement of any network. If the networks connection ports are unreachable, or the data routing and forwarding mechanisms are out of order, the network would cease to exist.

- **Confidentiality**

Confidentiality describes the need to protect the data roaming in the network from being understood by unauthorized parties. Confidentiality can be achieved by encrypting essential information so only the communicating nodes can analyze and understand it.

- **Authenticity**

Authenticity is crucial to keep eavesdroppers out of the network. With many services applicable in ad hoc networks (and other kinds of networks too, for that matter), it is important to ensure that when communicating with a certain node, that node is really who/what we expect it to be (node authentication). Message authentication ensures that the contents of a message are valid.

- **Integrity**

Integrity of communication data is required to ensure that the information is passed on between nodes has not been altered in any way. Data can be altered both intentionally and accidentally (for example through hardware glitches, or interference in the case of wireless connections).

III. TYPES OF ATTACKS

It includes any action that intentionally aims to cause any damage to the network; it can be divided according to their origins or their nature.

Origin based classification splits attacks up into two categories; external and internal, whereas, nature based classification splits them up into passive attacks and active attacks

External attacks: This category Includes attacks launched by a node that do not belong to the logical network, or is not allowed to access to it. Such a node penetrates the network area to launch its attack .

Internal attacks: This category includes attacks launched by an internal compromised node; It is a more several kind of threat to the network since the proposed defense toward external attacks is ineffective against compromised and internal malicious nodes.

Passive attacks: A passive attack is a continuous collection of information; this information would be used later when launching an active attack. That means the attacker eavesdrops packets and analyzes them to pick up required information. The security attribute that must be provided here is information confidentiality.

Active attacks: Include almost all the other attacks launched by actively interacting with victims, like sleep deprivation torture that aims the batteries charges, hijacking, in which the attacker takes control of a communication between two entities and masquerades as one of them, jamming, that causes channel unavailability, attacks against routing protocols, etc... Most of these attacks result in a denial of service (DoS) that is degradation or a complete halt in communication between nodes.

IV. ROUTING PROTOCOLS IN MANETS

Efficient routing of packets is a primary manet Challenge. Manets use multihop rather than single-hop routing to deliver packets to their destination. The goal of routing in a MANET is to discover the most recent topology of a continuously changing network to find a correct route to a specific node. At network layer, routing protocols are used to find route for transmission of packets. Routing is the most fundamental research issue in ad hoc networking. Mobile Ad Hoc Network presents unique advanced challenges, including the design of protocols for mobility management, effective routing, data transport, security, power management and Quality of Service provisioning. Many routing protocols have been proposed for MANETs with the goal of making the route selection efficient. Since the nodes move randomly, the topology of the network changes with time. Dynamically changing topology and lack of centralized control make the design of a routing protocol challenging. Routing Protocols used in Mobile Ad Hoc Networks must automatically adjust to environments that can vary between the extreme high mobility with low bandwidth and low mobility with high bandwidth.

4.1 PRO-ACTIVE PROTOCOLS

They attempt to maintain consistent up-to-date routing information from each node to every other node in the network. These protocols require each node to maintain one or more tables to store routing information, and any changes in network topology need to be reflected by propagating updates throughout the network in order to maintain a consistent network view.

4.1.1 DSDV

Dynamic Destination-Sequenced Distance-Vector routing algorithm[6].

Based on Bellman-Ford routing algorithm:- Every mobile station maintains and uses for routing packets ,a routing table, listing all available destinations, the number of hops to reach the destination and the sequence number assigned by the destination. The sequence number distinguishes old routes from new ones. Stations periodically and on significant changes transmit their routing tables to their neighbors.

Destination-Sequenced Distance-Vector Routing (DSDV) is a table-driven routing scheme for ad hoc mobile networks based on the Bellman-Ford algorithm. It was developed by C. Perkins and P.Bhagwat in 1994. The main contribution of the algorithm was to solve the routing loop problem. Each entry in the routing table contains a sequence number, the sequence numbers are generally even if a link is present; else, an odd number is used. The number is generated by the destination, and the emitter needs to send out the next update with this number. Routing information is distributed between nodes by sending *full dumps* infrequently and smaller incremental updates more frequently.

4.1.2 GSR

Global State Routing.

Based on link state routing but avoids flooding of routing messages. Each node maintains a Neighbor list, a Topology table, a Next hop table and a Distance table. The routing messages are generated on a link change and the node updates its topology table if the sequence number of the message is newer than the number stored in the table.

The link-state protocol is performed by every *switching node* in the network (i.e. nodes that are prepared to forward packets; in the Internet, these are called routers). The basic concept of link-state routing is that every node constructs a *map* of the connectivity to the network, in the form of a graph, showing which nodes are connected to which other nodes. Each node then independently calculates the next best logical *path* from it to every possible destination in the network. The collection of best paths will then form the node's routing table.

This contrasts with distance-vector routing protocols, which work by having each node share its **routing table** with its neighbors. In a link-state protocol the only information passed between nodes is **connectivity related**.

The routing messages are generated on a link change as in link state protocols. On receiving a routing message, the node updates its Topology table if the sequence number of the message is newer than the sequence number stored in the table. After this the node reconstructs its routing table and broadcasts the information to its neighbor.

4.1.3 FSR

Fisheye State Routing

In FSR each update message contains information about closest nodes frequently and farther nodes as required i.e. detail and accuracy of information decreases as the distance from node increases.

Fisheye State Routing (FSR) is an improvement of GSR. The large size of update messages in GSR wastes a considerable amount of network bandwidth. In FSR, each update message does not contain information about all nodes. Instead, it exchanges information about closer nodes more frequently than it does about farther nodes thus reducing the update message size. So each node gets accurate information about neighbors and the detail and accuracy of information decreases as the distance from node increases. Figure 1 defines the scope of fisheye for the center (red) node. The scope is defined in terms of the nodes that can be reached in a certain number of hops. The center node has most accurate information about all nodes in the white circle and so on. Even though a node does not have accurate information about distant nodes, the packets are routed correctly because the route information becomes more and more accurate as the packet moves closer to the destination. FSR scales well to large networks as the overhead is controlled in this scheme.

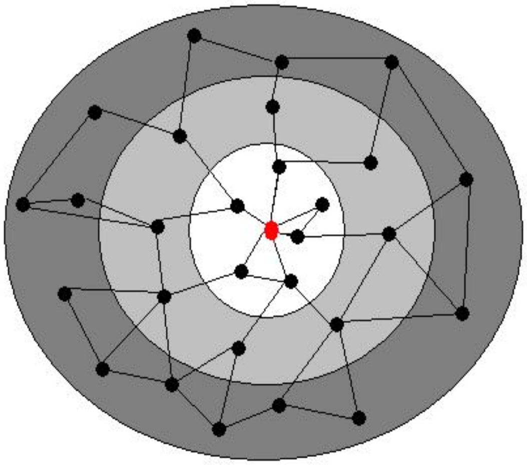


Fig 4.1.3. Accuracy of information in FSR

4.1.4 OLSR

Optimized Link State Routing.

In OLSR each node selects a set of its neighbor nodes as “multipoint relays”(MPR). These nodes announce to the network periodically their reach ability to the nodes that have selected them as MPR. This technique reduces the size of control messages as well as minimizes flooding of control traffic.

OLSR makes use of "Hello" messages to find its one hop neighbors and its two hop neighbors through their responses. The sender can then select its multipoint relays (MPR) based on the one hop node that offers the best routes to the two hop nodes. Each node has also an MPR selector set, which enumerates nodes that have selected it as an MPR node. OLSR uses topology control (TC) messages along with MPR forwarding to disseminate neighbor information throughout the network. *Host and network association* (HNA) messages are used by OLSR to disseminate network route advertisements in the same way TC messages advertise host routes.

4.2 RE-ACTIVE PROTOCOLS

Reactive Routing protocols are based on finding routes between two nodes , when it is required. This is different from traditional Proactive Routing Protocols in which nodes periodically sends messages to each other in order to maintain routes. Only Reactive Protocols are considered in this article, as they are extensively studied and used in MANETs. Among many Reactive Routing Protocols, only three of them are described below as they are mostly studied.

4.2.1 AODV

Ad hoc On Demand Distance Vector Routing

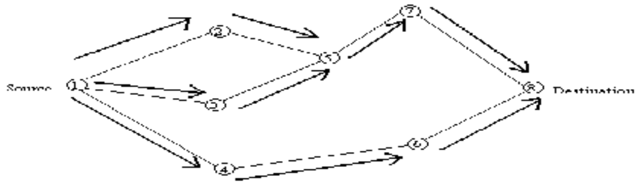
This algorithm enables dynamic, self-starting multi hop routing between nodes. This method does not require nodes to maintain routes to destinations that are out of active communication.

It is 1st protocol to do multicasting as well as unicasting. Sequence no. is used by routers.

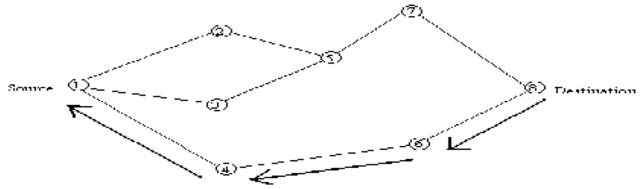
A reverse path is followed by it.

To find a path to the destination, the source broadcasts a route request packet. The neighbors in turn broadcast the packet to their neighbors till it reaches an intermediate node that has a recent route information about the destination or till it reaches the destination (Figure 3a). A node discards a route request packet that it has already seen. The route request packet uses sequence numbers to ensure that the routes are loop free and to make sure that if the intermediate nodes reply to route requests, they reply with the latest information only.

When a node forwards a route request packet to its neighbors, it also records in its tables the node from which the first copy of the request came. This information is used to construct the reverse path for the route reply packet. AODV uses only symmetric links because the route reply packet follows the reverse path of route request packet. As the route reply packet traverses back to the source (Figure 3b), the nodes along the path enter the forward route into their tables.



(a) Propogation of Route Request (RREQ) Packet



(b) Path taken by the Route Reply (RREP) Packet

Fig.4.2.1.AODV Routing Protocol

4.2.2TORA

Temporary-Ordered routing Algorithm

It is an adaptive routing protocol for multihop networks and has following features.

- Distributed execution ,
- Loop free and multipath routing,
- Reactive or Proactive root establishment.
- Localization of algorithmic reactions to topological changes.
- based on the concept of link reversal
- It finds multiple routes from a source node to a destination node

4.2.3 ZRP

Zone Routing Protocol

It combines the advantages of the proactive (for nodes within the zone) and reactive (for nodes outside) approaches

4.3 HYBRID APPROACH

A recently proposed hybrid approach6 captures the advantages of on-demand and optimized linkstate routing for wireless sensor networks. This algorithm discovers the route to each node only when it is needed. However, route discovery does not occur through simple flooding but through a mechanism similar to multipoint relays. The algorithm defines three types of nodes: master, gateway, and plain. A group of nodes selects a master to form a piconet and then synchronizes and maintains the neighbor list. A node can be a master in only one piconet, but it can be a plain member in any number of piconets. Gateway nodes belong to two or more piconets. Only masters and gateways forward routing information; plain nodes receive and process this information, but they do not forward it.

4.3.1 ZRP

Zone Routing Protocol

It combines the advantages of the proactive (for nodes within the zone) and reactive (for nodes outside) approaches

V. ROUTING ATTACKS AGAINST MANET PROTOCOLS

MANETs are much more vulnerable to attack than wired network. This is because of the following reasons:

- **Open Medium** - Eavesdropping is easier than in wired network.
- **Dynamically Changing Network Topology** – Mobile Nodes comes and goes from the network, thereby allowing any malicious node to join the network without being detected.
- **Cooperative Algorithms** - The routing algorithm of MANETs requires mutual trust between nodes which violates the principles of Network Security.
- **Lack of Centralized Monitoring** - Absence of any centralized infrastructure prohibits any monitoring agent in the system.
- **Lack of Clear Line of Defense** - The only use of I line of defense - attack prevention may not succeed. In addition to prevention, we need II line of defense - detection and response.

Table 1: Security Attacks on Protocol Stacks

LAYERS	ATTACKS
Multilayer Attack	DOS, Impersonation, Reply, Man in the middle
Application Layer	Repudiation, Data corruption
Transport Layer	Session hijacking, SYN flooding
Network Layer	Wormhole , Black whole, Flooding, Resource consumption ,Location disclosure
Data link Layer	Traffic analysis, Monitoring, Disruption MAC,WEP weakness
Physical layer	Jamming, interception, Eavesdropping

5.1 FLOODING ATTACK

The aim of the flooding attack is to exhaust the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance. For example, in AODV protocol, a malicious node can send a large number of RREQs in a short period to a destination node that does not exist in the network. Because no one will reply to the RREQs, these RREQs will flood the whole network. As a result, all of the node battery power, as well as network bandwidth will be consumed and could lead to denial-of-service. A flooding attack can decrease throughput by 84 percent.

5.1.1 SOLUTIONS TO THE FLOODING ATTACK

In this approach, each node monitors and calculates the rate of its neighbors' RREQ [11]. If the RREQ rate of any neighbor exceeds the predefined threshold, the node records the ID of this neighbor in a blacklist. Then, the node drops any future RREQs from nodes that are listed in the blacklist. One limitation of this approach is that it cannot prevent against the flooding attack in which the flooding rate is below the threshold. Another drawback of this approach is that if a malicious node impersonates the ID of a legitimate node and broadcasts a large number of RREQs, other nodes might put the ID of this legitimate node on the blacklist by mistake.

Another adaptive technique is to mitigate the effect of a flooding attack in the AODV protocol. This technique is based on statistical analysis to detect malicious RREQ floods and avoid the forwarding of such packets. In this approach, each node monitors the RREQ it receives and maintains a count of RREQs received from each sender during the preset time period. The RREQs from a sender whose RREQ rate is above the threshold will be dropped without forwarding. Unlike the method proposed in [11], where the threshold is set to be fixed, this approach determines the threshold based on a statistical analysis of RREQs. The key advantage of this approach is that it can reduce the impact of the attack for varying flooding rates.

5.2 BLACKHOLE ATTACK

In a blackhole attack, a malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. For example, in AODV, the attacker can send a fake RREP (including a fake destination sequence number that is fabricated to be equal or higher than the one contained in the RREQ) to the source node, claiming that it has a sufficiently fresh route to the destination node. This causes the source node to select the route that passes through the attacker. Therefore, all traffic will be routed through the attacker, and therefore, the attacker can misuse or discard the traffic. Figure shows an example of a blackhole attack, where attacker A sends a fake RREP to the source node S, claiming that it has a sufficiently fresher route than other nodes. Since the attacker's advertised sequence number is higher than other nodes' sequence numbers, the source node S will choose the route that passes through node A.

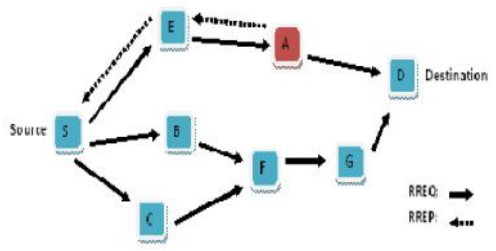


Fig.5.2 Blackhole Attack

5.2.1 SOLUTIONS TO BLACKHOLE ATTACK

The route confirmation request (CREQ) and route confirmation reply (CREP) are used to avoid the blackhole attack. In this approach, the intermediate node not only sends RREPs to the source node but also sends CREQs to its next-hop node toward the destination node. After receiving a CREQ, the next-hop node looks up its cache for a route to the destination. If it has the route, it sends the CREP to the source. Upon receiving the CREP, the source node can confirm the validity of the path by comparing the path in RREP and the one in CREP. If both are matched, the source node judges that the route is correct. One drawback of this approach is that it cannot avoid the blackhole attack in which two consecutive nodes work in collusion, that is, when the next-hop node is a colluding attacker sending CREPs that support the incorrect path.

Another solution requires a source node to wait until a RREP packet arrives from more than two nodes. Upon receiving multiple RREPs, the source node checks whether there is a shared hop or not. If there is, the source node judges that the route is safe. The main drawback of this solution is that it introduces time delay, because it must wait until multiple RREPs arrive.

5.3 *LINK WITHHOLDING ATTACK*

In this attack, a malicious node ignores the requirement to advertise the link of specific nodes or a group of nodes, which can result in link loss to these nodes. This type of attack is particularly serious in the OLSR protocol.

5.3.1 SOLUTIONS TO WITHHOLDING ATTACK

By withholding a TC message in OLSR, a malicious node can isolate a specific node and prevent it from receiving data packets from other nodes. After analyzing and evaluating the impact of this kind of attack in detail, a detection technique is proposed based on observation of both a TC message and a HELLO message generated by the MPR nodes. If a node does not hear a TC message from its MPR node regularly but hears only a HELLO message, a node judges that the MPR node is suspicious and can avoid the attack by selecting one or more extra MPR nodes.

The main drawback of this approach is that it cannot detect the attack that is launched by two colluding consecutive nodes, where the first attacker pretends to advertise a TC message, but the second attacker drops this TC message.

5.4 LINK SPOOFING ATTACK

In a link spoofing attack, a malicious node advertises fake links with non-neighbors to disrupt routing operations. For example, in the OLSR protocol, an attacker can advertise a fake link with a target's two-hop neighbors. This causes the target node to select the malicious node to be its MPR. As an MPR node, a malicious node can then manipulate data or routing traffic, for example, modifying or dropping the routing traffic or performing other types of DoS attacks.

Figure shows an example of the link spoofing attack in an OLSR MANET. In the figure, we assume that node A is the attacking node, and node T is the target to be attacked. Before the attack, both nodes A and B are MPRs for node T. During the link spoofing attack, node A advertises a fake link with node T's two-hop neighbor, that is, node D. According to the OLSR protocol, node T will select the malicious node A as its only MPR since node A is the minimum set that reaches node T's two-hop neighbors. By being node T's only MPR, node A can then drop or withhold the routing traffic generated by node T.

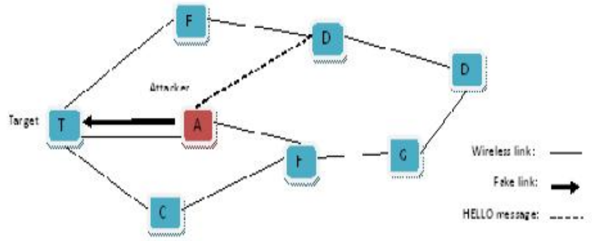


Fig. 5.4 Link Spoofing Attack

5.4.1 SOLUTIONS TO LINK SPOOFING ATTACK

To detect a link spoofing attack, a location information-based detection method is used by using cryptography with a GPS and a time stamp. This approach requires each node to advertise its position obtained by the GPS and the time stamp to enable each node to obtain the location information of the other nodes. This approach detects the link spoofing by calculating the distance between two nodes that claim to be neighbors and checking the likelihood that the link is based on a maximum transmission range. The main drawback of this approach is that it might not work in a situation where all MANET nodes are not equipped with a GPS. Furthermore, attackers can still advertise false information and make it hard for other nodes to detect the attack[19].

Another technique to detect the link spoofing attack is by adding two-hop information to a HELLO message. In particular, the proposed solution requires each node to advertise its two-hop neighbors to enable each node to learn complete topology up to three hops and detect the inconsistency when the link spoofing attack is launched. The main advantage of this approach is that it can detect the link spoofing attack without using special hardware such as a GPS or requiring time synchronization. One limitation of this approach is that it might not detect link spoofing with nodes further away than three hops.

5.5 REPLAY ATTACK

In a MANET, topology frequently changes due to node mobility. This means that current network topology might not exist in the future. In a replay attack [20], a node records another node's valid control messages and resends them later. This causes other nodes to record their routing table with stale routes. Replay attack can be misused to impersonate a specific node or simply to disturb the routing operation in a MANET.

5.5.1 SOLUTIONS TO REPLAY ATTACK

A solution to protect a MANET from a replay attack is by using a time stamp with the use of an asymmetric key. This solution prevents the replay attack by comparing the current time and time stamp contained in the received message. If the time stamp is too far from the current time, the message is judged to be suspicious and is rejected. Although this solution works well against the replay attack, it is still vulnerable to a wormhole attack where two colluding attackers use a high speed network to replay messages in a far-away location with almost no delay.

5.6WORMHOLE ATTACK

A wormhole attack [21] is one of the most sophisticated and severe attacks in MANETs. In this attack, a pair of colluding attackers record packets at one location and replay them at another location using a private high speed network. The seriousness of this attack is that it can be launched against all communications that provide authenticity and confidentiality. Figure 3 shows an example of the wormhole attack against a reactive routing protocol. In the figure, we assume that nodes *A*1 and *A*2 are two colluding attackers and that node S is the target to be attacked. During the attack, when source node S broadcasts an RREQ to find a route to a destination node D, its neighbors C and E forward the RREQ as usual. However, node *A*1, which received the RREQ, forwarded by node C, records and tunnels the RREQ to its colluding partner *A*2. Then, node *A*2 rebroadcasts this RREQ to its neighbor H. Since this RREQ passed through a high-speed channel, this RREQ will reach node D first. Therefore, node D will choose route D-H-C-S to unicast an RREP to the source node S and ignore the same RREQ that arrived later. As a result, S will select route S-CH- D that indeed passed through *A*1 and *A*2 to send its data.

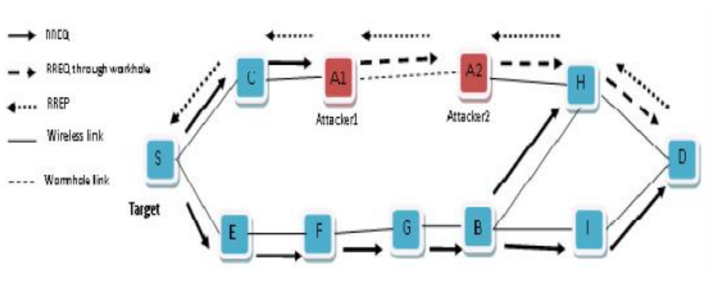


Fig. 5.6 Wormhole Attack

5.6.1 *SOLUTIONS TO WORMHOLE ATTACK*

Packet leashes are proposed to detect and defend against the wormhole attack. In particular, the authors proposed two types of leashes: temporal leashes and geographical leashes. For the temporal leash approach, each node computes the packet expiration time, *te*, based on the speed of light *c* and includes the expiration time, *te*, in its packet to prevent the packet from traveling further than a specific distance, *L*. The receiver of the packet checks whether or not the packet expires by comparing its current time and the *te* in the packet. The authors also proposed TIK, which is used to authenticate the expiration time that can otherwise be modified by the malicious node. The main drawback of the temporal leash is that it requires all nodes to have tightly synchronized clocks.

For the geographical leash, each node must know its own position and have loosely synchronized clocks. In this approach, a sender of a packet includes its current position and the sending time. Therefore, a receiver can judge neighbor relations by computing distance between itself and the sender of the packet. The advantage of geographic leashes over temporal leashes is that the time synchronization need not to be highly tight.

Another approach is based on protection against a wormhole attack in the OLSR protocol. This approach is based on location information and requires the deployment of ijhnnja public key infrastructure and timestamp synchronization between all nodes. In this approach, a sender of a HELLO message includes its current position and current time in its HELLO message. Upon receiving a HELLO message from a neighbor, a node calculates the distance between itself and its neighbor, based on a position provided in the HELLO message. If the distance is more than the maximum transmission range, the node judges that the HELLO message is highly suspicious and might be tunneled by a wormhole attack.

5.7 COLLUDING MISRELAY ATTACK

In this attack, multiple attackers work in collusion to modify or drop routing packets to disrupt routing operation in a MANET. This attack is difficult to detect by using the conventional methods such as *watchdog* and *pathrater* [23,24]. Figure shows an example of this attack. Consider the case where node *A*1 forwards routing packets for node T. In the figure, the first attacker *A*1 forwards routing packets as usual to avoid being detected by node T. However, the second attacker A2 drops or modifies these routing packets. In [19] the authors discuss this type of attack in OLSR protocol and show that a pair of malicious nodes can disrupt up to 100 percent of data packets in the OLSR MANET.

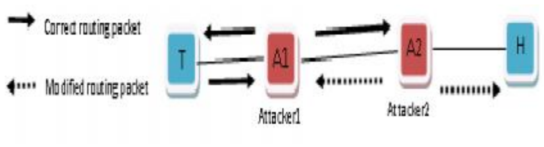


Fig. 5.7 Colluding Attack

5.7.1 SOLUTIONS TO COLLUDING ATTACK

A conventional acknowledgment-based approach might detect this type of attack in a MANET, especially in a proactive MANET, but because routing packets destined to all nodes in the network require all nodes to return an ACK, this could lead to a large overhead, which is considered to be inefficient [22].

To detect an attack in which multiple malicious nodes attempt to drop packets is by requiring each node to tune their transmission power when they forward packets. As an example, the author studies the case where two colluding attackers drop packets. The proposed solution requires each node to increase its transmission power twice to detect such an attack. However, this approach might not detect the attack in which three colluding attackers work in collusion. In general, the main drawback of this approach is that even if we require each node to increase transmission power to be *K* times, we still cannot detect the attack in which *K* + 1 attackers work in collusion to drop packets. Therefore, further work must be done to counter against this type of attack efficiently.

ADVANTAGES

The following are the advantages of MANETs:

- They provide access to information and services regardless of geographic position.
- These networks can be set up at any place and time.

DISADVANTAGES

Some of the disadvantages of MANETs are:

- Limited resources.
- Limited physical security.
- Intrinsic mutual trust vulnerable to attacks.
- Lack of authorization facilities.

- Volatile network topology makes it hard to detect malicious nodes.
- Security protocols for wired networks cannot work for ad hoc networks.

VI. FUTURE WORK

Future research should be focused not only on improving the effectiveness of the security schemes but also on minimizing the cost to make them suitable for a MANET environment. Furthermore, each proposed solution can work only with a specific attack and is still vulnerable to unexpected attacks. The Security research area is still open as many of the provided solutions are designed keeping a limited size scenario and limited kind of attacks and vulnerabilities. Therefore, MANET researchers should also focus on exploring, as well as preventing all possible attacks to make a MANET a secure and reliable network.

REFERENCES

[1] Marco Conti, Body, Personal, "Local Ad Hoc Wireless Networks", in Book The Handbook of Ad Hoc Wireless Networks (Chapter 1), CRC Press LLC, 2003.

[2] C. Perkins, E Royer,“Ad Hoc On-Demand Distance Vector Routing”, 2nd IEEE Wksp. Mobile Comp. Sys.and Apps., 1999.

[3] D. Johnson, D. Maltz, “Dynamic Source Routing in Ad Hoc Wireless Networks”, Mobile Computing, Imielinski and H. Korth, Ed., Kluwer, 1996. 3] M.S. Corson, J.P. Maker, and J.H. Cernicione, Internet-based Mobile Ad Hoc Networking, IEEE Internet Computing, pages 63–70, July-August 1999.

[4] Amitabh Mishra, Ketan M. Nadkarni, "Security in Wireless Ad Hoc Networks", in Book The Handbook of Ad Hoc Wireless Networks (Chapter 30), CRC Press LLC, 2003.

[5] Lidong Zhou, Zygmunt J. Hass, "Securing Ad Hoc Networks", IEEE Networks Special Issue on Network Security, November/December 1999.

Mobile Ad Hoc

Anil Dahiya[1]

[1]*Department of Computer Science &Engineering, Ganga Institute of Technology and Management, Kablana, Jhajjar, Haryana, INDIA*

Abstract: Mobile Ad hoc have been highly venerable to attacks due to the dynamic nature of its network infrastructure. Among these attacks ,routing attacks have received considerable attention since it could cause the most devastating damage to Mamet even though there exist several intrusion response techniques to mitigate such critical attacks ,exiting solutions typically attempt to isolate malicious nodes based on binary or naïve fuzzy response decision . however ,binary responses may result in the unexpected network partition ,causing additional damages to the network infrastructure and naïve fuzzy responses could lead to uncertainty in countering routing attacks in Mamet .In this paper we propose a risk, aware response mechanism to systematically cope with the identified routing attacks. our risk aware approach is based on an extended dempster _shafer mathematically theory of evidence introducing a notion of importance factors .

1. INTRODUCTION

A mobile ad hoc network (MANET) is a collection of mobile devices that can communicate with each other without the use of a predefined infrastructure or centralized administration. In addition to freedom of mobility, a MANET can be constructed quickly at a low cost, as it does not rely on existing network infrastructure. Due to this flexibility, a MANET is attractive for applications such as disaster relief, emergency operations, military service, maritime communications, vehicle networks, casual meetings, campus networks, robot networks, and so on.

Unlike the conventional network, a MANET is characterized by having a dynamic, continuously changing network topology due to mobility of nodes [1]. This feature makes it difficult to perform routing in a MANET compared with a conventional wired network.

Network: Another characteristic of a MANET is its resource constraints, that is, limited bandwidth and limited battery power. This characteristic makes routing in a MANET an even more challenging task. Therefore, early work in MANET research focused on providing routing service with minimum cost in terms of bandwidth and battery power.

Currently, several efficient routing protocols have been proposed. These protocols can be classified into two categories: reactive routing protocols and proactive routing protocols. In reactive routing protocols, such as the Ad hoc On Demand Distance Vector (AODV) protocol [2], nodes find routes only Infrastructure-less: Central servers, specialized hardware, and fixed infrastructures are necessarily absent. The lack of infrastructure precludes the deployment of hierarchical host relationships; instead, nodes uphold egalitarian relationships. That is, they assume contributory collaborative roles in the network rather than ones of dependence. i.e any security solution should rely on cooperative scheme instead of centralized one.

- Wireless links use: The use of wireless links renders a wireless ad hoc network susceptible to attacks. Unlike wired networks

when required. In proactive routing protocols, such as the Optimized Link State Routing (OLSR) protocol [3], nodes obtain routes by periodic exchange of topology information. Most of these routing protocols rely on cooperation between nodes due to the lack of a centralized administration and assume that all nodes are trustworthy and well-behaved.

Fig.1 Example of MANET

The survey has been done on the current state of the art of attacks on the network layer, that is, routing attacks such as link spoofing, wormhole attacks, and colluding misrelay attacks, as well as countermeasures in a MANET. Then, an overview of countermeasures for each attack and an overview of routing protocols in a MANET.

II. MANET'S FEATURES AND THEIR IMPACT ON SECURITY

The features of MANETs make them more vulnerable to attacks and misbehavior than traditional networks, and impose the security solution to be different from those used in other networks. These features are:

Infrastructure-less: Central servers, specialized hardware, and fixed infrastructures are necessarily absent. The lack of infrastructure precludes the deployment of hierarchical host relationships; instead, nodes uphold egalitarian relationships. That is, they assume contributory collaborative roles in the network rather than ones of dependence. i.e any

where an adversary must gain physical access to the network wires or pass through several lines of defense at firewalls and gateways, attacks on a wireless ad-hoc network can come from all directions and target at any node. Hence, a wireless ad hoc network will not have a clear line of defense, and every node must be prepared to threats. Moreover, since the channel is widely accessible, the MAC protocols used in ad hoc networks, such IEEE802.11, rely on trusted cooperation in a neighborhood to ensure channel access, which presents vulnerability.

- Multi-hop: Because the lack of central routers and gateways, hosts are themselves routers, then packets follow multi-hop routes and pass through different mobile nodes before arriving to the destination. Because of the possible untrustworthy of such nodes, this feature presents a serious vulnerability.

III. TYPES OF ATTACKS

It includes any action that intentionally aims to cause any damage to the network; it can be divided according to their origins or their nature.

Origin based classification splits attacks up into two categories; external and internal, whereas, nature based classification splits them up into passive attacks and active attacks

External attacks: This category Includes attacks launched by a node that do not belong to the logical network, or is not allowed to access to it. Such a node penetrates the network area to launch its attack .Internal attacks: This category includes attacks launched by an internal compromised node; It is a more several kind of threat to the network since the proposed defense toward external attacks is ineffective against compromised and internal malicious nodes.

Passive attacks: A passive attack is a continuous collection of information; this information would be used later when launching an active attack. That means the attacker eavesdrops packets and analyzes them to pick up required information. The security attribute that must be provided here is information confidentiality.

Active attacks: Include almost all the other attacks launched by actively interacting with victims, like sleep deprivation torture that aims the batteries charges, hijacking, in which the attacker takes control of a communication between two entities and masquerades as one of them, jamming, that causes channel unavailability, attacks against routing protocols, etc... Most of these attacks result in a denial of service (DoS) that is degradation or a complete halt in communication between nodes.

IV. ROUTING PROTOCOLS IN MANETS

Efficient routing of packets is a primary manet Challenge. Manets use multihop rather than single-hop routing to deliver packets to their destination. The goal of routing in a MANET is to discover the most recent topology of a continuously changing network to find a correct route to a specific node. At network layer, routing protocols are used to find route for transmission of packets. Routing is the most fundamental research issue in ad hoc networking. Mobile Ad Hoc Network presents unique advanced challenges, including the design of protocols for mobility management, effective routing, data transport, security, power management and Quality of Service provisioning.

Pro-Active Protocols: They attempt to maintain consistent up-to-date routing information from each node to every other node in the network. These protocols require each node to maintain one or more tables to store routing information, and any changes in network topology need to be reflected by propagating updates throughout the network in order to maintain a consistent network view.

Dynamic Destination-Sequenced Distance-Vector routing algorithm[6].Based on Bellman-Ford routing algorithm:- Every mobile station maintains and uses for routing packets ,a routing table, listing all available destinations, the number of hops to reach the destination and the sequence number assigned by the destination. The sequence number distinguishes old routes from new ones. Stations periodically and on significant changes transmit their routing tables to their neighbors.

Destination-Sequenced Distance-Vector Routing (DSDV) is a table-driven routing scheme for ad hoc mobile networks based on the Bellman-Ford algorithm. It was developed by C. Perkins and P.Bhagwat in 1994. The main contribution of the algorithm was to solve the routing loop problem. Each entry in the routing table contains a sequence number, the sequence numbers are generally even if a link is present; else, an odd number is used. The number is generated by the destination, and the emitter needs to send out the next update with this number. Routing information is distributed between nodes by sending *full dumps* infrequently and smaller incremental updates more frequently.

Global State Routing.: Based on link state routing but avoids flooding of routing messages. Each node maintains a Neighbor list, a Topology table, a Next hop table and a Distance table. The routing messages are generated on a link change and the node updates its topology table if the sequence number of the message is newer than the number stored in the table.

The link-state protocol is performed by every *switching node* in the network (i.e. nodes that are prepared to forward packets; in the Internet, these are called routers). The basic concept of link-state routing is that every node constructs a *map* of the connectivity to the network, in the form of a graph, showing which nodes are connected to which other nodes. Each node then independently calculates the next best logical *path* from it to every possible destination in the network. The collection of best paths will then form the node's routing table.

This contrasts with distance-vector routing protocols, which work by having each node share its routing table with its neighbors. In a link-state protocol the only information passed between nodes is connectivity related.

The routing messages are generated on a link change as in link state protocols. On receiving a routing message, the node updates its Topology table if the sequence number of the message is newer than the sequence number stored in the table. After this the node reconstructs its routing table and broadcasts the information to its neighbor.

Fisheye State Routing: In FSR each update message contains information about closest nodes frequently and farther nodes as required i.e. detail and accuracy of information decreases as the distance from node increases.

Fisheye State Routing (FSR) is an improvement of GSR. The large size of update messages in GSR wastes a considerable amount of network bandwidth. In FSR, each update message does not contain information about all nodes. Instead, it exchanges information about closer nodes more frequently than it does about farther nodes thus reducing the update message size.

V. RE-ACTIVE PROTOCOLS

Reactive Routing protocols are based on finding routes between two nodes , when it is required. This is different from traditional Proactive Routing Protocols in which nodes periodically sends messages to each other in order to maintain routes. Only Reactive Protocols are considered in this article, as they are extensively studied and used in MANETs. Among many

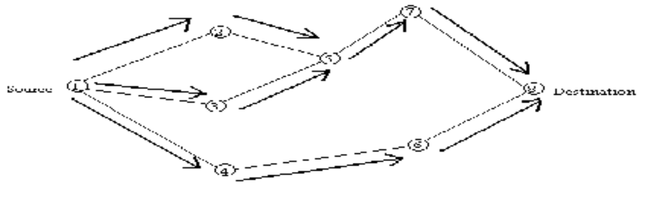
Reactive Routing Protocols, only three of them are described below as they are mostly studied.

Ad hoc On Demand Distance Vector Routing: This algorithm enables dynamic, self-starting multi hop routing between nodes. This method does not require nodes to maintain routes to destinations that are out of active communication. It is 1st protocol to do multicasting as well as unicasting. Sequence no. is used by routers.A reverse path is followed by it.

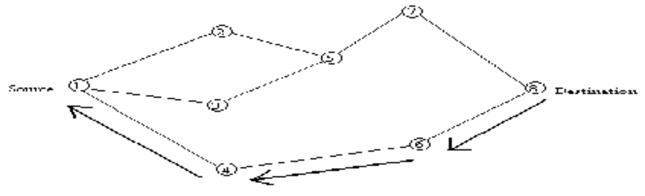
To find a path to the destination, the source broadcasts a route request packet. The neighbors in turn broadcast the packet to their neighbors till it reaches an intermediate node that has a recent route information about the destination or till it reaches the destination (Figure 3a). A node discards a route request packet that it has already seen. The route request packet uses sequence numbers to ensure that the routes are loop free and to make sure that if the intermediate nodes reply to route requests, they reply with the latest information only.

When a node forwards a route request packet to its neighbors, it also records in its tables the node from which the first copy of the request came. This information is used to construct the reverse path for the route reply packet. AODV uses only symmetric links because the route reply packet follows the reverse path of route request packet. As the route reply packet traverses back to the source (Figure 3b), the nodes along the path enter the forward route into their tables.

LAYERS	ATTACKS
Multilayer Attack	DOS, Impersonation, Reply, Man in the middle
Application Layer	Repudiation, Data corruption
Transport Layer	Session hijacking, SYN flooding
Network Layer	Wormhole , Black whole, Flooding, Resource consumption ,Location disclosure
Data link Layer	Traffic analysis, Monitoring, Disruption MAC,WEP weakness
Physical layer	Jamming, interception, Eavesdropping



(a) Propogation of Route Request (RREQ) Packet



(b) Path taken by the Route Reply (RREP) Packet

Fig.2.Aodv Routing Protocol

Temporary-Ordered routing Algorithm: It is an adaptive routing protocol for multihop networks and has following features.

- Distributed execution ,
- Loop free and multipath routing,
- Reactive or Proactive root establishment.
- Localization of algorithmic reactions to topological changes.
- based on the concept of link reversal
- It finds multiple routes from a source node to a destination node

Zone Routing Protocol It combines the advantages of the proactive (for nodes within the zone) and reactive (for nodes outside) approaches

Hybrid Approach: A recently proposed hybrid approach6 captures the advantages of on-demand and optimized linkstate routing for wireless sensor networks.

Zone Routing Protocol: It combines the advantages of the proactive (for nodes within the zone) and reactive (for nodes outside) approaches

VI. ROUTING ATTACKS AGAINST MANET PROTOCOLS

MANETs are much more vulnerable to attack than wired network. This is because of the following reasons:

- Open Medium - Eavesdropping is easier than in wired network.
- Dynamically Changing Network Topology – Mobile Nodes comes and goes from the network, thereby allowing any malicious node to join the network without being detected.
- Cooperative Algorithms - The routing algorithm of MANETs requires mutual trust between nodes which violates the principles of Network Security.
- Lack of Centralized Monitoring - Absence of any centralized infrastructure prohibits any monitoring agent in the system.
- Lack of Clear Line of Defense - The only use of I line of defense - attack prevention may not succeed. In addition to prevention, we need II line of defense - detection and response.

Security Attacks on Protocol Stacks:

Fig.3 Table of layers & related attacks

VII. FLOODING ATTACK

SOLUTIONS TO THE FLOODING ATTACK: In this approach, each node monitors and calculates the rate of its neighbors' RREQ [11]. If the RREQ rate of any neighbor exceeds the predefined threshold, the node records the ID of this neighbor in a blacklist. Then, the node drops any future RREQs from nodes that are listed in the blacklist. One limitation of this approach is that it cannot prevent against the flooding attack in which the flooding rate is below the threshold. Another drawback of this approach is that if a malicious node impersonates the ID of a legitimate node and broadcasts a large number of RREQs, other nodes might put the ID of this legitimate node on the blacklist by mistake.

Another adaptive technique is to mitigate the effect of a flooding attack in the AODV protocol. This technique is based on statistical analysis to detect malicious RREQ floods and avoid the forwarding of such packets. In this approach, each node monitors the RREQ it receives and maintains a count of RREQs received from each sender during the preset time period. The RREQs from a sender whose RREQ rate is above the threshold will be dropped without forwarding. Unlike the method proposed, where the threshold is set to be fixed, this approach determines the threshold based on a statistical analysis of RREQs. The key advantage of this approach is that it can reduce the impact of the attack for varying flooding rates.

VIII. BLACKHOLE ATTACK

In a blackhole attack, a malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. For example, in AODV, the attacker can send a fake RREP (including a fake destination sequence number that is fabricated to be equal or higher than the one contained in the RREQ) to the source node, claiming that it has a sufficiently fresh route to the destination node. This causes the source node to select the route that passes through the attacker. Therefore, all traffic will be routed through the attacker, and therefore, the attacker can misuse or discard the traffic. Figure shows an example of a blackhole attack, where attacker A sends a fake RREP to the source node S, claiming that it has a sufficiently fresher route than other nodes. Since the attacker's advertised sequence number is higher than other nodes' sequence numbers, the source node S will choose the route that passes through node A.

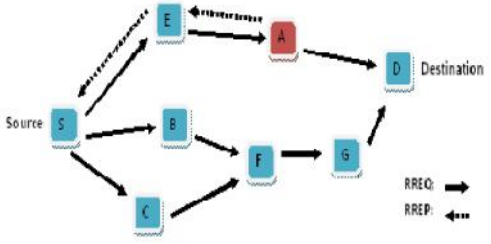


Fig.4 Blackhole Attack

SOLUTIONS TO BLACKHOLE ATTACK: The route confirmation request (CREQ) and route confirmation reply (CREP) are used to avoid the blackhole attack. In this approach, the intermediate node not only sends RREPs to the source node but also sends CREQs to its next-hop node toward the destination node. After receiving a CREQ, the next-hop node looks up its cache for a route to the destination. If it has the route, it sends the CREP to the source. Upon receiving the CREP, the source node can confirm the validity of the path by comparing the path in RREP and the one in CREP. If both are matched, the source node judges that the route is correct. One drawback of this approach is that it cannot avoid the blackhole attack in which two consecutive nodes work in collusion, that is, when the next-hop node is a colluding attacker sending CREPs that support the incorrect path.

Another solution requires a source node to wait until a RREP packet arrives from more than two nodes. Upon receiving multiple RREPs, the source node checks whether there is a shared hop or not. If there is, the source node judges that the route is safe. The main drawback of this solution is that it introduces time delay, because it must wait until multiple RREPs arrive.

IX. LINK WITHHOLDING ATTACK

In this attack, a malicious node ignores the requirement to advertise the link of specific nodes or a group of nodes, which can result in link loss to these nodes. This type of attack is particularly serious in the OLSR protocol.

SOLUTIONS TO WITHHOLDING ATTACK: By withholding a TC message in OLSR, a malicious node can isolate a specific node and prevent it from receiving data packets from other nodes. After analyzing and evaluating the impact of this kind of attack in detail, a detection technique is proposed based on observation of both a TC message and a HELLO message generated by the MPR nodes. If a node does not hear a TC message from its MPR node regularly but hears only a HELLO message, a node judges that the MPR node is suspicious and can avoid the attack by selecting one or more extra MPR nodes.

The main drawback of this approach is that it cannot detect the attack that is launched by two colluding consecutive nodes, where the first attacker pretends to advertise a TC message, but the second attacker drops this TC message.

X LINK SPOOFING ATTACK

In a link spoofing attack, a malicious node advertises fake links with non-neighbors to disrupt routing operations. For example, in the OLSR protocol, an attacker can advertise a fake link with a target's two-hop neighbors. This causes the target node to select the malicious node to be its MPR. As an MPR node, a malicious node can then manipulate data or routing traffic, for example, modifying or dropping the routing traffic or performing other types of DoS attacks.

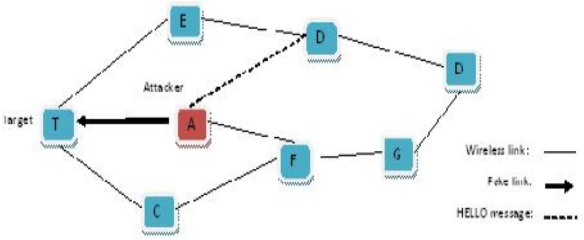


Fig. 5 Link Spoofing Attack

SOLUTIONS TO LINK SPOOFING ATTACK: To detect a link spoofing attack, a location information-based detection method is used by using cryptography with a GPS and a time stamp. This approach requires each node to advertise its position obtained by the GPS and the time stamp to enable each node to obtain the location information of the other nodes. This approach detects the link spoofing by calculating the distance between two nodes that claim to be neighbors and checking the likelihood that the link is based on a maximum transmission range. The main drawback of this approach is that it might not work in a situation where all MANET nodes are not equipped with a GPS. Furthermore, attackers can still advertise false information and make it hard for other nodes to detect the attack[19].

Another technique to detect the link spoofing attack is by adding two-hop information to a HELLO message. In particular, the proposed solution requires each node to advertise its two-hop neighbors to enable each node to learn complete topology up to three hops and detect the inconsistency when the link spoofing attack is launched. The main advantage of this approach is that it can detect the link spoofing attack without using special hardware such as a GPS or requiring time synchronization. One limitation of this approach is that it might not detect link spoofing with nodes further away than three hops.

X. REPLAY ATTACK

In a MANET, topology frequently changes due to node mobility. This means that current network topology might not exist in the future. In a replay attack [20], a node records another node's valid control messages and resends them later. This causes other nodes to record their routing table with stale routes. Replay attack can be misused to impersonate a specific node or simply to disturb the routing operation in a MANET.

SOLUTIONS TO REPLAY ATTACK: A solution to protect a MANET from a replay attack is by using a time stamp with the use of an asymmetric key. This solution prevents the replay attack by comparing the current time and time stamp contained in the received message. If the time stamp is too far from the current time, the message is judged to be suspicious and is rejected. Although this solution works well against the replay attack, it is still vulnerable to a wormhole attack where two colluding attackers use a high speed network to replay messages in a far-away location with almost no delay.

XI. WORMHOLE ATTACK

A wormhole attack is one of the most sophisticated and severe attacks in MANETs. In this attack, a pair of colluding attackers record packets at one location and replay them at another location using a private high speed network. The seriousness of this attack is that it can be launched against all communications that provide authenticity and confidentiality. Figure 3 shows an example of the wormhole attack against a reactive routing protocol. In the figure, we assume that nodes *A*1 and *A*2 are two colluding attackers and that node S is the target to be attacked. During the attack, when source node S broadcasts an RREQ to find a route to a destination node D, its neighbors C and E forward the RREQ as usual. However, node *A*1, which received the RREQ, forwarded by node C, records and tunnels the RREQ to its colluding partner *A*2. Then, node *A*2 rebroadcasts this RREQ to its neighbor H. Since this RREQ passed through a high-speed channel, this RREQ will reach node D first. Therefore, node D will choose route D-H-C-S to unicast an RREP to the source node S and ignore the same RREQ that arrived later. As a result, S will select route S-CH- D that indeed passed through *A*1 and *A*2 to send its data.

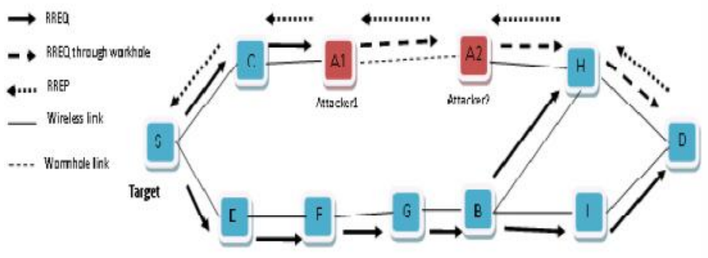


Fig. 6 Wormhole Attack

SOLUTIONS TO WORMHOLE ATTACK: Packet leashes are proposed to detect and defend against the wormhole attack. In particular, the authors proposed two types of leashes: temporal leashes and geographical leashes. For the temporal leash approach, each node computes the packet expiration time, *te*, based on the speed of light *c* and includes the expiration time, *te*, in its packet to prevent the packet from traveling further than a specific distance, *L*. The receiver of the packet checks whether or not the packet expires by comparing its current time and the *te* in the packet. The authors also proposed TIK, which is used to authenticate the expiration time that can otherwise be modified by the malicious node. The main drawback of the temporal leash is that it requires all nodes to have tightly synchronized clocks.

For the geographical leash, each node must know its own position and have loosely synchronized clocks. In this approach, a sender of a packet includes its current position and the sending time. Therefore, a receiver can judge neighbor relations by computing distance between itself and the sender of the packet. The advantage of geographic leashes over temporal leashes is that the time synchronization need not to be highly tight.

Another approach is based on protection against a wormhole attack in the OLSR protocol. This approach is based on location information and requires the deployment of ijhnnja public key infrastructure and timestamp synchronization between all nodes. In this approach, a sender of a HELLO message includes its current position and current time in its HELLO message. Upon receiving a HELLO message from a neighbor, a node calculates the distance between itself and its neighbor, based on a position provided in the HELLO message. If the distance is more than the maximum transmission range, the node judges that the HELLO message is highly suspicious and might be tunneled by a wormhole attack.

XII. COLLUDING MISRELAY ATTACK

In this attack, multiple attackers work in collusion to modify or drop routing packets to disrupt routing operation in a MANET. This attack is difficult to detect by using the conventional methods such as *watchdog* and *pathrater* [23,24]. Figure shows an example of this attack. Consider the case where node *A*1 forwards routing packets for node T. In the figure, the first attacker *A*1 forwards routing packets as usual to avoid being detected by node T. However, the second attacker A2 drops or modifies these routing packets. In the authors discuss this type of attack in OLSR protocol and show that a pair of malicious nodes can disrupt up to 100 percent of data packets in the OLSR MANET.

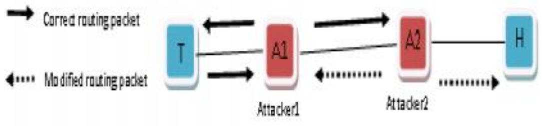


Fig. 7 Colluding Attack

SOLUTIONS TO COLLUDING ATTACK: A conventional acknowledgment-based approach might detect this type of attack in a MANET, especially in a proactive MANET, but because routing packets destined to all nodes in the network require all nodes to return an ACK, this could lead to a large overhead, which is considered to be inefficient.

To detect an attack in which multiple malicious nodes attempt to drop packets is by requiring each node to tune their transmission power when they forward packets. As an example, the author studies the case where two colluding attackers drop packets. The proposed solution requires each node to increase its transmission power twice to detect such an attack. However, this approach might not detect the attack in which three colluding attackers work in collusion. In general, the main drawback of this approach is that even if we require each node to increase transmission power to be K times, we still cannot detect the attack in which $K + 1$ attackers work in collusion to drop packets. Therefore, further work must be done to counter against this type of attack efficiently.

XIII. ADVANTAGE & DISADVANTAGE

The following are the advantages of MANETs:

- They provide access to information and services regardless of geographic position.
- These networks can be set up at any place and time.

Some of the disadvantages of MANETs are:

- Limited resources.
- Limited physical security.
- Intrinsic mutual trust vulnerable to attacks.
- Lack of authorization facilities.
- Volatile network topology makes it hard to detect malicious nodes.
- Security protocols for wired networks cannot work for ad hoc networks.

XIV. FUTURE WORK

Future research should be focused not only on improving the effectiveness of the security schemes but also on minimizing the cost to make them suitable for a MANET environment. Furthermore, each proposed solution can work only with a specific attack and is still vulnerable to unexpected attacks. The Security research area is still open as many of the provided solutions are designed keeping a limited size scenario and limited kind of attacks and vulnerabilities. Therefore, MANET researchers should also focus on exploring, as well as preventing all possible attacks to make a MANET a secure and reliable network.

REFERENCES

[1] Marco Conti, Body, Personal, "Local Ad Hoc Wireless Networks", in Book The Handbook of Ad Hoc Wireless Networks (Chapter 1), CRC Press LLC, 2003.

[2] C. Perkins, E Royer,“Ad Hoc On-Demand Distance Vector Routing”, 2nd IEEE Wksp. Mobile Comp. Sys.and Apps., 1999.

[3] D. Johnson, D. Maltz, “Dynamic Source Routing in Ad Hoc Wireless Networks”, Mobile Computing, Imielinski and H. Korth, Ed., Kluwer, 1996. 3] M.S. Corson, J.P. Maker, and J.H. Cernicione, Internet-based Mobile Ad Hoc Networking, IEEE Internet Computing, pages 63–70, July-August 1999.

[4] Amitabh Mishra, Ketan M. Nadkarni, "Security in Wireless Ad Hoc Networks", in Book The Handbook of Ad Hoc Wireless Networks (Chapter 30), CRC Press LLC, 2003.

[5] Lidong Zhou, Zygmunt J. Hass, "Securing Ad Hoc Networks", IEEE Networks Special Issue on Network Security, November/December 1999.

Mobile Phone Cloning

Sonal[1], Upasna[2]

[1,2]*Department of Computer Science & Engineering, Ganga Institute of Technology and Management, Kablana, Jhajjar, Haryana, INDIA*

Abstract— **Mobile communication has been most popular from many years, and is major need of todays business and life. It provides most valuable service to its users who are willing to pay a considerable premium over fixed line phone such as landline, to be able to walk and talk freely. Because of its usefulness and importance in business and other normal lifestyle, it is subject to fraud.**

Mobile phone cloning is a technique where the data from one cell phone is transferred into another phone. The other cell phone becomes the exact replicate copy of the original mobile phone like a clone. As a result, while calls can be made from both phones, only the original is billed. Though communication channels are equipped with security algorithms, yet cloners get away with the help of loop holes in systems. So when one gets huge bills, the chances are that the phone is being cloned.

This paper describes about the cell phone cloning with implementation in GSM and CDMA technology phones. It gives an insight into the security mechanism in CDMA and GSM phones along with the loop holes in the systems and discusses on the different ways of preventing this cloning.

Keywords— **Mobile phone cloning, GSM, CDMA, IMEI, SIM, ESN and MIN, Patagonia.**

I. INTRODUCTION

When we look up the dictionary meaning of cloning it states, to create the exact replica or a mirror image of an subject understudy. The idea behind the cloning of mobile communications is simple. Here the object of the exercise is to make calls free of charge. Unfortunately, while such calls might well be free to the caller, no such luck for the genuine renter/end-user. To make a mobilephone call (analogue) the system requires two pieces of information, mobile identification number (MIN) and electronic serial number (ESN), commonly referred to as the 'handshake'. Once the mobilephone network validates these pieces of information, service is allowed. There are a number of ways for fraudsters to obtain such information; for example an unsuspecting mobile-phone user may be called and informed that the engineers are carrying out diagnostic checks of the network[1]. Customer cooperation is then sought, with the customer being directed to the ESN written on a label under the battery compartment. Here obviously the culprit must make a second call to retrieve the information, as the battery must be removed.This information is then input into another mobile, with the result that all calls made by the clone are charged to the original user's account. Unfortunately, here the fraud is aided unwittingly by the carrier who fails to produce an itemized account free of charge.The fraudster may well find himself in clover, should the cloned number belong to a company or a person who fails to check usage. Such a methodology for obtaining handshake information is extremely slow and time consuming. Therefore other resources must be utilized. Here, to speed matters up, scanning devices are deployed.The idea here is to place the scanner near to an underpass or bridge near a motorway.Then as the vehicles pass, those who have established mobile calls in progress, to maintain communication have to re-establish the network connection.This means that the MIN and ESN is forwarded to the network, and as the link is not encrypted, the scanner grabs the salient information. Another alternative is to seek out and to corrupt an employee of a service provider or to steal the customer database containing the handshake information. This information can then be inputted into analogue mobiles and fraudulent calls made.There are parts of the UK where 'dial a clone' is more lucrative than 'dial a pizza' service. Here the cloner rents out the clones for a set fee.

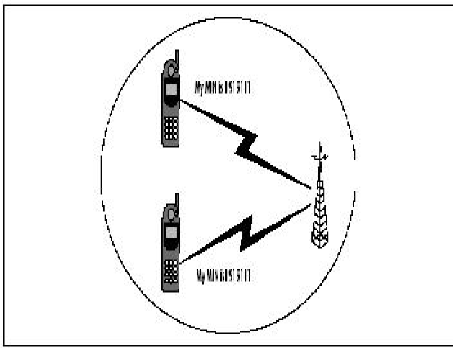


Fig. 1 Mobile Phone Cloning

II. HISTORY OF MOBILE PHONE CLONING

The early 1990s were boom times for eavesdroppers. Any curious teenager with a £100 Tandy Scanner could listen in to nearly any analogue mobile phone call. As a result, Cabinet Ministers, company chiefs and celebrities routinely found their most intimate conversations published in the next day's tabloids Cell phone cloning[1] started with Motorola "bag" phones and reached its peak in the mid 90's with a commonly And Dolly the lamb, cloned from a six-year-old ewe in 1997, available modification for the Motorola "brick" phones, such as the Classic, the Ultra Classic, and the Model 8000.

by a group of researchers at the Roslin Institute in Scotland. While the debate on the ethics of cloning continues, human race, for the first time, are faced with a more tangible and harmful version of cloning and this time it is your cell phone that is the target.

According to media reports, recently the Delhi (India) police arrested a person with 20 cell- phones, a laptop, a SIM scanner, and a writer. The accused was running an exchange illegally wherein he cloned CDMA based cell phones. He used software named Patagonia for the cloning and provided cheap international calls to Indian immigrants in West Asia.

III. TYPES OF MOBILE PHONES

A. GSM Mobile Phones

Global System for Mobile Communications. A digital cellular phone technology based on TDMA GSM phones[2] use a Subscriber Identity Module (SIM) card that contains user account information. Any GSM phone becomes immediately programmed after plugging in the SIM card, thus allowing GSM phones to be easily rented or borrowed. Operators who provide GSM service are Airtel, Reliance, Vodafone, Idea etc.

B. CDMA Mobile Phones

Code Division Multiple Access. A method for transmitting simultaneous signals over a shared portion of the spectrum. There is no Subscriber Identity Module (SIM) card unlike in GSM Operators who provides CDMA service in India are Reliance and Tata Indicom[2].

Both GSM and CDMA handsets are prone to cloning. Technically, it is easier to clone a CDMA handset over a GSM one, though cloning a GSM cell phone is not impossible. There are also Internet sites that provide information on how one could go about hacking into cell-phones.

IV. HOW MOBILE PHONES ARE CLONED

A. Cloning GSM Mobile Phones

GSM handsets, on the contrary, are safer, according to experts. Every GSM phone has a 15 digit electronic serial number (referred to as the IMEI)[3][4]. It is not a particularly secret bit of information and you don't need to take any care to keep it private. The important information is the IMSI, which is stored on the removable SIM card that carries all your subscriber information, roaming database and so on. GSM employs a fairly sophisticated asymmetric-key cryptosystem for over-the-air transmission of subscriber information. Cloning a SIM using information captured over-the-air is therefore difficult, though not impossible. As long as you don't lose your SIM card, you're safe with GSM. GSM carriers use the COMP128 authentication algorithm for the SIM, authentication center and network which make GSM a far secure technology.

GSM networks which are considered to be impregnable can also be hacked. The process is simple: a SIM card is inserted into a reader. After connecting it to the computer using data cables, the card details were transferred into the PC. Then, using freely available encryption software on the Net, the card details can be encrypted on to a blank smart card. The result: A cloned cell phone is ready for misuse.

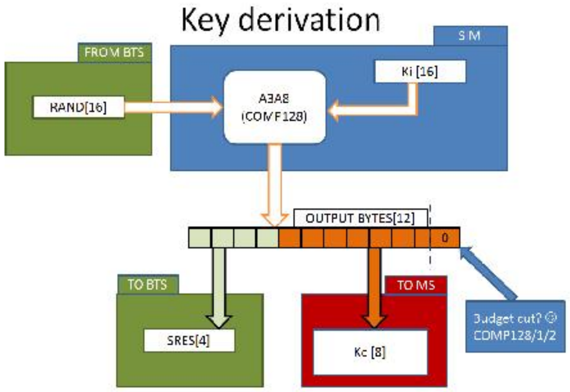


Fig. 2 GSM Cloning

B. Cloning CDMA Mobile Phones

Cellular telephone thieves monitor the radio frequency spectrum and steal the cell phone pair as it is being anonymously registered with a cell site. The technology uses spread-spectrum techniques to share bands with multiple conversations. Subscriber information is also encrypted and transmitted digitally. CDMA[3] handsets are particularly vulnerable to cloning, according to experts. First generation mobile cellular networks allowed fraudsters to pull subscription data (such as ESN and MIN) from the analog air interface and use this data to clone phones. A device called as DDI, Digital Data Interface (which comes in various formats from the more expensive stand-alone box, to a device which interfaces with your 800 MHz capable scanner and a PC) can be used to get pairs by simply making the device mobile and sitting in a busy traffic area (freeway overpass) and collect all the data you need. The stolen ESN and EMIN[5] were then fed into a new CDMA handset, whose existing program was erased with the help of downloaded software. The buyer then programs them into new phones which will have the same number as that of the original subscriber.

But Looking at the recent case, it is quite possible to clone both GSM and CDMA sets. The accused in the Delhi case used software called Patagonia to clone only CDMA phones (Reliance and Tata Indicom). However, there are software packages that can be used to clone even GSM phones (e.g. Airtel, BSNL, Hutch, Idea). In order to clone a GSM phone, knowledge of the International Mobile Equipment Identity (IMEI) or instrument number is sufficient.

V. SOFTWARE FOR MOBILE PHONES CLONING

A Software tool is used for modifying the and configuring the cell phone. The EEPROM chip is replaced of modified with a new chip which will reconfigure ESN (Electronic Serial Number) or IMEI (International Mobile Equipment Identity) and via MIN (Mobile Identification Number) software. When the ESN/MIN pair had changed successfully then an effective clone of the original phone has created.

A. Patagonia

Patagonia is a software available in the market which is used to clone CDMA phone.Using this software a cloner can take over the control of a CDMA[6] phone i.e. cloning of phone. There are other Software’s avai;able in the market to clone GSM phone.This software’s are easily available in the market.A SIM can be cloned again and again and they can be used at different places.Messages and calls sent by cloned phones can be tracked.However,if the accuses manages to also clone the IMEI number of the handset,for which software’s are available,there is no way he can be traced.

Fig. 3 Mobile Cloning Device

VI. SYMPTOMS OF MOBILE PHONE CLONING

1) Frequent wrong number phone calls to your phone, or hang-ups.
2) Difficulty in placing outgoing calls.
3) Difficulty in retrieving voice mail messages.
4) Incoming calls constantly receiving busy signals or wrong numbers. Unusual calls appearing on your phone bills

VII. HOW TO DETECT MOBILE PHONE CLONING IN A NETWORK

There are various communication companies do deploy fraud detection/reduction measures. The aims of which are to identify potential fraudulent activity[7]. Some of these measures are simple for example; the systems look for simultaneous or over lapping calls made by the same mobile number, an impossible event.The exception is informed to an operator for investigation. Here access to calling records takes place, and a decision made concerning the activity. In reality, call barring is applied to the number, inessence only local calls are allowed and the genuine renter is contacted concerning the situation. Also the system may well 'tear down' both numbers and prevent them from making calls. This is a very quick way of ensuring customer contact. Because no one wants to be without service. Then there are the exception reports. Here cash limits are set against each mobile, in consultation with the customer, once this level is reached, only local calls are allowed, and contact is made with the customer. In reality it is only the customer who can confirm the true situation. Obviously, here a degree of trust must exist between the customer and service provider, because the customer's word on usage must be accepted. It is amazing how honest the vast majority of customers are. Once a mobile has been cloned, the carrier often offers the customer the prospect of retaining the existing number, but to migrate free of charge to the digital service. Naturally, this is in addition to an account reduction, no one is expected to pay for unmade calls.

Several countermeasures were taken with varying success. Here are various methods to detect cloned phones on the network:

A. *Duplicate Detection*

The network sees the same phone in several places at the same time. Reactions include shutting them all off so that the real customer will contact the operator because he lost the service he is paying for, or tearing down connections so that the clone users will switch to another clone but the real user will contact the operator.

B. *Velocity Trap*

The mobile phone seems to be moving at impossible, or most unlikely speeds. For example, if a call is first made in Helsinki, and five minutes later, another call is made but this time in Tampere, there must be two phones with the same identity on the network.

C. *RF (Radio Frequency)*

Fingerprinting is originally a military technology. Even nominally identical radio equipment has a distinguishing ``fingerprint", so the network software stores and compares fingerprints for all the phones that it sees. This way, it will spot the clones with the same identity but different fingerprints.

D. *Usage Profiling*

Profiles of customers' phone usage are kept, and when discrepancies are noticed, the customer is contacted. Credit card companies use the same method. For example, if a customer normally makes only local network calls but is suddenly placing calls to foreign countries for hours of airtime, it indicates a possible clone.

E. *Call counting*

Both the phone and the network keep track of calls made with the phone, and should they differ more than the usually allowed one call, service is denied.

F. *Pin Codes*

Prior to placing a call, the caller unlocks the phone by entering a PIN code and then calls as usual. After the call has been completed, the user locks the phone by entering the PIN code again. Operators may share PIN information to enable safer roaming.

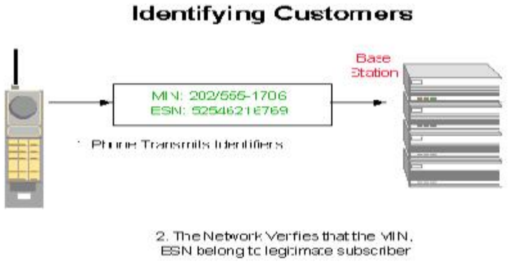

Identifying Customers
MIN: 202/555-1706
ESN: 52546216769
Base Station
Phone Transmits Identifiers
2. The Network Verfies that the MIN, ESN belong tc legitimate subscriber

Fig 4:Operators sharing PIN information

VIII. SECURITY FUNDAMENTALS

So far we have considered trust and security in fairly general terms, but at this stage it is necessary to define some trust items that we will examine further in our cellular usag scenarios. Firstly we will introduce some information security fundamentals[7];

A. *Call counting*

To ensure that entities involved in our trusted solution are legitimate/authentic.

B. *Confidentiality*

Information, signals, commands or functionality that are restricted to certain authorised entities must be protected from disclosure/discovery by unauthorised entities.

C. *Integrity*

Critical data and applications code should be protected from modification when in storage, operation or during communications/transactions.

These fundamentals can in turn be underpinned by some practical capabilities;

1) Cryptographic algorithm(s) plus supporting data for authentication/encryption/integrity
2) Secure storage and verification of critical data, with strictaccess controls
3) Secure verification and execution of algorithm(s) and other critical functions
4) Secure communication protocols
5) Controlled operating environment and isolated ''security domains".

The word ''Secure'' has been used rather freely in the above points and so we should be clear what it means in this context;

The functionality that embodies our security fundamentals has been correctly designed, implemented and tested to strongly resist the anticipated attacks that may be made against it.

IX. SOME FACTS AND FIGURES

1) Southwestern Bell claims wireless fraud costs the industry $650 million each year in the US. Some federal

agents in the US have called phone cloning an especially `popular' crime because it is hard to trace. In one case, more than 1,500 telephone calls were placed in a single day by cellular phone thieves using the number of a single unsuspecting owner[1].

2) A Home Office report in 2002 revealed that in London around 3,000 mobile phones were stolen in one month alone which were used for cell phone cloning.
3) Authorities, in the case, estimated the loss at $3,000 to $4,000 for each number used in cell phone cloning.
4) Ualcomm, which develops CDMA technology globally, says each instance of mobile hacking is different and therefore there is very little an operator can do to prevent hacking[1]. "It's like a virus hitting the computer. The software which is used to hack into the network is different, so operators can only keep upgrading their security firewall as and when the hackers strike," says a Qualcomm executive.

X. FUTURE THREATS

Resolving subscriber fraud can be a long and difficult process for the victim. It may take time to discover that subscriber fraud has occurred and an even longer time to prove that you did not incur the debts. As described in this paper there are many ways to abuse telecommunication system, and to prevent abuse from occurring it is absolutely necessary to check out the weakness and vulnerability of existing telecom systems. If it is planned to invest in new telecom equipment, a security plan should be made and the system tested before being implemented. It is therefore mandatory to keep in mind that a technique which is described as safe today can be the most unsecured technique in the future.

XI. CONCLUSION

To conclude, cell phone communication is one of the most reliable, efficient and widespread. The usage of the system can be changed in either constructive or destructive ways. Unfortunately because of its the security standards it is very easy to break and also takes very less amount of time. Moreover, cloning can be easily increased and also can be implemented easily. Hence, it must be considered that the security which is currently used is not fruitful enough to secure the system in future. So it is very important to verify the working of security system time-to-time and also must change or update it over every month or year once. Preventive steps should be taken by the network provider and the government the enactment of legislation to prosecute crime related to cellular phones is not viewed as a priority.

Existing cellular system have number of weaknesses, it is not good for us. And it is very harmful of our society, So the security staff must take these cloning kind of problems seriously.

REFERENCES

[1] http://www.wikipedia.com

[2] IEEE journal for mobile communication

[3] http://www.hackinthebox.org/

[4] *Security in the GSM network* by Marcin Olawski

[5] *CDG Document 138 Version 0.34*

CDMA Development Group, 575 Anton Boulevard, Suite 560 Costa Mesa, California 92626

[6] http://www.cdmasoftware.com/eng.html

[7] Sankaranarayanan ,“Mobile phone cloning”, Wireless And Optical Communications Networks (WOCN), 2010 Seventh International Conference in Sept,2010.

More Secured Authentication: 3D Password

Parul[1], Neetu Sharma[2]
[1,2] *Department of Computer Science and Engineering, Ganga Institute of Technology and Management, Kablana, Jhajjar, Haryana, INDIA*

Abstract—Current authentication systems suffer from many weaknesses. Textual passwords are commonly used; however, users do not follow their requirements. Users tend to choose meaningful words from dictionaries, which make textual passwords easy to break and vulnerable to dictionary or brute force attacks. Many available graphical passwords have a password space that is less than or equal to the textual password space. Smart cards or tokens can be stolen. Many biometric authentications have been proposed; however, users tend to resist using biometrics because of their intrusiveness and the effect on their privacy. Moreover, biometrics cannot be revoked. In this paper, we present and evaluate our contribution, i.e., the 3-D password. The 3-D password is a multifactor authentication scheme. To be authenticated, we present a 3-D virtual environment where the user navigates and interacts with various objects. The sequence of actions and interactions toward the objects inside the 3-D environment constructs the user's 3-D password. The 3-D password can combine most existing authentication schemes such as textual passwords, graphical passwords, and various types of biometrics into a 3-D virtual environment. The design of the 3-D virtual environment and the type of objects selected determine the 3-D password key space.

Keywords- 3-D password, authentication, biometric, virtual environment

I. INTRODUCTION

Users nowadays are provided with major password stereotypes such as textual passwords, biometric scanning, tokens or cards (such as an ATM) etc .Mostly textual passwords follow an encryption algorithm as mentioned above. Biometric scanning is your "natural" signature and Cards or Tokens prove your validity. But some people hate the fact to carry around their cards, some refuse to undergo strong IR exposure to their retinas(Biometric scanning).Mostly textual passwords, nowadays, are kept very simple say a word from the dictionary or their pet names, girlfriends etc. Years back Klein performed such tests and he could crack 10-15 passwords per day. Now with the technology change, fast processors and many tools on the Internet this has become a Child's Play.

Therefore we present our idea, the 3D passwords which are more customizable and very interesting way of authentication. Now the passwords are based on the fact of Human memory. Generally simple passwords are set so as to quickly recall them. The human memory, in our scheme has to undergo the facts of Recognition, Recalling, Biometrics or Token based authentication. Once implemented and you log in to a secure site, the 3D password GUI opens up. This is an additional textual password which the user can simply put. Once he goes through the first authentication, a 3D virtual room will open on the screen. In our case, let's say a virtual garage. Now in a day to day garage one will find all sorts of tools, equipments, etc.each of them having unique properties. The user will then interact with these properties accordingly. Each object in the 3D space, can be moved around in an (x,y,z) plane. That's the moving attribute of each object. This property is common to all the objects in the space. Suppose a user logs in and enters the garage. He sees and picks a screw-driver (initial position in xyz coordinates (5, 5, 5)) and moves it 5 places to his right (in XY plane i.e. (10, 5, 5).That can be identified as an authentication. Only the true user understands and recognizes the object which he has to choose among many. This is the Recall and Recognition part of human memory coming into play. Interestingly, a password can be set as approaching a radio and setting its frequency to number only the user knows. Security can be enhanced by the fact of including Cards and Biometric scanner as input. There can be levels of authentication a user can undergo.

II. EXISTING SYSTEM

Current authentication systems suffer from many weaknesses. Textual passwords are commonly used. Users tend to choose meaningful words from dictionaries, which make textual passwords easy to break and vulnerable to dictionary or brute force attacks. Many available graphical passwords have a password space that is less than or equal to the textual password space. Smart cards or tokens can be stolen. Many biometric authentications have been proposed. However, users tend to resist using biometrics because of their intrusiveness and the effect on their privacy. Moreover, biometrics cannot be revoked. The 3Dpassword is a multi factor authentication scheme. The design of the 3D virtual environment and the type of objects selected determine the 3D password key space. User have freedom to select whether the 3D password will be solely recall, recognition, or token based, or combination of two schemes or more.

DRAWBACKS IN EXISTING SYSTEM

Textual Passwords: Textual passwords should be easy to remember at the same time hard to guess. But if a textual password is hard to guess then it will also be hard to remember.

Graphical Passwords: They are based on idea that users can recall and recognize pictures better than words. Some graphical schemes require a long time to perform. They are vulnerable to shoulder surfing attacks.

Biometrics: Many biometric schemes have been proposed; fingerprints, palm prints, hand geometry, face recognition, voice recognition,

iris recognition, and retina recognition are all different biometric schemes. Each biometric recognition scheme has its advantages and disadvantages based on several factors such as consistency, uniqueness, and acceptability. One of the main drawbacks of applying biometrics is its intrusiveness upon a user's personal characteristic. Moreover, retina biometrical recognition schemes require the user to willingly subject their eyes to a low-intensity infrared light. In addition, most biometric systems require a special scanning device to authenticate users, which is not applicable for remote and Internet users.

III. PROPOSED SYSTEM

The proposed system is a multi factor authentication scheme that combines the benefits of various authentication schemes. Users have the freedom to select whether the 3D password will be solely recall, biometrics, recognition, or token based, or a combination of two schemes or more. This freedom of selection is necessary because users are different and they have different requirements. Therefore, to ensure high user acceptability, the user’s freedom of selection is important.

The following requirements are satisfied in the proposed scheme

1. The new scheme provide secrets that are easy to remember and very difficult for intruders to guess.

2. The new scheme provides secrets that are not easy to write down on paper. Moreover, the scheme secrets should be difficult to share with others.

3. The new scheme provides secrets that can be easily revoked or changed.

3.1 BRIEF DESCRIPTION OF SYSTEM

The proposed system is a multi factor authentication scheme. It can combine all existing authentication schemes into a single 3D virtual environment .This 3D virtual environment contains several objects or items with which the user can interact. The user is presented with this 3D virtual environment where the user navigates and interacts with various objects. The sequence of actions and interactions toward the objects inside the 3D environment constructs the user’s 3D password. The 3D password can combine most existing authentication schemes such as textual passwords, graphical passwords, and various types of biometrics into a 3D virtual environment. The choice of what authentication schemes will be part of the user's 3D password reflects the user's preferences and requirements. A user who prefers to remember and recall a password might choose textual and graphical password as part of their 3D password. On the other hand users who have more difficulty with memory or recall might prefer to choose smart cards or biometrics as part of their 3D password. Moreover user who prefers to keep any kind of biometric data private might not interact with object that requires biometric information. Therefore it is the user's choice and decision to construct the desired and preferred 3D password.

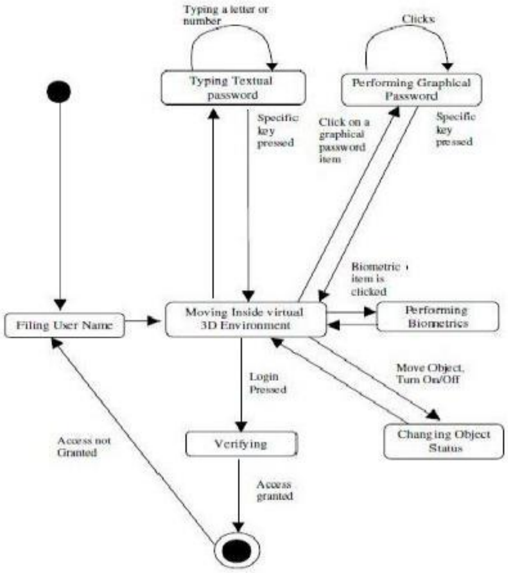


Fig1. State diagram

3.2 SYSTEM IMPLEMENTATION

The 3D password is a multi factor authentication scheme. The 3D password presents a 3D virtual environment containing various virtual objects. The user navigates through this environment and interacts with the objects. The 3D password is simply the combination and the sequence of user interactions that occur in the 3D virtual environment. The 3D password can combine recognition, recall, token, and biometrics based systems into one authentication scheme. This can be done by designing a 3D virtual environment that contains objects that request information to be recalled, information to be recognized, tokens to be presented, and biometric data to be verified.

For example, the user can enter the virtual environment and type something on a computer that exists in (x1 , y1 , z1) position, then enter a room that has a fingerprint recognition device that exists in a position (x2 , y2 , z2) and provide his/her fingerprint. Then, the user can go to the virtual garage, open the car door, and turn on the radio to a specific channel. The combination and the sequence of the previous actions toward the specific objects construct the user’s 3D password.

Virtual objects can be any object that we encounter in real life. Any obvious actions and interactions toward the real life objects can be done in the virtual 3D environment toward the virtual objects. Moreover, any user input (such as speaking in a specific location) in the virtual 3D environment can be considered as a part of the 3D password.

We can have the following objects:

1) A computer with which the user can type;

2) A fingerprint reader that requires the user’s fingerprint;

3) A biometric recognition device;

4) A paper or a white board that a user can write, sign, or draw on;

5) An automated teller machine (ATM) that requests a token;

6) A light that can be switched on/off;

7) A television or radio where channels can be selected;

8) A staple that can be punched;

9) A car that can be driven;

10) A book that can be moved from one place to another;

11) Any graphical password scheme;

12) Any real life object;

13) Any upcoming authentication scheme.

The action toward an object (assume a fingerprint recognition device) that exists in location (x1, y1 , z1) is different from the actions toward a similar object (another fingerprint recognition device) that exists in location (x2 , y2 , z2), where x1 = x2 , y1 = y2 , and z1 = z2 . Therefore, to perform the legitimate 3D password, the user must follow the same scenario performed by the legitimate user. This means interacting with the same objects that reside at the exact locations and perform the exact actions in the proper sequence.

IV. 3D PASSWORD SELECTION AND INPUT

Let us consider a 3D virtual environment space of size G ×G × G. The 3D environment space is represented by the coordinates (x, y, z)   [1, . . . , G] ×[1, . . . , G] ×[1, . . . , G]. The objects are distributed in the 3D virtual environment with unique (x, y, z) coordinates. We assume that the user can navigate into the 3D virtual environment and interact with the objects using any input device such as a mouse, key board, fingerprint scanner, iris scanner, stylus, card reader, and microphone. We consider the sequence of those actions and interactions using the previous input devices as the user's 3D password.

For example, consider a user who navigates through the 3D virtual environment that consists of an office and a meeting room. Let us assume that the user is in the virtual office and the user turns around to the door located in (10, 24, 91) and opens it. Then, the user closes the door. The user then finds a computer to the left, which exists in the position (4, 34, 18), and the user types "FALCON." Then, the user walks to the meeting room and picks up a pen located at (10, 24, 80) and draws only one dot in a paper located in (1, 18, 30), which is the dot (x, y) coordinate relative to the paper space is (330, 130). The user then presses the login button. The initial representation of user actions in the 3Dvirtual environment can be recorded as follows:

(10, 24, 91) Action = Open the office door;

(10, 24, 91) Action = Close the office door;

(4, 34, 18) Action = Typing, "F";

(4, 34, 18) Action = Typing, "A";

(4, 34, 18) Action = Typing, "L";

(4, 34, 18) Action = Typing, "C";

(4, 34, 18) Action = Typing, "O";

(4, 34, 18) Action = Typing, "N";

Fig 2. User entering textual password in 3D environment

3D VIRTUAL ENVIRONMENT DESIGN GUIDELINES

The design of the 3 D virtual environments affects the usability, effectiveness, acceptability of 3D password. The first step in building a 3D password system is to design a 3D environment that reflects the administration needs and the security requirements. The design of 3D virtual environments should follow these guidelines.

1) Real Life Similarity The prospective 3D virtual environment should reflect what people are used to seeing in real life. Objects used in virtual environments should be relatively similar in size to real objects (sized to scale). Possible actions and interactions toward virtual objects should reflect real life situations. Object responses should be realistic. The target should have a 3D virtual environment that users can interact
2) Object uniqueness and distinction every virtual object or item in the 3D virtual environment is different from any other virtual object. The uniqueness comes from the fact that every virtual object has its own attributes such as position. Thus, the prospective interaction with object 1 is not equal to the interaction with object 2. However, having similar objects such as 20 computers in one place might confuse the user. Therefore, the design of the 3D virtual environment should consider that every object should be distinguishable from other objects. Similarly, in designing a 3D virtual environment, it should be easy for users to navigate through and to distinguish between objects. The distinguishing factor increases the user's recognition of objects. Therefore, it improves the system usability.
3) Three Dimensional Virtual Environment Size A 3D virtual environment can depict a city or even the world. On the other hand, it can depict a space as focused as a single room or office. A large 3D virtual environment will increase the time required by the user to perform a 3D password. Moreover, a large 3D virtual environment can contain a large number of virtual objects. Therefore, the probable 3D password space broadens. However, a small 3D virtual environment usually contains only a few objects, and thus, performing a 3D password will take less time.
4) Number of objects and their types Part of designing a 3D virtual environment is determining the types of objects and how many objects should be placed in the environment. The types of objects reflect what kind of responses the object will have. For simplicity, we can consider requesting a textual password or a fingerprint as an object response type.

Selecting the right object response types and the number of objects affects the probable password space of a 3D password.

5) System Importance The 3D virtual environment should consider what systems will be protected by a 3D password The number of objects and the types of objects that Have been used in the 3D virtual environment should reflect the importance of the protected system.

V. 3D PASSWORD APPLICATION

The 3D password can have a password space that is very large compared to other authentication schemes, so the 3D password's main application domains are protecting critical systems and resources.

1. Critical server many large organizations have critical servers that are usually protected by a textual password. A 3D password authentication proposes a sound replacement for a textual password.

2. Nuclear and military facilities such facilities should be protected by the most powerful authentication systems. The 3D password has a very large probable password space, and since it can contain token, biometrics, recognition and knowledge based Authentications in a single authentication system, it is a sound choice for high level security locations.

3. Airplanes and jet fighters Because of the possible threat of misusing airplanes and jet fighters for religion, political agendas, usage of such airplanes should be protected by a powerful authentication system In addition, 3D passwords can be used in less critical systems because the 3D virtual environment can be designed to fit to any system needs. A small virtual environment can be used in the following systems like

1) ATM
2) Personal Digital Assistance
3) Desktop Computers & laptop logins
4) Web Authentication
5) Security Analysis

To analyze and study how secure a system is, we have to consider,

• How hard it is for the attacker to break such a system

▪ A possible measurement is based on the information content of a password space. It is important to have a scheme that has a very large possible password space which increases the work required by the attacker to break the authentication system.

▪ Find a scheme that has no previous or existing knowledge of the most probable user password selection.

5.1 Attacks and Countermeasures

To realize and understand how far an authentication scheme is secure, we have to consider all possible attack methods. We have to study whether the authentication scheme proposed is immune against such attacks or not. Moreover, if the proposed authentication scheme is not immune, we then have to find the countermeasures that prevent such attacks. In this section, we try to cover most possible attacks and whether the attack is valid or not. Moreover, we try to propose countermeasures for such attacks.

1) **Brute Force Attack**: The attacker has to try all possible 3D passwords. This kind of attack is very difficult for the following reasons.

1. Time required to login The total time needed for a legitimate user to login may vary depending on the number of interactions and actions, the size of the 3D virtual environment, and the type of actions and interactions. Therefore, a brute force attack on a 3D password is very difficult and time consuming

2. Cost of attacks the 3D virtual environment contains biometric recognition objects and token based objects. The attacker has to forge all possible biometric information and forge all the required tokens. The cost of forging such information is very high, therefore cracking the 3D password is more challenging. The high number of possible 3D password spaces leaves the attacker with almost no chance of breaking the 3D password.

2) Well-Studied Attack : The attacker tries to find the highest probable distribution of 3D passwords. In order to launch such an attack, the attacker has to acquire knowledge of the most probable 3D password distributions. This is very difficult because the attacker has to study all the existing authentication schemes that are used in the 3D environment. It requires a study of the user's selection of objects for the 3D password. Moreover, a well studied attack is very hard to accomplish since the attacker has to perform a customized attack for every different 3D virtual environment design. This environment has a number of objects and types of object responses that differ from any other 3D virtual environment. Therefore, a carefully customized study is required to initialize an effective attack.

2) **Shoulder Surfing Attack** : An attacker uses a camera to record the user's 3D password or tries to watch the legitimate user while the 3D password is being performed. This attack is the most successful type of attack against 3D passwords and some other graphical passwords. However, the user's 3D password may contain biometric data or textual passwords that cannot be seen from behind. Therefore, we assume that the 3D password should be performed in a secure place where a shoulder surfing attack cannot be performed.

3) **Timing Attack**: In this attack, the attacker observes how long it takes the legitimate user to perform a correct sign in using the 3D password. This observation gives the attacker an indication of the legitimate user's 3D password length. However, this kind of attack alone cannot be very successful since it gives the attacker mere hints. Therefore, it would probably be launched as part of a well studied or brute force attack. Timing attacks can be very effective if the 3D virtual environment is poorly designed.

VI. CONCLUSION

The 3D password is a multi factor authentication scheme that combines the various authentication schemes into a single 3D virtual environment. The virtual environment can contain any existing authentication scheme or even any upcoming authentication scheme or even any upcoming authentication schemes by adding it as a response to actions performed on an object. Therefore the resulting password space becomes very large compared to any existing authentication schemes. The design of the 3D virtual environment the selection of objects inside the environment and the object's type reflect the resulted password space. It is the task of the system administrator to design the environment and to select the appropriate object that reflects the protected system requirements. Designing a simple and easy to use 3D virtual environment is a factor that leads to a higher user acceptability of a 3D password system. The choice of what authentication scheme will be part of user's 3D password reflects the user's preferences and requirements.

REFERENCES

[1]. Fawaz Alsulaiman and Abdulmotaleb El Saddik "Three Dimensional Password for more Secure Authentication" ,IEEETransactions on Instrumentations and Measurement.

[2]. Tejal Kognule and Yugandhara Thumbre and Snehal Kognule,"3D password", International Journal of Computer

Applications(IJCA),2012.

[3]. NBC news, ATM Fraud: Banking on Your Money, Dateline Hidden Cameras Show Criminals Owning ATMs, Dec. 11, 2003.

[4].Manila M V," Three Dimensional Password for More SecureAuthentiction",netlab.cs.iitm.ernet.in/cs648/2009/tpf/cs08m028.pdf,2009.

[5].http://www.123rf.com/photo_10326797_3d-man-secure-loginwith-administrator-id-and-password.html.

[6]. Prof. Gauri Rao ,"SECUREZZA", IT Journal of Research,Volume 1, May 2010

[7]. Fawaz A Alsulaiman and Abdulmotaleb El Saddik, "A Novel 3D Graphical Password Schema", IEEE International Conference on virtual environments

National Conference on Emerging Trends in Engineering, Management and Science (NCETEMS – 2015)
Sponsored by: International Journal Of Engineering Research and Technology (IJERT)

Nanotechnology & Environment

Mridula Chugh[1]
[1]*Department of Applied Sciences, Ganga Institute of Technology and Management, Kablana, Jhajjar, Haryana, INDIA*

mridula.chugh@gmail.com

Abstract-***Advances in nanoscale science and engineering suggest that many of the current problems involving water quality could be resolved or greatly improved using nanoparticles. Currently, the most widely used method for the removal and separation of toxic metal ions/organic compounds is the solid phase extraction technique. Recently, there have been reports in the literature on the enrichment and separation of trace elements and organic compound in the sample solutions by means of nanoparticles like*** TiO_2,Al_2O_3, ZrO_2, ***MnO and*** CeO_2. ***Nanoparticles have unique properties like large specific surface area, high adsorption capacity and low temperature modification, so they are promising solid-phase extractants and have contaminant scavenging mechanisms. This feature article includes application of nanoparticles in preconcentration, separation and determination of trace pollutants from various environmental samples.***

I. INTRODUCTION

Recent advancements suggest that many issues involving water quality could be resolved or greatly ameliorated using nanoparticles and other products resulting from the development of nanotechnology. In addition to obvious advantages for industrialized nations, the benefits for developing countries would also be enormous. Innovative use of nanoparticles for treatment of industrial wastewater is another potentially useful application. Many industries generate large amounts of wastewater. Removal of contaminants and recycling of the purified water would provide significant reductions in cost, time and energy to the industry and result in improved environmental stewardship. Aquifer and groundwater remediation are also critical issues, becoming more important as water supplies steadily decrease and demand continues to increase. Most remediation technologies available today, while effective, very often are costly and time consuming. The ability to remove toxic compounds from subsurface and other environments that are very difficult to access in situ, and doing so rapidly, efficiently and within reasonable costs, is the ultimate goal. Use of nanoparticles in analytical processes is the most extensively explored area of analytical nanotechnology. The objective is to exploit the excellent properties of nanoparticles to improve well established analytical methods or to develop others for new analytes or matrices. In addition to the typical advantages of nanoparticles, their use should lead to improved selectivity, sensitivity, rapidity, miniaturizability or portability of the analytical system. Nanoparticles can be incorporated or used in analytical methods either as such or chemically bonded. In the latter case, nanoparticles can be chemically bonded to a surface or functionalized with other organic or inorganic compounds in order to increase their solubility. Chemically unmodified nanoparticles can be used as raw randomized materials or as self-assembled raw materials. The explored nanoparticle properties can be electrical, optical, thermal, magnetic or chemical. Frequently, however, two or more properties are explored at once. Nanoparticles can be used for purposes such as sample treatment, instrumental separation of analytes, or even detection. In combination with the large variety of nanoparticles available, this provides a wide range of potential applications.The nanoparticles most widely used in analytical sciences at present include (a) silica nanoparticles, (b) carbon nanoparticles (mainly fullerenes and carbon nanotubes), (c) metallic nanoparticles and (d) supramolecular aggregates. Nanoparticles have two key properties that make them particularly attractive sorbents. On a mass basis, they have much larger surface area than bulk particles. Nanoparticles can also be functionalized with various chemical groups to increase their affinity towards target compounds. It has been found that the unique properties of nanoparticles enable their development as high capacity and selective sorbents for metal ions and pollutants. Due to these reasons, now nanoparticles are designed and synthesized to act as either separation or reaction media for pollutants or scaffolds and delivery vehicles for bioactive compounds,thus providing unprecedented opportunities to develop more efficient and cost effective water purification processes and systems. Consequently, nanometer-sized material can selectively adsorb metal ions and have a very high adsorption capacity. Nanoparticles play a central role in purification and preconcentration of analytes from the sample matrix.Nanoparticles are used for the preconcentration and separation of pollutants from environmental sources. Investigation of the surface chemistry of highly dispersed metal oxides, e.g. TiO_2,Al_2O_3, ZrO_2, CeO_2 and MnO nanoparticles, indicates that these materials have very high adsorption capacity and give promising results when they are used for trace metal analytes of different types of sample. Thus, carbon nanotubes have been widely used as sorbents for solid-phase extraction. Ferric hydroxide is used to scavenge a variety of heavy metal contaminants.. This feature article deals with nanomaterials used in the separation and preconcentration of different pollutants from various samples.

A. *Production techniques*

There is a wide variety of techniques for producing nanoparticles.

B. *Vapour condensation*

This approach is used to make metal, metal oxide and ceramic nanoparticles. It involves evaporation of a solid metal followed by rapid condensation to formnanosized clusters that settle in the form of a powder. The main advantage of this approach is low contamination levels. The final particle size is controlled by variation of parameters such as temperature, gas environment and evaporation rate. This technique was developed originally in Russia.

C. Chemical synthesis

The most widely used chemical synthesis techniques consist essentially of growing nanoparticles in a liquid medium composed of various reactants. This is typified by the sol-gel approach, and is also used to create quantum dots. Chemical techniques are generally better than vapour condensation techniques for controlling the final shape of the particles. Scheme 1 represents the reactions involved in the sol-gel formation of nanoparticles.

D. Solid state process

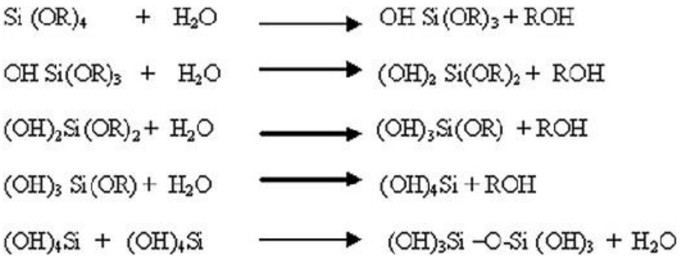
Grinding or milling can be used to create nanoparticles. The milling materials, milling time and atmosphere affect the resultant nanoproperties .The contamination from milling materials is one of the great disadvantages.

Biological process

This is a natural system to create almost atomically perfect nanostructures .Yeast cells can create cadmium sulfide nanoparticles and viral proteins to create silver nanoparticles.

E. Characterization

Nanoparticles are characterized by different techniques, including structure analysis of nanostructure using the scattering effects of an e-beam., Early equipment did not have the required magnification or reflection capability to observe materials at the nanoscale. With the introduction of equipment like SEM, TEM, STM, AFM and SNOM, the hidden nano world is now before us to give us new materials which will change the world in the coming years. It may or may not be like the revolution brought about by information technology but it will be similar and it will help maintain the tempo of the IT revolution in addition to making the entry of nano to all other subjects including basic subjects like physics, chemistry, biology, medicine, biotechnology, materials science, electronics etc. SEM is now the most widely used technique in the characterization of nanomaterials. The revolution of SEM approaches a few nanometers and instruments can operate at magnifications that are easily adjusted from 10 to over 3 000 000 keV. Not only does SEM produce topographical information as optical microscopes do, it also provides chemical composition information near the surface. TEM uses a condenser lens system to accelerate electrons to 100 keV or higher, up to 1 MeV, projecting them onto a thin specimen (less than 200 nm) to penetrate the sample thickness undetected. Its greatest advantages are the high magnification, ranging from 50 to 106 keV, and the ability to provide both image and diffraction from a single sample. Scanning probe microscopy has emerged as the most effective tool for observation and manipulation at the nanoscale and is used effectively in advanced laboratories globally. Scanning probe microscopy is a general term used to describe a growing number of techniques and tools that use a sharp probe to scan over a surface and measure some property of that surface by observation of the interaction between the two and provide nanometre scale information concerning the sample. Some examples are STM, AFM and SNOM. SPM is avery important and versatile set of tools for nanotechnology. It operates in real space with A ° ngstrom to nanometre spatial resolution, in contrast to scattering techniques such as SEM that operate in reciprocal space. Rather than using a beam of light or electrons, SPM uses a fine probe that is scanned over a surface. The resolution obtained with this technique can resolve atoms, and true 3-D maps of surfaces are possible. STM is a tool for directly observing the positions of individual atoms in the reconstruction of a material. STM is one of a number of instruments that allow scientists to view and manipulate nanoscale particles, atoms and small molecules AFM is used to measure magnetic forces between a magnetized cantilever and the sample, if the sample is ferromagnetic. The interacting force between the probe and the sample is measured as an indication of the sample–probe distance. Since no current is involved, it can image both conducting and insulating surfaces. This is a major advantage over STM. Compared to a SEM, it has a simpler instrumentation set-up, it can be operated with the sample in the ambient air, and it is much cheaper, hence it is found commonly in laboratories. AFM has been widely used in research laboratories as an extremely high power microscope. It has a significant advantage over STM and SEM in that it can image insulating or semiconducting surfaces directly in ambient atmosphere or even liquids. In SNOM a tapered micropipette or optical fiber is used.It is a technique that can achieve spatial resolution performance beyond the classical diffraction limit by employing a sub-wavelength light source or detector positioned in close proximity to a specimen. Such a sub-wavelength source usually consists of an aperture at the end of a tapered probe, which functions basically as a wave guide. The resolution of SNOM is not high as STM and AFM.



$$Si(OR)_4 + H_2O \longrightarrow OH\,Si(OR)_3 + ROH$$
$$OH\,Si(OR)_3 + H_2O \longrightarrow (OH)_2\,Si(OR)_2 + ROH$$
$$(OH)_2Si(OR)_2 + H_2O \longrightarrow (OH)_3Si(OR) + ROH$$
$$(OH)_3\,Si(OR) + H_2O \longrightarrow (OH)_4Si + ROH$$
$$(OH)_4Si + (OH)_4Si \longrightarrow (OH)_3Si-O-Si\,(OH)_3 + H_2O$$

Scheme 1: Sol-gel formation of nanoparticles.

II. APPLICATION OF NANOPARTICLES FOR THE REMOVAL OF VARIOUS POLLUTANTS

The selective sorption of certain elements based on the stability of complexes formed with functional groups of sorbents has led to the use of these materials for selective enrichments and separation of inorganic ions from different natural and industrial sources. According to researchers at the Pacific North Laboratory (PNL), chemically modified nanoporous ceramics are used to remove contaminants from all types of waste streams faster and at a significantly lower cost than conventional techniques such as ion-exchange resins and activated carbon filters. These nanosponges could be used in a wide range of environmental applications, including drinking-water purification, wastewater treatment, site remediation and waste stabilization. Granular activated carbons (GACs) have been accepted as the industry standard for adsorbing unwanted chemical compounds from water. As a result, they have become ubiquitous throughout industry, wastewater treatment facilities and even in households for purification of drinking water. Scientists have developed robust filters composed entirely of multiwalled carbon nanotubes for the removal of benzene and ferrocene· These filters, shaped like hollow cylinders, are easy to clean and reusable. They can remove bacteria and viruses from water, eliminate heavy hydrocarbons from petroleum, and separate mixtures of benzene and naphthalene· Preconcentration of metal ions using nanoparticles.Recently, it has been found that iron sulfide (FeS) nanoparticles produced by certain bacteria act as excellent adsorbents for a wide range of metal ions in solution, such as As(III), Cd(II), Hg(II) and Pb(II). Waychunas et al. have discussed the structures and reactivity of goethite, akaganeite, hematite, ferrihydrite and schwertmannite nanoparticles (collectively referred to as FeOXnanoparticles). These are the important constituents of soil.Goethite nanoparticles are used for the adsorption of As(V),Cu(II), Hg(II) and Zn(II). The applicability of maghemite(g-Fe$_2$O$_3$) nanoparticles for the selective removal of Cr(VI), Cu(II)and Ni(II) from electroplating wastewater had been studied by Hu et al. Ceria nanoparticles supported on carbon nanotubes (CeO$_2$-CNTs) were used for the removal of arsenate from water by Peng et al. Allophane and boehmite are natural nanomaterials and do not pose much risk either to the physical environment or to human health Allophane has been used as a nanoscavenger for Cu(II) in environmental samples. Boehmite (ALOOH) nanoparticles have been used for the adsorption of arsenic by Anderson. The adsorption behaviour of toxic metal ions like Cu(II), Cr(III),Mn(II), Ni(II), Zn(II), Cd(II), Mo(VI) and rare earth elements on TiO$_2$ nanoparticles has been reported in environmental samplesThe adsorption properties of many oxides strongly depend on the characteristics of solids e.g. morphology, crystal structure, defects, specific surface area, hydroxyl coverage, surface impurities and modifiers and these factors can be controlled by using appropriate modification methods. The basic disadvantage of solid sorbents is the lack of selectivity, which results in interference with target metal ions. To overcome this problem, physical or chemical modification of the sorbent surface with some organic compounds, especially chelating ones, is required. Some examples are given in Table 1.

TABLE 1:
PRECONCENTRATION OF METAL IONS BY NANOPARTICLES

Nanoparticles	Analytical method	Analyte	LOD (mg/L)	Sample	Reference
TiO2	ICP-AES	Cu(II)	0.34	Environmental water samples	118
		Cr(III)	1.14		
		Mn(I I)	0.52		
		Ni(II)	1.78		
TiO2	FAAS	Zn(II)	1.8	Environmental water samples	119
		Cd(II)	3.0		
TiO2	GFAAS	Se(IV)	0.16	Sediment, water samples	120
		Se(VI)	0.14		
TiO2	ICP-AES	Sm(III)	0.08	Stream sediments	121
		Ho(III)	0.1		
		Nd(III)	0.1		
		Tm(III)	0.06		
TiO2	ICP-AES	Au(III)	0.016	Geological samples	122
		Pd(II)	0.012		
		Ag(I)	0.006		
TiO2	ICP-AES	La(III)	0.124	Stream sediments	123
		Yb(III)	0.108		
		Y(III)	0.108		
		Eu(III)	0.28		
		Dy(III)	0.36		
TiO2	ICP-AES	Cr(III)	0.32	Water samples	124

MWCNs	ICP-OES	La(III)
		Yb(III)
		Eu(III)
		Dy(III)
		Y(III)
			3–57	Water samples	125

Al_2O_3	ICP-MS	Mn(II)	0.0067	Environmental water samples	126
		Zn(II)	0.078		
		Pb(II)	0.027		
		Ni(II)	0.038		
		Co(II)	0.0082		
		Cd(II)	0.079		
ZrO_2	ICP-OES	Mn(II)	0.012	Water samples	127
		Zn(II)	0.002		
		Cu(II)	0.058		
		Ni(II)	0.007		

III. CONCLUSIONS

Nanotechnology is a revolutionary science that will have a large impact on our life. A core piece of this technology is the production of nanomaterials for chemical, medical, and environmental applications. Nanomaterials have a number of key physicochemical properties that make them particularly attractive as separation media for purification of natural water and industrial effluents. Environmental application is an important avenue of nanomaterials research. Their capacity together with their relatively low cost and wide availability could increase the use of nanoparticles for environmental and heath protection.Nanoparticles have been found to be suitable replacements for organic solvents and reactive complexants in the extraction and preconcentration of trace metals and organic compounds from natural waters and environmental samples. Only small quantities of largely environmentally benign reagents are used in the synthesis of nanoparticles. No organic solvents are used in the application of nanoparticles as nanoscavengers. The physical advantages of the nanoscavengers approach over the conventional liquid–liquid extraction technique is that large numbers of samples can be rapidly treated with nanoscavengers. This can be carried out at the sampling site, stabilizing the analyte during transport and preanalysis storage. This leads to extractions being carried out without further intervention during the sampling excursion. The last but not least advantage of nanoparticles is that they are highly efficient in the preconcentration of toxic metals and organic compounds. They can be repeatedly used andthe matrix effects are low. There are different types of nanomaterials used for removal of environmental pollutants.

1) The applicability of carbon nanotubes for analytical purposes can be expanded. CNTs present a higher adsorption capacity toward organic pollutants and metal ions than commonly used activated carbon, and the analytes retained on this solid phase can be easily desorbed. Wider practical applications of carbon nanotubes may be hampered by their relatively high unit cost.

2) Zero-valent Fe0/Ni0 nanoparticles have given promising results for the removal of environmental pollutants, but background corrosion of iron particles not only limits the lifetime of these nanoparticles but also substantially decreases the reactivity of these nanoparticles.

3) Surface modifications of nanoparticles give good results for the preconcentration of environmental pollutants. Chemically modified nanoparticles of silica, titania, zirconia and magnesia are more effective, highly selective and more efficient for the preconcentration of the pollutants. Chemisorption of chelating molecules on silica surfaces provides immobility, mechanical stability and water insolubility, thereby increasing the efficiency,sensitivity and selectivity of the analytical application.

ABBREVIATIONS

AAS	atomic absorption spectrometry
CVAAS	cold vapor atomic absorption spectrometry
ESV	electrochemical stripping voltammetry
FAAS	flame atomic absorption spectrometry
GFAAS	graphite furnace atomic absorption spectrometry
HPLC	high-performance liquid chromatography

REFERENCES

[1] K. A. D. Guzman, M. R. Taylor and J. F. Banfield,Environ.Sci.Technol, 2006, 40, 1401.

[2] C. L. Chun, R. L. Penn and W. A. Arnold, Environ.Sci.Technol,2006, 40, 3299.

[3] M. F. Hochella, Geochim.Cosmochim.Acta, 2002, 66, 735.

[4] A. Kay, I. Cesar and M. Gratzel, J.Am. Chem.Soc, 2006, 128, 15714.

[5] D. K. Kim, M. Mikhaylova, Y. Zhang and M. Muhammed,Chem.Mater, 2003, 15, 1617.

[6] D. E.Miser, E. J. Shin, M. R. Hajaligol and F. Rasouli, Appl. Catal.A., 2004, 258, 7.

[7] A. R. Turker, Clean, 2007, 35, 545.

[8] N. S.Wigginton, K. L. Haus and M. F. Hochella, J. Environ. Monit,2007, 9, 1306.

[9] K. Cottingham, Anal.Chem., 2003, 77, 51.

[10] M. Valcarcel, S. Cardens and B. M. Simonet, Anal.Chem, 2007, 79,4788.

Network Intrusion detection and Counter measure selection in virtual network systems

Mandeep Singh[1], Neetu Sharma[2]
[1,2] *Department of Computer Science &Engineering, Ganga Institute of Technology and Management, Kablana, Jhajjar, Haryana, INDIA*

***Abstract*—Network Intrusion detection and Counter measure is a multiphase distributed network intrusion detection and prevention framework in a virtual networking environment that captures and inspects suspicious cloud traffic without interrupting users applications and cloud service. Cloud security is one of most important issues that has attracted a lot of research and development effort in past few years. The proposed solution utilizes a new network control approach called SDN, where networking functions can be programmed through software switch and OpenFlow protocol. NICE is a multiphase distributed network intrusion detection and prevention framework in a virtual networking environment that capture and inspects suspicious cloud traffic without interrupting users applications and cloud service. It employs a reconfigurable virtual networking approach to detect and counter the attempts to compromise VMs, thus preventing Zombie VMs. It optimizes the implementation on cloud servers to minimize resource consumption and consumes less computational overhead compared to proxy-based network intrusion detection solution.**

Abbreviations

1. QG - Queue Graph
2. DG - Dependency Graph
3. ACT - Attack Countermeasure Tree
4. BDD - Binary Decision Diagram
5. BAG - Bayesian Attack Graph
6. IaaS - Infrastructure as a Service
7. SAG - Scenario Attach Graph
8. ACG - Alert Correlation Graph
9. NIDS - Network Intrusion Detection System

I. INTRODUCTION

The area of detecting malicious behaviour has been well explored in the following approaches. *SPOT* focuses on the detection of compromised machines that have been recruited to serve as spam zombies. It is based on sequentially scanning outgoing messages while employing a statistical method *Sequential Probability Ratio Test (SPRT),* to quickly determine whether a host has been compromised. Bot Hunter detects compromised machines based on the fact that a thorough malware infection process has a number of well-defined stages that allow correlating the intrusion alarms triggered by inbound traffic with resulting outgoing communication patterns. Bot Sniffer exploits uniform spatial-temporal behavior characteristics of compromised machines to detect zombies by grouping flows according to server connections and searching for similar behavior in the flow. An *attack graph* is used to represent a series of exploits, called atomic attacks, that lead to an undesirable state. There are many automation tools to construct attack graph. A technique based on a modified symbolic model checking Nu SMV and *Binary Decision Diagrams* (BDDs) was pro-posed to construct attack graph. This model can generate all possible attack paths, but, the scalability is a big issue for this solution. The assumption of monotonicity was introduced, which states that the precondition of a given exploit is never invalidated by the successful pplication of another exploit, ie. attackers never need to backtrack. With this assumption, a concise, scalable graph representation for encoding attack tree can be obtained. An attack graph tool called Mul VAL, adopts a logic programming approach and uses Datalog language to model and analyze network system. The attack graph in the Mul VAL is constructed by accumulating true facts of the monitored network system. The attack graph construction process will terminate efficiently because the number of facts is polynomial in system.

The major problems for any IDS implementation are the false alarms and the large volume of raw alerts from IDS. Many attack graph-based alert correlation techniques have been proposed. An in memory structure, called queue graph (QG), was devised to trace alerts matching each exploit in the attack graph. However, the implicit correlations in this design make it difficult to use the correlated alerts in the graph for analysis of similar attack scenarios. A modified attack-graph-based correlation algorithm was proposed to create explicit correlations only by matching alerts to specific exploitation nodes in the attack graph with multiple mapping functions, and devised an alert dependencies graph (DG) to group related alerts with multiple correlation criteria. However, this algorithm involved all pairs shortest path searching and sorting in DG, which consumes considerable computing power. Several solutions have been proposed to select optimal counter measures based on the likelihood of the attack path and cost benefit analysis. An *attack countermeasure tree* (ACT) was proposed to consider attacks and countermeasures together in an attack tree structure. Here several objective functions based on greedy and branch and bound techniques were devised to minimize the number of countermeasure, reduce investment cost, and maximize the benefit from implementing a certain countermeasure set. In this design, each countermeasure optimization problem could be solved with and without probability assignments to the model. However, this solution focuses on a static attack scenario and predefined countermeasure for each attack. Another attack graph, *Bayesian attack graph* (BAG) was proposed to address dynamic security risk management problem and applied a genetic algorithm to solve countermeasure optimization problem.

II. MODELS FOR COUNTERMEASURES

Threat Model : This protection model focuses on virtual network based attack detection and reconfiguration solutions to improve the resiliency to zombie explorations. The proposed solution can be deployed in an IaaS cloud networking system. Cloud service users are free to install whatever operating systems or applications they want, even if such action may introduce vulnerabilities to their controlled VMs.

.

Attack Graph Model : An attack graph is a modeling tool to illustrate all possible multistage, multihost attack paths that are crucial to understand threats and then to decide appropriate countermeasures. In an attack graph, each node represents either precondition or consequence of an exploit. Attack graph is helpful in identifying potential threats, possible attacks, and known *vulnerabilities* in a cloud system. If an event is recognized as a potential attack, specific countermeasures can be applied to mitigate its impact or take actions to prevent it from contaminating the cloud system. To represent the attack and the result of such actions, the notation of MulVAL logic attack graph is extended and is defined as *SAG*. An SAG is a tuple SAG = (V, E), where

• V= N_C N_D N_R denotes a set of vertices that include three types namely

i. conjunction nodeN_C to represent exploit,
ii. disjunction node N_D to denote result of exploit,
iii. and root node N_R for showing initial step of an attack scenario.

• E = Epre Epost denotes the set of directed edges. An edge e Epre $N_D \times N_C$ represents that N_D must be satisfied to achieve N_C. An edge e Epost $N_C \times N_D$ means that the consequence shown by N_D can be obtained if N_C is satisfied. Node vc N_C is defined as a three tuple *(Hosts, vul, alert*) representing a set of IP addresses, vulnerability information such as CVE , and alerts related to vc, respectively. N_D behaves like a logical OR operation and contains details of the results of actions. N_R represents the root node of the SAG. A new *Alert Correlation Graph (ACG)* is defined to map alerts in ACG to their respective nodes in SAG. To keep track of attack progress, the source and destination IP addresses are tracked for attack activities. An ACG is a three tuple *ACG = (A,E,P*), where

i. A is a set of aggregated alerts. An alert a A is a data structure *(src,dst,cls,ts)* representing source IP address, destination IPaddress, type of the alert, and time stamp of the alert respectively.
ii. Each alert *a* maps to a pair of vertices (v_c,v_d) in SAG using map(a) function, ie. map(*a*) : $a \rightarrow \{(v_c,v_d)|$ (a.src v_c.Hosts) (a.dst v_d.Hosts) (a.cls=v_c.vul)}
iii. E is a set of directed edges representing correlation between two alerts (a,a’) if criteria below satisfied:
  a. (a.ts < a’.ts) (a’.ts - a.ts<threshold).
  b. (v_d,v_d) E_{pre} : (a.dst v_d.Hosts a’.src v_c.Hosts).

P is set of paths in ACG. A path Si | P is a set of related alerts in chronological order.

A contains aggregated alerts rather than raw alerts. Raw alerts having same source and destination IP addresses, attack type, and time stamp within a specified window are aggregated as *Meta Alerts*. Each ordered pair (a, a’) in ACG maps to two neighbor vertices in SAG with time stamp difference of two alerts within a predefined threshold. ACG shows dependency of alerts in chronological order and related alerts are found in the same attack scenario by searching the alert path in ACG. A set P is used to store all paths from root alert to the target alert in the SAG, and each path Si | P represents alerts that belong to the same attack scenario. Alert Correlation algorithm is followed for every alert detected and returns one or more paths Si. For every alert ac that is received from the IDS, it is added to ACG if it does not exist. For this new alert ac, the corresponding vertex in the SAG is found by using function map(ac). For this vertex in SAG, alert related to its parent vertex of type NC is then correlated with the current alert ac. This creates a new set of alerts that belong to a path Si in ACG or splits out a new path Si+1 from Si with subset of Si before the alert a and appends ac to Si+1. In the end of this algorithm, the ID of ac will be added to alert attribute of the vertex in SAG. Algorithm 1 returns a set of attack paths S in ACG.

Algorithm 1. Alert Correlation

```
Require: alert ac, SAG, ACG
if (ac is a new alert) then
    create node ac in ACG
    n1 ← vc     map(ac)
    for all n2     parent(n1) do
        create edge (n2.alert,ac)
        for all Si containing a do
            if a is the last element in Si then
                append ac to Si
            else
                create path Si+1 = { subset(Si,a),ac}
            end if
        end for
        add ac to n1.alert
    end for
end if
return S
```

VM Protection Model : The VM protection model of NICE consists of a VM profiler, a security indexer, and a state monitor. Security index is specified for all the VMs in the network based on various factors like connectivity, the number of vulnerabilities present and their impact scores. The impact score of a vulnerability helps to judge the confidentiality, integrity, and availability impact of the vulnerability being exploited. Connectivity metric of a VM is decided by evaluating incoming and outgoing connections. VM states can be defined as follows:

i. *Stable*: There does not exist any known vulnerability on the VM.
ii. *Vulnerable*: Presence of one or more vulnerabilities on a VM, which remains unexploited.
iii. *Exploited*: At least one vulnerability has been exploited and the VM is compromised.
iv. *Zombie*: VM is under control of attacker.

III. System Design and Implementation

The NICE framework is illustrated in Fig. 1. Major components in this framework are distributed and light-weighted NICE-A on each physical cloud server, a network controller, a VM profiling server, and an attack analyzer. The latter three components are located in a centralized control center connected to software switches on each cloud server.

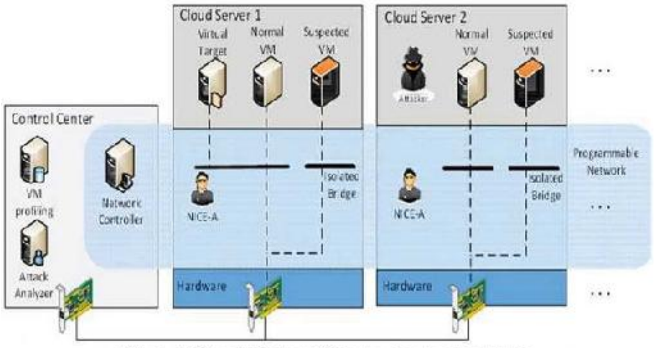


Fig. 1. NICE architecture within one cloud server cluster.

NICE-A is a software agent implemented in each cloud server connected to the control center through a dedicated and isolated secure channel, which is separated from the normal data packets using *OpenFlow tunneling* or *VLAN* approaches. The network controller is responsible for deploying attack countermeasures based on decisions made by the attack analyzer. Intrusion detection alerts are sent to control center when suspicious or anomalous traffic is detected. After receiving an alert, attack analyzer evaluates the severity of the alert based on the attack graph, decides what countermeasure strategies to take, and then initiates it through the network controller. An attack graph is established according to the vulnerability information derived from both offline and real-time vulnerability scans. Offline scanning can be done by running penetration tests and online real-time vulnerability scanning can be triggered by the network controller or when new alerts are generated by the NICE-A. Once new vulnerabilities are discovered or countermeasures are deployed, the attack graph will be reconstructed. Countermeasures are initiated by the attack analyzer based on the evaluation results from the cost benefit analysis of the effectiveness of countermeasures. Then, the network controller initiates countermeasure actions by reconfiguring virtual or physical OFSs. The components of NICE are as follows:

NICE-A : The NICE-A is a *Network-based Intrusion Detection System (NIDS)* agent installed in either Dom0 or DomU in each cloud server. It scans the traffic going through Linux bridges that control all the traffic among VMs and in/out from the physical cloud servers. Here Snort is used to implement NICE-A in Dom0. It will sniff a mirroring port on each virtual bridge in the Open vSwitch (OVS). Each bridge forms an isolated subnet in the virtual network and connects to all related VMs. The traffic generated from the VMs on the mirrored software bridge will be mirrored to a specific port on a specific bridge using SPAN, RSPAN, or ERSPAN methods. Dom0 in the Xen environment is a privilege domain, that includes a virtual switch for traffic switching among VMs and network drivers for physical network interface of the cloud server. It is more efficient to scan the traffic in Dom0 because all traffic in the cloud server needs go through it. The alert detection quality of NICE-A depends on the implementation of NICE-A, which uses Snort. The individual alert detections false alarm rate does not change. However, the false alarm rate could be reduced through this architecture design.

VM Profiling : Virtual machines in the cloud can be profiled to get precise information about their state, services running, open ports, and so on. Any VM that is connected to more number of machines is more crucial than the one connected to fewer VMs because the effect of compromise of a highly connected VM can cause more damage. An attacker can use port-scanning program to perform an intense examination of the network to look for open ports on any VM. So information about any open ports on a VM and the history of opened ports plays a significant role in determining how vulnerable the VM is. All these factors combined will form the VM profile. VM profiles are maintained in a database and contain comprehensive information about vulnerabilities, alert, and traffic. The data comes from:

- *Attack graph generator*. While generating the attack graph, every detected vulnerability is added to its corresponding VM entry in the database.
- *NICE-A*. The alert involving the VM will be recorded in the VM profile database.
- *Network controller*. The traffic patterns involving the VM are based on five tuples *(source MAC address, destination MAC address, source IP address, destination IP address, protocol)*. There can be traffic pattern, where packets emanate from a single IP and are delivered to multiple destination IP addresses, and vice versa.

Attack Analyzer : The major functions of NICE system are performed by attack analyzer, which includes procedures such as attack graph construction and update, alert correlation, and countermeasure selection. The process of constructing and utilizing the SAG consists of three phases: Information gathering, attack graph construction, and potential exploit path analysis. With this information, attack paths can be modeled using SAG. Each node in the attack graph represents an exploit by the attacker. Each path from an initial node to a goal node represents a successful attack. NICE attack graph is constructed based on the following information:

- Cloud system information is collected from the node controller (i.e., Dom0 in XenServer).The information includes the number of VMs in the cloud server, running services on each VM, and VMs Virtual Interface (VIF) information.
- Virtual network topology and configuration information is collected from the network controller, which includes virtual network topology, host connectivity, VM connectivity, every VMs IP address, MAC address, port information, and traffic flow information.
- Vulnerability information is generated by both on demand vulnerability scanning (i.e., initiated by the network controller and NICE-A) and regular penetration testing using the well-known vulnerability databases. The attack analyzer also handles alert correlation and analysis operations. This component has two major functions: 1) constructs ACG, and 2) provides threat information and appropriate countermeasures to network controller for virtual network reconfiguration. After receiving an alert from NICE-A, alert analyzer matches the alert in the ACG. If the alert already exists in the graph and it is a known attack, the attack analyzer performs countermeasure selection procedure according to the Countermeasure Selection algorithm, and then notifies network controller immediately to deploy countermeasure or mitigation actions. If the alert is new, attack analyzer will perform alert correlation and analysis according to Algorithm 1, and updates ACG and SAG. This algorithm correlates each new alert to a matching alert correlation set (i.e., in the same attack scenario). A selected countermeasure is applied by the network controller based on the severity of evaluation results. If the alert is a new vulnerability and is not present in the NICE attack graph, the attack analyzer adds it to attack graph and then reconstructs it.

Network Controller : The network controller is a key component to support the programmable networking capability to realize the virtual network reconfiguration feature based on OpenFlow protocol. The network controller is responsible for collecting network information of current OpenFlow network and provides input to the attack analyzer to construct attack graphs. Through the cloud internal discovery modules that use DNS, DHCP, LLDP, and flow initiations, network controller is able to discover the network connectivity information from OVS and OFS. This information includes current data paths on each switch and detailed flow information associated with these paths, such as

TCP/IP and MAC header. The network flow and topology change information will be automatically sent to the controller and then delivered to attack analyzer to reconstruct attack graphs. Another important function of the network controller is to assist the attack analyzer module. According to the OpenFlow protocol, when the controller receives the first packet of a flow, it holds the packet and checks the flow table for complying traffic policies. In NICE, the network control also consults with the attack analyzer for the flow access control by setting up the filtering rules on the corresponding OVS and OFS. Once a traffic flow is admitted, the following packets of the flow are not handled by the network controller, but monitored by the NICE-A. Network controller is also responsible for applying the countermeasure from attack analyzer. Based on VM Security Index (VSI) and severity of an alert, countermeasures are selected by NICE and executed by the network controller. If a severe alert is triggered and identifies some known attacks, or a VM is detected as a zombie, the network controller will block the VM immediately. An alert with medium threat level is triggered by a suspicious compromised VM. Countermeasure in such case is to put the suspicious VM with exploited state into quarantine mode and redirect all its flows to NICE-A DPI mode. An alert with a minor threat level can be generated due to the presence of a vulnerable VM. For this case, to intercept the VMs normal traffic, suspicious traffic to/from the VM will be put into inspection mode, in which actions such as restricting its flow bandwidth and changing network configurations will be taken to force the attack exploration behavior to stand out.

IV. COUNTERMEASURE SELECTION

When vulnerabilities are discovered or some VMs are identified as suspicious, several countermeasures can be taken to restrict attackers capabilities and it is important to differentiate between compromised and suspicious VMs. The countermeasure serves the purpose of: 1) protecting the target VMs from being compromised, and 2) making attack behavior stand prominent so that the attackers actions can be identified.

Security Measurement Metrics : The issue of security metrics has attracted much attention and there has been significant effort in the development of quantitative security metrics in recent years. Among different approaches, using attack graph as the security metric model for the evaluation of security risks is a good choice. To assess the network security risk condition for the current network configuration, security metrics are needed in the attack graph to measure risk likelihood. After an attack graph is constructed, vulnerability information is included in the graph. For the initial node or external node (i.e., the root of the graph, N_R N_D), the priori probability is assigned on the likelihood of a threat source becoming active and the difficulty of the vulnerability to be exploited. GV is used to denote the *priori risk probability* for the root node of the graph and usually the value of GV is assigned to a high probability, e.g., from 0.7 to 1. For the internal exploitation node, each attack-step node e N_C will have a probability of vulnerability exploitation denoted as $G_M[e]$. $G_M[e]$ is assigned according to the Base Score (BS) from Common Vulnerability Scoring System (CVSS). The BS is calculated by the impact and exploitability factor of the vulnerability. BS can be directly obtained from National Vulnerability Database by searching for the vulnerability CVE id

$$BS = (0.6 \times IV + 0.4 \times E - 1.5) \times f(IV),$$

where

$$IV = 10.41 \times (1 - (1 - C) \times (1 - I) \times (1 - A)),$$

$$E = 20 \times AC \times AU \times AV ,$$

and

$$f(IV) = \begin{cases} 0 & \text{if } IV = 0, \\ 1.176 & \text{otherwise.} \end{cases}$$

The impact value (IV) is computed from three basic parameters of security namely *confidentiality* (C), *integrity* (I), and *availability* (A). The *exploitability* (E) score consists of *access vector* (AV), *access complexity* (AC), and *authentication instances* (AU). The value of BS ranges from 0 to 10. In the attack graph, each internal node is assigned with its BS value divided by 10, as shown in

$$GM = Pr(e=T) = BS(e)/10, \quad e \quad N_C$$

In the attack graph, the relations between exploits can be disjunctive or conjunctive according to how they are related through their dependency conditions. Such relationships can be represented as conditional probability, where the risk probability of current node is determined by the relationship with its predecessors and their risk probabilities. Given below are the probability derivation relations:

- for any attack-step node n NC with immediate predecessors set W = parent(n),

$$P_r(n \mid W) = G_M[n] \times \prod_{s \varepsilon W} P_r(s \mid W);$$

- for any privilege node n N_D with immediate predecessors set W= parent(n), and then

$$P_r(n \mid W) = 1 - \prod_{s \varepsilon W} (1 - P_r(s \mid W)).$$

Once conditional probabilities have been assigned to all internal nodes in SAG, risk values from all predecessors can be merged to obtain the cumulative risk probability or absolute risk probability for each node. Based on derived conditional probability assignments on each node, an effective security hardening plan or a mitigation strategy can be derived:

- for any attack-step node n N_C with immediate predecessor set W = parent(n),

$$P_r(n) = Pr(n \mid W) \times \prod_{s \varepsilon W} P_r(s);$$

- for any privilege node n N_D with immediate predecessor set W= parent(n), and then

$$P_r(n) = 1 - \prod_{s \varepsilon W} (1 - P_r(s)).$$

Mitigation Strategies : Based on the security metrics defined in the previous section, NICE is able to construct the mitigation strategies in response to detected alerts. *Countermeasure pool* can be defined as follows:

A countermeasure pool CM = cm1, cm2, ... , cm2 is a set of countermeasures. Each cm is a tuple *cm*=(cost, intrusiveness, condition, effectiveness), where

i. cost is the unit that describes the expenses required to apply the countermeasure in termsof resources and operational complexity, and it is defined in a range from 1 to 5, and higher metric means higher cost;
ii. intrusiveness is the negative effect that a countermeasure brings to the SLA and the value of intrusiveness is 0 if the countermeasure has no impacts on the SLA;
iii. condition is the requirement for the corresponding countermeasure;

iv. effectiveness is the percentage of probability changes of the node, for which this counter measure is applied.

In general, there are many countermeasures that can be applied to the cloud virtual networking system depending on available countermeasure techniques that can be applied. The optimal countermeasure selection is a multiobjective optimization problem, to calculate MIN (impact, cost) and MAX(benefit). In NICE, the network reconfiguration strategies mainly involve two levels of action: Layer-2 and layer-3. At layer-2, virtual bridges and VLANs are main component in clouds virtual networking system to connect two VMs directly. A virtual bridge is an entity that attaches VIFs. Virtual machines on different bridges are isolated at layer 2. VIFs on the same virtual bridge but with different VLAN tags cannot communicate to each other directly. Based on this layer-2 isolation, NICE can deploy layer-2 network reconfiguration to isolate suspicious VMs. Layer-3 reconfiguration is another way to disconnect an attack path. Through the network controller, the flow table on each OVS or OFS can be modified to change the network topology. Using the virtual network reconfiguration approach at lower layer has the advantage in that upper layer applications will experience minimal impact. Especially, this approach is only possible when using software switching approach to automate the reconfiguration in a highly dynamic networking environment. Countermeasures such as traffic isolation can be implemented by utilizing the traffic engineering capabilities of OVS and OFS to restrict the capacity and reconfigure the virtual network for a suspicious flow. When a suspicious activity such as network and port scanning is detected in the cloud system, it is important to determine whether the detected activity is indeed malicious or not. For example, attackers can purposely hide their scanning behavior to prevent the NIDS from identifying their actions. In such situation, changing the network configuration will force the attacker to perform more explorations, and in turn will make their attacking behaviour stand out.

Countermeasure Selection Algorithm : Algorithm2 presents how to select the optimal countermeasure for a given attack scenario. Input to the algorithm is an alert, attack graph G, and a pool of countermeasures CM. The algorithm starts by selecting the node vAlert that corresponds to the alert generated by a NICE-A. Before selecting the countermeasure, the distance of vAlert to the target node is counted. If the distance is greater than a threshold value, countermeasure selection is not performed, but the ACG is updated to keep track of alerts in the system. For the source node vAlert, all the reachable nodes (including the source node) are collected into a set T. Because the alert is generated only after the attacker has performed the action, the probability of vAlert is set to 1 and calculate the new probabilities for all of its child (downstream) nodes in the set T. Now, for all t   T the applicable countermeasures in CM are selected and new probabilities are calculated according to the effectiveness of the selected countermeasures. The change in probability of target node gives the benefit for the applied countermeasure. In the next double for-loop, the Return of Investment(ROI) is computed for each benefit of the applied countermeasure. The countermeasure which when applied on a node gives the least value of ROI, is regarded as the optimal countermeasure. Finally, SAG and ACG are also updated before terminating the algorithm. The complexity of Algorithm 2 is O(| V | × | CM |,where | V | is the number of vulnerabilities and | CM | represents the number of counter measures.

Algorithm 2. Countermeasure Selection

```
Require: Alert,G(E,V),CM
Let $v_{Alert}$ = Source node of the Alert
if Distance to Target($v_{Alert}$)>threshold then
    Update_ACG
    return
end if
Let T=Descendant($v_{Alert}$)     $v_{Alert}$
Set $P_r(v_{Alert})$=1
Calculate Risk Prob(T)
Let benefit[ | T |, | C |] =∅
for each t     T do
    for each cm     CM do
        if cm.condition(t) then
            Pr(t)= Pr(t)     (1 - cm.effectiveness)
            Calculate Risk Prob(Descendant(t))
            benefit[t,cm]=     Pr(target node)
        end if
    end for
end for
Let ROI[| T |, | CM |] =∅
for each t     T do
    for each cm     CM do
        ROI[t,cm]= benefit[t,cm]/(cost.cm + intrusiveness.cm)
    end for
end for
Update_SAG and Update_ACG
return Select_Optimal_CM(ROI)
```

V. PERFORMANCE EVALUATION

The performance evaluation is conducted in two directions: The *security performance*, and *the system computing and network reconfiguration overhead due to introduced security mechanism.*

Security Performance Analysis : The security performance of NICE is demonstrated by creating a virtual network testing environment consisting of all the components of NICE.

To evaluate the security performance, a demonstrative virtual cloud system consisting of public (public virtual servers) and private (VMs) virtual domains is established as shown in Fig. 2. Cloud Servers 1 and 2 are connected to Internet through the external firewall. In the DMZ on Server 1, there is one Mail server, one DNS server and one web server. Public network on Server 2 houses SQL server and NAT Gateway Server.

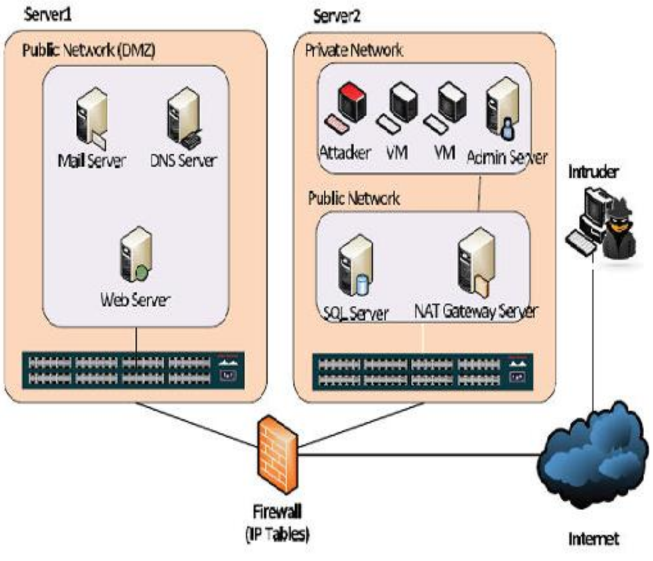
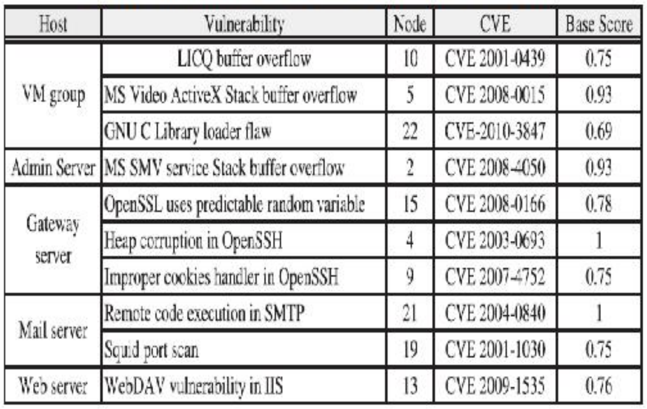


Fig.2 Virtual network topology for security evaluation.

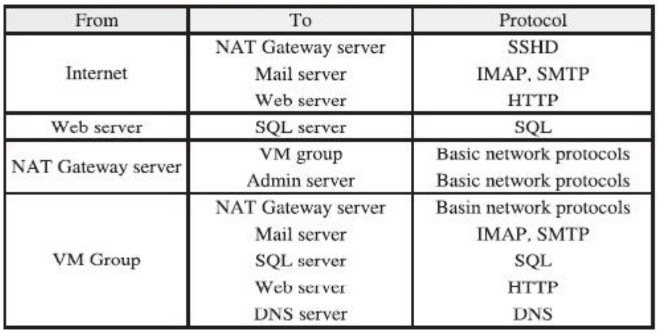
Remote access to VMs in the private network is controlled through SSHD (i.e., SSH Daemon) from the NAT Gateway Server. Table 1 shows the vulnerabilities present in this network and Table 2 shows the corresponding network connectivity that can be explored based on the identified vulnerabilities.

TABLE 1
Vulnerabilities in the Virtual Networked System



Host	Vulnerability	Node	CVE	Base Score
VM group	LICQ buffer overflow	10	CVE 2001-0439	0.75
	MS Video ActiveX Stack buffer overflow	5	CVE 2008-0015	0.93
	GNU C Library loader flaw	22	CVE-2010-3847	0.69
Admin Server	MS SMV service Stack buffer overflow	2	CVE 2008-4050	0.93
Gateway server	OpenSSL uses predictable random variable	15	CVE 2008-0166	0.78
	Heap corruption in OpenSSH	4	CVE 2003-0693	1
	Improper cookies handler in OpenSSH	9	CVE 2007-4752	0.75
Mail server	Remote code execution in SMTP	21	CVE 2004-0840	1
	Squid port scan	19	CVE 2001-1030	0.75
Web server	WebDAV vulnerability in IIS	13	CVE 2009-1535	0.76

TABLE 2
Virtual Network Connectivity



From	To	Protocol
Internet	NAT Gateway server	SSHD
	Mail server	IMAP, SMTP
	Web server	HTTP
Web server	SQL server	SQL
NAT Gateway server	VM group	Basic network protocols
	Admin server	Basic network protocols
VM Group	NAT Gateway server	Basin network protocols
	Mail server	IMAP, SMTP
	SQL server	SQL
	Web server	HTTP
	DNS server	DNS

Attack Graph and Alert Correlation : The attack graph can be generated by utilizing network topology and the vulnerability information, and it is shown in Fig. 3. As the attack progresses, the system generates various alerts that can be related to the nodes in the attack graph. Creating an attack graph requires knowledge of network connectivity, running services, and their vulnerability information. This information is provided to the attack graph generator as the input. Whenever a new vulnerability is discovered or there are changes in the network connectivity and services running through them, the updated information is provided to attack graph generator and old attack graph is updated to a new one. SAG provides information about the possible paths that an attacker can follow. ACG serves the purpose of confirming attackers behavior, and helps in determining false positive and false negative. ACG can also be helpful in predicting attackers next steps.

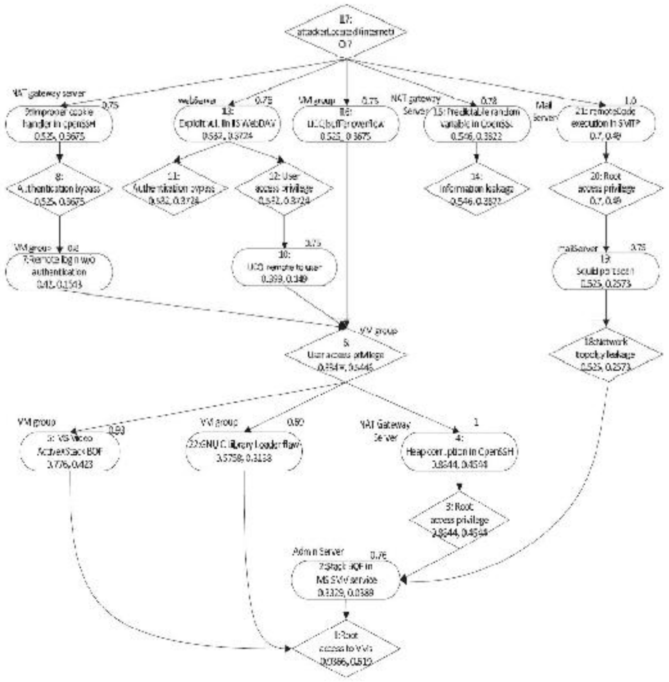


Fig. 3. Attack graph for the test network

Countermeasure Selection : To illustrate how NICE works, consider an example where an alert is generated for node 16 (v_{Alert}=16) when the system detects LICQ Buffer overflow. After the alert is generated, the cumulative probability of node 16 becomes 1 because that attacker has already compromised that node.This triggers a change in cumulative probabilities of child nodes of node 16. Now, the next step is to select the countermeasures from the pool of countermeasures CM. If the countermeasure CM4: Create filtering rules is applied to node 5 and assuming that this countermeasure has effectiveness of 85 percent, the probability of node 5 will change to 0.1164, which causes change in probability values of all child nodes of node 5 thereby accumulating to a decrease of 28.5 percent for the target node 1. Following the same approach for all possible countermeasures that can be applied, the percentage change in the cumulative probability of node 1, i.e., benefit computed are shown in Fig. 4. Apart from calculating the benefit measurements, the evaluation based on ROI is done and represent a comprehensive evaluation considering benefit, cost, and intrusiveness of countermeasure. Fig. 5 shows the ROI evaluations for presented countermeasures. Results show that countermeasures CM2 and CM8 on node 5 have the maximum benefit evaluation; however, their cost and intrusiveness scores indicate that they might not be good candidates for the optimal countermeasure and ROI evaluation results confirm this. The ROI evaluations demonstrate that CM4 on node 5 is the optimal solution.

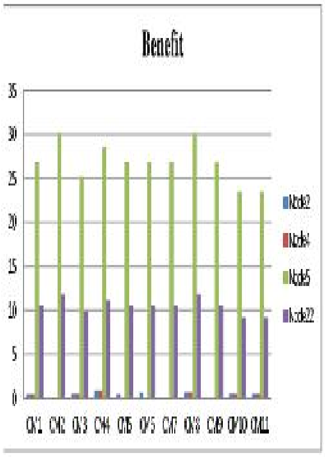


Fig. 4. Benefit evaluation chart.

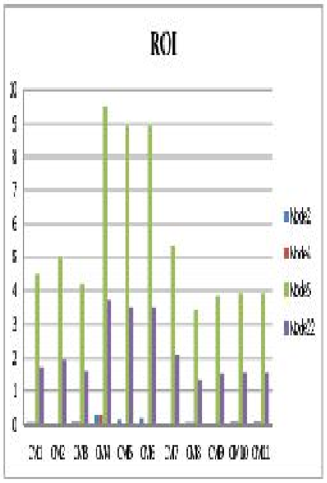


Fig 5. ROI evaluation chart.

Experiment in Private Cloud Environment : For performance analysis and capacity test, configuration in Table 3 is extended to create another test environment, which includes 14 VMs across three cloud servers and configured each VM as a target node to create a dedicated SAG for each VM. These VMs consist of Windows (W) and Linux(L) machines in the private network 172.16.11.0/24, and contains more number of vulnerabilities related to their OSes and applications. Penetration testing scripts are created with Metasploit framework and Armitage as attackers in the test environment. These scripts emulate attackers from different places in the internal and external sources, and launch diversity of attacks based on the vulnerabilities in each VM. To evaluate security level of a VM, a VSI is defined to represent the security level of each VM in the current virtual network environment. This VSI refers to the VEAbility metric and utilizes two parameters that include Vulnerability and Exploitability as security metrics for a VM. The VSI value ranges from 0 to 10, where lower value means better security.VSI for a virtual machine k is defined as

$$VSI_k = (V_k+E_k)/2$$

where

i. V_k is vulnerability score for VM k. The score is the exponential average of BS from each vulnerability in the VM or a maximum 10, i.e.,V_k= min{10, $\ln\Sigma e^{BaseScore(v)}$}

ii. E_k is exploitability score for VM k. It is the exponential average of exploitability score for all vulnerabilities or a maximum 10 multiplied by the ratio of network services on the VM, i.e.,$E_k = (\min\{10, \ln\Sigma\ e^{ExploitabilityScore(v)}\}) \times S_k/NS_k$. S_k represents the number of services provided by VM k. NS_k represents the number of network services the VM k can connect to.

Basically, vulnerability score considers the BSs of all the vulnerabilities on a VM. The BS depicts how easy it is for an attacker to exploit the vulnerability and how much damage it may incur. The exponential addition of BSs allows the vulnerability score to incline toward higher BS values and increases in logarithm-scale based on the number of vulnerabilities. The exploitability score on the other hand shows the accessibility of a target VM, and depends on the ratio of the number of services to the number of network services. Higher exploitability score means that there are many possible paths for that attacker to reach the target. VSI can be used to measure the security level of each VM in the virtual network in the cloud system. A VM with higher value of VSI means is easier to be attacked. To prevent attackers from exploiting other vulnerable VMs, the VMs with higher VSI values need to be monitored closely by the system (e.g., using DPI) and mitigation strategies may be needed to reduce the VSI value when necessary. Fig. 6 shows the plotting of VSI for these virtual machines before countermeasure selection and application. Fig. 7 compares VSI values before and after applying the countermeasure CM4, i.e., creating filtering rules. It shows the percentage

change in VSI after applying countermeasure on all of the VMs. Applying CM4 avoids vulnerabilities and causes VSI to drop without blocking normal services and ports.

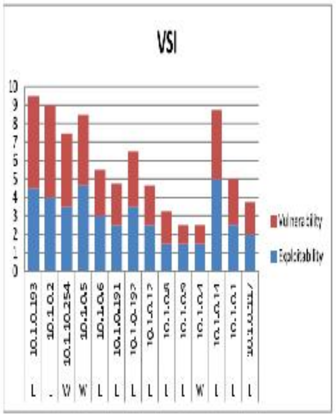


Fig.6. VM security index.

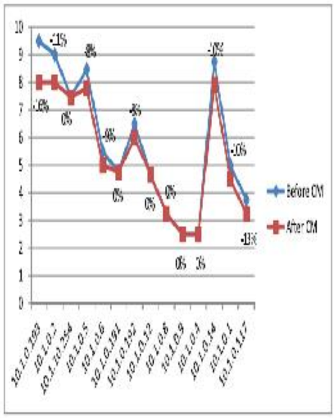


Fig.7. Change in VSI.

False Alarms : A cloud system with hundreds of nodes will have huge amount of alerts raised by Snort. Not all of these alerts can be relied upon, and an effective mechanism is needed to verify if such alerts need to be addressed. Since Snort can be programmed to generate alerts with CVE id, one approach that NICE provides is to match if the alert is actually related to some vulnerability being exploited. If so, the existence of that vulnerability in SAG means that the alert is more likely to be a real attack. Thus, the false positive rate will be the joint probability of the correlated alerts, which will not increase the false positive rate compared to each individual false positive rate. In the case of zero-day attack, where the vulnerability is discovered by the attacker but is not detected by vulnerability scanner, the alert being real will be regarded as false, given that there does not exist corresponding node in SAG. Thus, current research does not address how to reduce the false negative rate. It is important to note that vulnerability scanner should be able to detect most recent vulnerabilities and sync with the latest vulnerability database to reduce the chance of Zero-day attacks.

NICE System Performance

NICE was evaluated based on Dom0 and DomU implementations with mirroring-based and proxy-based attack detection agents (i.e., NICE-A). In mirrorbased IDS scenario, two virtual networks were established in each cloud server: Normal network and monitoring network. NICE-A is connected to the monitoring network. Traffic on the normal network is mirrored to the monitoring network using Switched Port Analyzer (SPAN) approach. In the proxy-based IDS solution, NICE-A interfaces two VMs and the traffic goes through NICE-A. Additionally, the NICE-A have been deployed in Dom0 and it removes the traffic duplication function in mirroring and proxy-based solutions. NICE-A running in Dom0 is more efficient because it can sniff the traffic directly on the virtual bridge. However, in DomU, the traffic need to be duplicated on the VMs VIF, causing overhead. When the IDS is running in Intrusion Prevention System (IPS) mode, it needs to intercept all the traffic and perform packet checking, which consumes more system resources as compared to IDS mode. To demonstrate performance evaluations, four metrics namely CPU utilization, network capacity, agent processing capacity, and communication delay were used. The evaluation on cloud servers with Intel quad-core Xeon 2.4-GHz CPU and 32-G memory was performed. Packet generator was used to mimic real traffic in the cloud system. As shown in Fig. 8, the traffic load, in the form of packet sending speed, increases from 1 to 3,000 packets per second. The performance at Dom0 consumes less CPU and the IPS mode consumes the maximum CPU resources. When the packet rate reaches to 3,000 packets per second, the CPU utilization of IPS at DomU reaches its limitation, while the IDS mode at DomU only occupies about 68 percent.

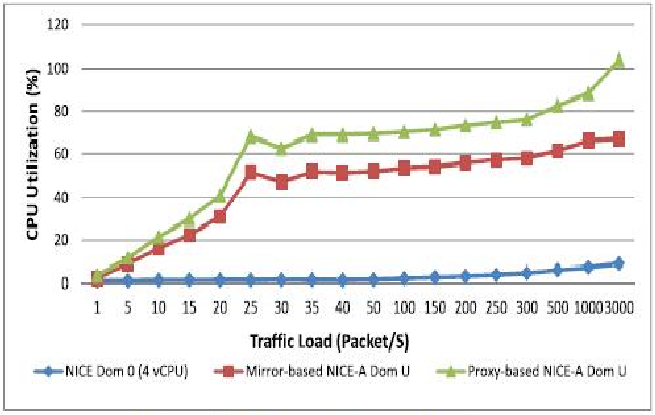


Fig.8. CPU utilization of NICE-A.

Fig. 8, represents the performance of NICE-A in terms of percentage of successfully analyzed packets. The higher this value is, more packets this agent can handle. IPS agent demonstrates 100 percent performance because every packet captured by the IPS is cached in the detection agent buffer. However, 100 percent success analyzing rate of IPS is at the cost of the analyzing delay. For other two types of agents, the detection agent does not store the captured packets and, thus, no delay is introduced. However, they all experience packet drop when traffic load is huge. For a small-scale cloud system this approach works well. The performance evaluation includes two parts. First, security performance evaluation. It shows that the system helps to prevent vulnerable VMs from being compromised and do so in less intrusive and cost effective manner. Second, CPU and throughput performance evaluation. It shows the limits of using the proposed solution in terms of networking throughputs based on software switches and CPU usage when running detection engines on Dom 0 and Dom U. The performance results provide a benchmark for the given hardware setup and shows how much traffic can be handled by using a single detection domain.

VI. CONCLUSION

NICE is used to detect and mitigate collaborative attacks in the cloud virtual networking environment. NICE utilizes the attack graph model to conduct attack detection and prediction. The proposed solution investigates how to use the programmability of software switches-based solutions to improve the detection accuracy and defeat victim exploitation phases of collaborative attacks. The system performance evaluation demonstrates the feasibility of NICE and shows that the proposed solution can significantly reduce the risk of the cloud system from being exploited and abused

by internal and external attackers. NICE only investigates the network IDS approach to counter zombie explorative attacks.

VII. FUTURE SCOPE

To improve the detection accuracy, *host-based IDS* solutions are needed to be incorporated and to cover the whole spectrum of IDS in the cloud system. This should be investigated in the future work. The scalability of the proposed NICE solution can be investigated by investigating the decentralized network control and attack analysis model.

REFERENCES

[1] Chun-Jen Chung, Pankaj Khatkar, TianyiXing,Jeongkeun Lee and Dijiang Huang: Nice-Network Intrusion Detection and Countermeasure Selection in Virtual Network Systems:IEEE Transactions on Dependable and Secure Computing, 10(4):198 211, July 2013.
[2] Cloud Sercurity Alliance: Top Threats to Cloud Computing v1.0:https://cloudsecurityalliance.org/topthreats/csathreats. v1.0.pdf, Mar. 2010.
[3] B. Joshi, A. Vijayan, and B. Joshi: Securing Cloud Computing Environment Against DDoS Attacks: Proc. IEEE Intl Conf. Computer Comm. and Informatics (ICCCI 12), Jan. 2012.
[4] Open vSwitch Project: http://openvswitch.org, May 2012
[5] Z. Duan, P. Chen, F. Sanchez, Y. Dong, M. Stephenson, and J.Barker: Detecting Spam Zombies by Monitoring Outgoing Messages: IEEE Trans. Dependable and Secure Computing, vol. 9, no. 2, pp. 198-210, Apr. 2012.
[6] X. Ou, S. Govindavajhala, and A.W. Appel: MulVAL: A Logic-Based Network Security Analyzer: Proc. 14th USENIX Security Symp., pp. 113-128, 2005.
[7] S. Roschke, F. Cheng, and C. Meinel: A New Alert Correlation Algorithm Based on Attack Graph: Proc. Fourth Intl Conf. Computational Intelligence in Security for Information Systems, pp. 58-67, 2011.
[8] M. Tupper and A. Zincir-Heywood: VEA-bility Security Metric: A Network Security Analysis Tool: Proc. IEEE Third Intl Conf. Availability, Reliability and Security (ARES 08), pp. 950-957, Mar.2008.

New Era in Technological Development: NGN

Savita[1]

[1] *Department of Electronics and Communicaton Enggineering, Ganga Institute of Technology and Management, Kablana, Jhajjar, Haryana, INDIA*

***Abstract*—NGN is a shift from a “one network-one service” approach to a “one network-may services”. Next generation networks are the migration to fully Internet Protocol enabled networks and services. Limitations of Internet era can be overcome by Next generation network protocols and their advanced features and technologies. Research and development on Next Generation Network (NGNs) have been carried out over the last few years. Due to the efficiency and flexibility of IP technology, most new network being established are also IP based. The advent of NGN’s therefore heralds a shift from vertically to horizontally integrated networks, enabling unfettered, consistent and ubiquitous access for both users of these networks and competing service providers. In this article we discusses the major driving forces for network evolution, we outline the fundamental reasons why neither the control infrastructure of the PSTN nor that of the present-day Internet is adequate to support the legion of new services in next-generation networks and overview of its architecture and control and management and its evaluation from fixed and mobile network infrastructure. Its control and management architecture is different from internet and PSTN but NGN inherit heavily from both.**

***Keywords*— Automatic Transfer Mode, Multi protocol Label Switching (MPLS), IP Multimedia Subsystem (IMS),Session Initiation Protocol, Network Attachment Control Functions(NACF) ,Media gateway control(MGC)**

I. INTRODUCTION

Since Internet was born, we have experienced its expansion regarding both the number of users and the number of different services available. As a consequence of this rapid expansion until today, service providers have more and more the needs to speed up the implementation of new network solutions in a effective and efficient way. These newest and innovative network solutions are generally referred to as Next Generation Networks (NGN).

The market for information and communications technology is currently undergoing a structural change. The classic telecommunication networks were planned and implemented for the transfer of specific data such as telephone calls or pure data packages. The recent growth in competition, new requirements for the market and technological developments have fundamentally changed

the traditional attitudes of the telecommunications industry. The present industry is characterized by the rapid growth of broadband connections, the convergence processes of various network technologies and the emergence of a uniform IP standard for individual and mass communications.

The traditionally familiar market boundaries between fixed networks, mobile telephony and data networks are disappearing more and more quickly. This gives the customer the advantage that he can call on an extremely wide range of services, regardless of his access technology. This development requires a meta-infrastructure beyond the existing, subordinated networks – a core network for all the access networks called as Next Generation Network. The Internet Protocol is the most significant integration factor because it is available globally and, at least in principle, it can use almost all the services and applications in all the networks.

An NGN, the result of merging the internet with the telephone network, combines the best features of both. It provides:

- Adaptability for transmitting any type of traffic, which can be compared to the internet's adaptability as opposed to the inefficiency of a PSTN in transmitting data.
- Guaranteed quality of voice telephony services and critical data applications; in this case an NGN offers PSTN reliability as opposed to the best effort of the internet's capacity.
- Low transmission costs per content unit - the price is closer to the internet than to a PSTN, the total amount of data and voice traffic trebles every year.

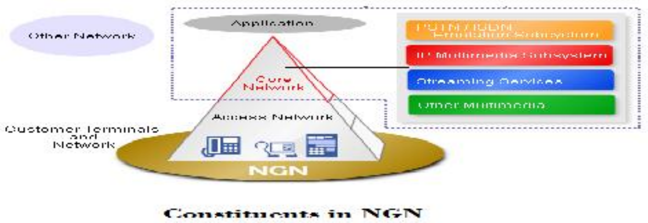


Fig:1

MAJOR DRIVING FORCES OF NGN

Heterogeneity of the Telecommunications Infrastructure

In the traditional network infrastructure, the introduction of new services and applications can be an arduous and expensive process. The process requires high staffing costs. Many functionalities in the network have to be configured manually in order to implement new features. Moreover, the variety of networks and the heterogeneous subscriber end devices make the provision of infrastructure-independent services more difficult. As a result, the services can only be used via specific networks and appropriately adjusted end devices such as fixed network phones, cell phones, televisions, etc.

The growing number of services has led to an increase in the platforms needed to provide them, which in turn has increased the complexity of the overall infrastructure. The problems of interoperability between the various systems are becoming more serious, and this growing complexity is also placing greater demands on staff. Maintaining these platforms involves high annual operating costs for the network operators.

GROWING COMPETITION FROM OTHER SECTORS

Apart from the fixed-network and cell phone operators, companies from other sectors will also establish themselves in future on the convergent market. Portal suppliers with strong brand names and powerful financial backing – including Google, MSN, eBay and Yahoo – are planning to penetrate the voice and infrastructure business. They will also be joined by cable network operators and companies that provide media content, such as Microsoft. This convergence is therefore producing virtually inevitable conflicts and incompatibilities. Technologies and market forces are colliding with each other. The market participants are crowding each other out and defending their positions strongly. In the course of this convergence, the value of the network business will gradually decrease and the service range will make a much larger contribution to end-customer sales. Traditional network operators will have to rethink their business model and also position themselves much more strongly on the upper levels of the value-added chain.

FALLING CALL SALES

The increasing competition due to the liberalization of the markets and the arrival of market participants from other sectors are causing great concern to the operators of former state monopolies. The classic telephone business, known as a Public Switched Telephone Network (PSTN), is particularly unsatisfactory. The golden age of the high-margin business with revenue in the billions based on classical phone calls is clearly over. Figure shows the estimated development of the global number of telephone minutes since 1990 end some predictions for market trends till 2015. In spite of the current fall in fixed-network minutes, a strong growth in the total of telephone minutes is to be expected. Experts see particularly strong potential in the use of the Internet Protocol for phone calls. This so-called Voice over IP (VoIP) is possible with all IP-based networks.

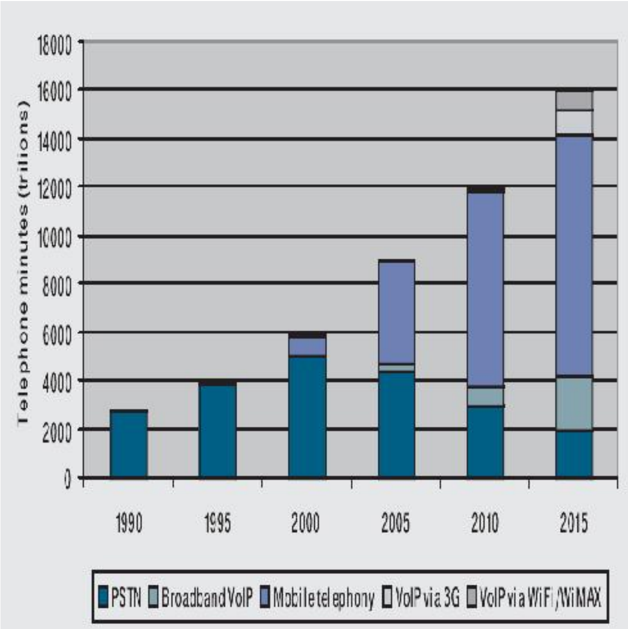


Fig:2

II. ARCHITECTURE

Access Layer(Gateway layer):

It is responsible for direct subscriber function.NGN can support all kind of existing access as well as upcoming access and is capable of processing traffic originated from PSTN, XDSL, Wimax or any other system and depending upon the type of access.Protocol conversion or media conversion may be required at the NGN gateways.

NGN gateways:-

i) Media gateway:- It terminates media, coming from PSTN/PLMN . Here, it is responsible for packetization of media under the instruction of control layer. It performs the task of packetizing voice and providing connections from switched circuits(TDM)to packetized circuits (IP, Frame relay or ATM).It is responsible for media conversion, resource allocation and resource management and event notifications and reports events to Media Gateway Controller within its zone.

ii) Access Gateway:- Allows the connection of subscriber lines to the packet network and Provides subscriber access to NGN network and services
iii) Signalling gateway:- It works as a bridge to PSTN and converts between SS7 address and IP address.

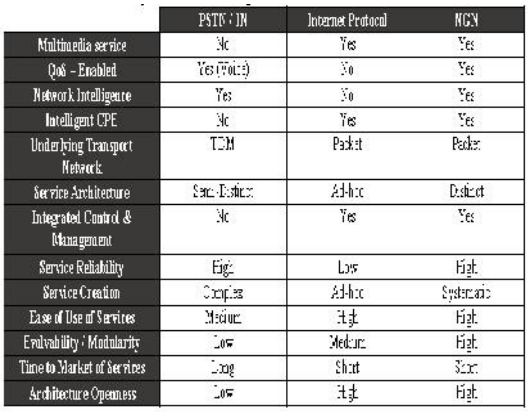
Softswitch/MGC – referred to as the Call Agent or Media Gateway Controller (MGC). It provides the "service delivery control" within the network and in charge of Call Control and handling of Media Gateways control (Access and/or Trunking).It connects to Intelligent Network /applications servers to offer the same services as those available to TDM subscribers

Transport Layer

Transport Layer of NGN is based on IP and forms the core of network. It consists of routers,which are responsible for carrying traffic originated by access layer.It's use is to transfer between nodes of network. It is consisting from one or from multiple high-speed backbone packet switched networks.

It is possible to serve to a flows of different character with different requirements on quality of transfer (delay, data loss,...).

III. COMPARISON BETWEEN NGN AND TRADITIONAL TECHNOLOGIES



	PSTN / IN	Internet Protocol	NGN
Multimedia service	No	Yes	Yes
QoS – Enabled	Yes (Voice)	No	Yes
Network Intelligence	Yes	No	Yes
Intelligent CPE	No	Yes	Yes
Underlying Transport Network	TDM	Packet	Packet
Service Architecture	Semi-Distinct	Ad-hoc	Distinct
Integrated Control & Management	No	Yes	Yes
Service Reliability	High	Low	High
Service Creation	Complex	Ad-hoc	Systematic
Ease of Use of Services	Medium	High	High
Evolvability / Modularity	Low	Medium	High
Time to Market of Services	Long	Short	Short
Architecture Openness	Low	High	High

Fig:3

The potential obstacles to NGN deployment QoS

Service quality will always come first when users think of alternative services. IP is a connectionless packet switching network protocol which was designed for network flexibility but lacks QoS guarantee. In contrast the connection-oriented (whatever physical or virtual circuit) network protocols are better at quality control because of the dedicated communication route. Thus, the connectionless protocols are usually working in conjunction with connection oriented protocols in packet switching networks to achieve higher QoS.

The IP suite cannot meet the QoS requirements, it is why usually the VoIP voice is considered low quality compared to PSTN voice within the current network infrastructure. On the other hand, one of the key improvements expected from an NGN network is the enhanced QoS. Thus, extra mechanisms are definitely needed within the NGN architecture: a virtual circuit switching protocol Multi Protocol Label Switching (MPLS) and its subsequent development Generalized-MPLS (GMPLS, developed for 37 optical networks) are introduced to mitigate the QoS problem by its traffic engineering mechanisms. Through traffic engineering, the packets labeled with higher priority such as VoIP traffic can be transmitted over some faster pathways to achieve higher QoS without extra requirements on existing network bandwidths. However, it is noted that within the NGN infrastructure the achievement of acceptable QoS relies on the combination of various QoS-integrated mechanisms from the edge to the core. Despite the great efforts made during the NGN development, the industry still has doubts on the quality of voice services provided by an all-IP packet-switching network, whether the current widespread VoIP or future NGN voice services. Thus, along with other reasons, QoS issues may prevent the fast deployment of the NGN.

SECURITY CONCERNS

On interface in direction to access networks and to networks of another operators are mediation gateways (MGW) situated, which are adapting and routing data flows between these networks and unified transport network. It's function is coding, decoding and packetization.

As a unified network based on IP technology to integrate and replace the existing PSTN/ISDN and the Internet, besides the strengths, the weaknesses from the current Internet are also inherited by NGN; security issues may not be so important as quality issues especially in NGN optical backbone networks, but for end users it still could be another critical concern. Within the existing network infrastructure, traditional voice networks are well protected by being physically separate from computer networks; usually it is difficult for computer criminals to intrude into local PSTN networks from the Internet unless they can physically access lines, switches or terminals. However, the convergence between PSTN and the Internet provides facilities for cyber crimes as there will be no more differences between voice networks and computer networks in the future. In pace with an initial transition from PSTN/ISDN to the Internet, VoIP, which has been deployed for years as a cheaper alternative to PSIN in particular in long distance communications, the cyber crimes involving VoIP networks are raising. Thus, it is not surprising to see a number of enhanced and complex security mechanisms adopted and integrated in NGN, such as the concept of Security Domain, NGN IMS Authentication, and IPSec. At present it is difficult to judge how secure an NGN is until it goes to practice, but it is certain that security will be a big challenge for NGN implementation in the future.

EMERGENCY CALL HANDLING

Special attention is focused on the emergency call handling within the NGN infrastructure. Historically, at a very early stage of VoIP, the emergency call service was neglected by service providers, as VoIP was considered as the complement only to PSTN at that time, but later when VoIP was widely deployed, many governments regulated the emergency call service as mandatory in VoIP services.

IV. CONCLUSIONS

As we draw our conclusion, demands of users and market need are the main factors which introduce Next Generation Networks. This paper represents an overview of NGN and how we can differentiate NGN from pre-NGN networks based on its architecture and working. We can see NGN provides completely ip packet based, multimedia open service network and guaranteed QOS. Standardization and research activities on NGN and its management have been taking place quite actively in the past several years but much more work is needed before NGN can be fully realized. Although there are so many challenges in deployment however, we require NGN to fulfill today’s generation’s demands and requirement of advanced networking as it provides:

- Mobility of a cellular networks round the globe

- Concept richness of internet and packet based data transmission
- Bandwidth of optical networks
- Security of private networks
- Flexibility of Ethernet
- Video delivery of cable and television

REFERENCES

[1] Next Generation Networks – NGN :ITU NGN standards and architectures; http://www.itu.int/en/

[2]Strategies for the deployment of NGN and NGA in a broadband environment – regulatory and economic aspects;

http://www.itu.int/ITU-D/finance/Studies/NGN%20deployment%20strategies-en.pdf

[3]Directorate general for internal policies.A: economic and scientific policy ; http://www.europarl.europa.eu/

[4]Reference Specification for Next Generation Networks (NGN) Technical Framework; www.hit.bme.hu_~jakab_edu_litr_NGN_Architecture_IDARSNGNTechFrw

[5]Alleman A.-Rappoport P.-Final:The Future of Communications in Next Generation Network; http://www.itu.int/osg/spu/ni/voice/papers/FoV-Alleman-Rappoport-Final.pdf

[6]NGN Network Architecture :ITU/BDT Regional Seminar on Costs and Tariffs for Member Countries of the Tariff Group for Africa (TAF) Midrand, South Africa, June 2005;

www.itu.int_ITU-D_finance_work-cost-tariffs_events_tariff-seminars_south-africa-05_presentation-3-soto-en

[7] Standardization Trends in ITU-T NGN UNI and NNI Signaling;

https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr200902gls.html

Optimization of Facility Layout Problem of an Automotive company using Simulated Annealing: a Case Study

Bhoopsingh[1] ,Bhupender Singh[2]

[1] *Department of Mechanical Engineering., Ganga Institute of Technology and Management, Kablana, Jhajjar, Haryana, INDIA*
[2]*Department of Mechanical Engineering.,YMCAUST ,Faridabad, Haryana, INDIA*

Abstract--In this paper a solution to the facility layout problem is presented. It is based on Simulated Annealing (SA), a recent and meta-heuristic approach to solve NP hard combinatorial optimization problems (like FLP).Increased competition globally in manufacturing industries and increases their focus towards the reducing manufacturing cost so an efficient facility layout required. Facility layout directly affects the productivity of industries as a result, there are need for various procedure and method for solving the facility layout problems. In manufacturing industries, the material handling cost function includes the transporting work in process, finished parts, tool and raw material between the facilities, the distance travelled by personnel or material handling between the facilities to be minimized. Simulated annealing (SA), a meta-heuristic technique is employed to solve a facility layout problem modeled as Quadratic Assignment Problem (QAP). In this paper work problem is taken from an automotive industry. The main objective is to find the best possible arrangement of all the facilities on the layout so as to minimize the total material handling cost of the company while satisfying all the constraints and keeping material flow smooth.

***Keywords*: Simulated annealing (SA); Facility layout problem (FLP); Optimization.**

I. INTRODUCTION

Facility layout problem is concern with is to find an optimal relative location of facilities on planar site (kouvelis et al.), in general terms smooth way to access the facilities. As defined in the literature the main objective of the facility layout problem is to minimize the total material handling cost (MHC). It estimated that 20-50% of operating cost in manufacturing industries are related to material handling and layout planning (Tompkins et al.). The main concern with the plant facility layout planning is to reduce the cost of materials handling as poor materials handling can generate business problems. To stay competitive in today's market a company must reduce costs by planning for the future. Material handling cost is an indirect cost and every company wants to reduce this indirect cost and it constitutes a major part of indirect costs in a facility. Therefore even small improvements in material handling costs makes a large reduction in total indirect costs. The cost of material flow is a function of the distance the material is moved between divisions called departments in a manufacturing facility.

II. LITERATURE REVIEW

The aim of the literature review is to expose the various aspects and dimensions over which facility layout problems are disseminated. We carried out the literature review to know that how facility layout (design) problems are formulated and what are the various solution approaches. As we are using simulated Annealing (SA) technique for solution of our problem so review is also carried out to know about the simulated Annealing (SA) algorithm, its application over facility layout problems and the efficacy of this method compared to other meta-heuristics in finding out an optimum solution.

- Matai et al. (2013), this paper, they presents a modified simulated annealing (SA) based approach to solve multi objective facility layout problem. It can incorporate more than two objectives that may be qualitative or quantitative in nature. Computational results show superiority of the proposed modified SA based approach for multi objective facility layout problem over past approaches available in literature.
- Matai et al. (2012), In this paper, they presented modified simulated annealing approach to solve the multi objective facility layout problem. It can incorporate more than two objectives which can be quantitative or qualitative in nature. Computation result for proposed simulated annealing approach show the better result to solve the multi objective facility layout problem.
- Lin lin And Chen fei (2012), this paper explained the basic principle of simulated annealing (SA) algorithm which was applied to solve the function optimization problem and algorithm realization process by using MATLAB. Through the improvement algorithm results show that the method is able to function for global optimization effectively. Improved simulated annealing (SA) algorithm not only can deepen the understanding of simulated annealing (SA) but also can achieve the purpose of design intelligent system.
- Matai et al. (2010), In this paper, they classified all the facility layout (design) problems on the basis of various factors affecting the layout. Various solution approaches are described for solving the FLP’s and are compared on the basis of their efficacy to find the best possible solution and time taken to finish the iterations to do this..
- McKendall and Shang (2006), This paper gave the procedure to deal with the solution of dynamic facility layout (design) problems (DFLP) using two different approaches of Simulated Annealing (SA). First approach considers the direct application of Simulated Annealing (SA) meta-heuristic for solving dynamic facility layout problem (DFLP). The second one is the improved one of the first approach. The whole procedure remains same with addition of look-ahead and look-back strategy. This data is taken from the

literature for the experiment work to check the performance of these two approaches. The interpreted results show that multi dynamic facility layout problem (DFLP) can be dealt effectively by the proposed heuristics.

- Chwif et al. (1998), this paper gave the simulated Annealing (SA) algorithm for solution of facility layout (design) problem in a continual plane using simulated annealing (SA). And also present simulated annealing for general facility layout problem considering facilities area, shapes, orientation or in machine layout considering machine pick up and drop off point. They also discussed on problem formulation, formulation of objective function and proposed a simulated annealing (SA) algorithm based on Monte Carlo simulation allowing to solve the combinatorial optimization of facility layout problem (FLP) having different shape and size fixed facilities. The main problem faced by proposed Simulated annealing (SA) based algorithm to avoid overlapping with occupied space ratio above 75%. Although SA based algorithm is reasonable computationally and it shows good results.
- Connolly (1997), This paper discussed on the use of simulated annealing (SA) applied to the quadratic assignment problem (i.e. the assignment of inter-communicating objects to locations to minimize the total material handling cost between facilities). The result is a much-improved annealing scheme for this problem which performs well on a range of examples, finding improved solutions for several of the largest problems available in the literature and requiring only modest amounts of computational effort.

III. IDENTIFICATION & FORMULATION OF FACILITY LAYOUT PROBLEM

Facility layout problem (FLP) is a well-known problem and the finding location of facilities is a general problem encountered in manufacturing, service sector and many others. Formulation of FLP is done as Quadratic assignment problem (QAP) and QAP is NP-hard type which needs so much computation time even for a small size problem. Computational requirement grows exponentially as the size (number of facilities) of the problem increases.

Traditionally the facility layout problem modelled as Quadratic Assignment Problem (QAP) was proposed by Koopmans and Beckaman for the first time. The QAP has applied to wide range of application such as urban planning, control panel layout, facility layout design etc. The QAP is a special case of facility layout problem that all facility have equal areas and that all location. The name was so given because the objective function is a second degree function of variables and constraints are linear function of variables.

A. Problem Identification

Due to improper facility layout of the ABC Pvt. Ltd. company is facing the problem of high material handling cost, complex flow of materials. Due to improper arrangement of facilities the material has to travel unnecessary distance from starting to finish with in the plant. This increases the material handling cost. It also complicates the material flows. Facilities are not arranged in close affinity according to the process flows of the parts. Company has 9 no. of facilities from raw material to dispatch of finished parts. Facilities are located in such a way in plant so as to increases the center to center distance between facilities having material flow. Due to unnecessary distance travelled makes total material handling cost high and hence final cost of product. After consulting design and development head some of objectives given are to design a proper facility layout design which makes the flow of material smooth within plant. The following figure 3.1 and 3.2 represents the current layout of the company and current material flow in the plant.

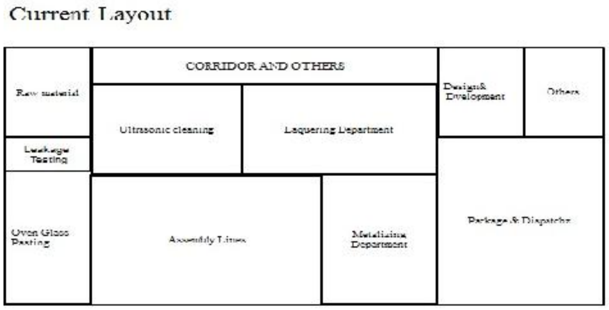


Fig. 1 Current layout

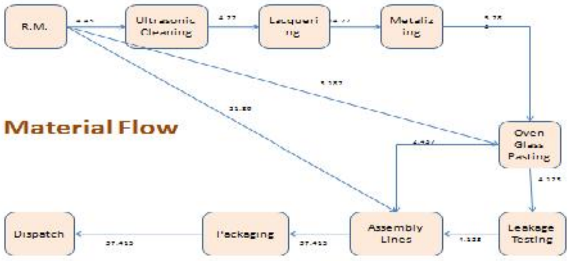


Fig. 2 Material flow diagram between various facilities

TABLE 1

CENTROIDS OF VARIOUS FACILITIES IN EXISTING LAYOUT

Sr. No.	**Name of facility**	**Co ordinate X**	**Co ordinate Y**
1	Raw Material	2.25	14.1
2	Ultrasonic cleaning	8.4	11.7
3	Lacquering department	15.3	11.7
4	Metalizing department	19.5	4.35
5	Oven glass for pasting	2.25	4.45
6	Ultrasonic welding & leakage test	2.25	10
7	Assembly department	10.5	4.35
8	Packing & dispatch	27	6

9	Design & development deptt.	20.55	15

B. *Assumptions*

To develop the mathematical model and to solve the facility layout problem some assumptions are taken as:

- All facilities are square or rectangular in shape with flexible dimensions and we assume all the facilities as square taking aspect ratio of length to width equal to one for using in Simulated Annealing (SA).
- The rectilinear distance between two facilities is calculated with respect to their centers.
- Only one location is assigned to a facility and only single facility can be assigned to a particular location.
- There should be no overlapping between the facilities.
- Flow data between all facilities is known.
- Each facility area remains unchanged.
- Aspect ratio value for all facility is known.
- Problem is formulated as single objective and single period problem facility layout problem.

C. *Mathematical Modeling of the Facility Layout Problem*

Facility layout problem mathematical modeled as:

- Problem formulation i.e. objective function that we have to optimize.
- Geometric constraints which need to satisfy
- Decision variable which need to determine.
- Solving Facility layout problem using Simulated Annealing (SA) with MATLAB coding.

The definition of decision variables is first important part towards the development of the mathematical model. Once the variable defined the construction of objective function and constraints is an easy task.

D. *Center to Center Distance between Facilities*

Here we have calculated the travel distance using rectilinear distance method. The formula used for this is given below

$D_{ij} = | x_i - x_j | + | y_i – y_j |$

TABLE 2

DISTANCE MATRIX

	Facilities *(i-j)*	**Centroidal Distance between facilities (m)**
1	1-2	8.55
2	1-5	9.65
3	1-7	18
4	2-3	6.9
5	3-4	11.55
6	4-5	17.35
7	5-6	5.55
8	5-7	8.35
9	6-7	13.9
10	7-8	18.15

TABLE 3

WEIGHT FLOW PER MONTH IN TONE AND DISTANCE BETWEEN FACILITIES

Facilities *(i-j)*	**Weight of Material Flow/month (tonne)**	**Centroidal Distance between facilities (m)**
1-2	4.43	8.55
1-5	3.187	9.65
1-7	21.89	18
2-3	4.27	6.9
3-4	4.27	11.55
4-5	5.783	17.35
5-6	4.123	5.55
5-7	2.437	8.35
6-7	4.123	13.9
7-8	37.415	18.15

TABLE 4

ASPECT RATIOS (MIN AND MAX) FOR EACH FACILITY

Facility No.	**Min Aspect Ratio (a_{il})**	**Max Aspect Ratio(a_{iu})**
1	0.1	6.5
2	0.15	7.5
3	0.3	2.6
4	0.5	1.8
5	0.5	1
6	0.15	2.5
7	0.3	1.8
8	0.5	1.5
9	0.5	1

E. *Objective function and constraints*

1) *Objective Function:*

$$\min Z = \sum_{i=1}^{m}\sum_{j=1}^{m} F_{ij}.D_{ij}.C_{ij}$$

Where

m **= 9** = no. of facilities between which material moves or flow takes place

F_{ij} = Weight(volume) of flow between facilities i and j, measured as moves/frequency/weight per unit time and per unit distance or may be volume or weight of flow per unit time and per unit distance.

D_{ij} = Rectilinear distance of material flow between facilities i and j in meters.

C_{ij} = Rs. 25.89/tonne/m = cost/move among activities i and j per unit distance or we can say unit material handling cost

2) *Constraints:*

$D_{ij} = | x_i - x_j | + | y_i – y_j |$

Overlap Check

$(l_i + l_j)/2 - | x_i - x_j | \leq 0$

or

$(b_i + b_j)/2 - | y_i – y_j | \leq 0$

(l = b as facilities are taken as square)

$l_i , l_j , x_i , x_j , b_i , b_j , y_i , y_j \geq 0$

i = 1, 2, 3 ………….. n

j = 1, 2, 3 ………….. n

$i \neq j$

F. *Minimum Safe Distance between Facilities to avoid Overlapping*

Second and third constraints are introduced to avoid overlapping of facilities. One is to avoid interference along x-axis and another along y-axis. Figure 5.4 shows the minimum distance calculation to avoid interference.

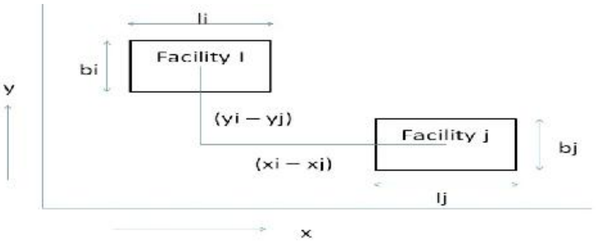


Fig. 3 the minimum distance calculation to avoid interference

IV. SIMULATED ANNEALING (SA) FOR FLP

A. Simulated Annealing

SA is a stochastic approach for solving combinatorial optimization problems, in which the basic idea comes from the annealing process of solids. In this process, a solid is heated until it melts, and then the temperature of the solid is slowly decreased (according to an annealing schedule) until the solid reaches the lowest energy state or the ground state. If the initial temperature is not high enough or if the temperature is decreased rapidly, the solid at the ground state will have many defects or imperfections. (Kirkpatrick et al.) were the first to use simulated annealing(SA) to solve a combinatorial optimization problem.

Before the development of meta-heuristics such as SA, tabu search, and genetic algorithms, many local search techniques (e.g., add/drop and exchange heuristics) were used to solve large combinatorial optimization problems. These heuristics, more specifically, the random descent pair-wise exchange heuristic, starts with an initial solution and move to r generate a neighboring solution (i.e., a solution slightly different from the initial solution) randomly. The cost of the neighboring solution is obtained and compared to the cost of the initial solution. If the cost of the neighboring solution is better (less than the cost of the initial solution), this solution becomes the best solution, and it is used as the starting solution at the next iteration. Otherwise, the initial solution is used as the starting solution at the next iteration. This process continues until a stopping criterion is reached. Often times this type of heuristic performs poorly (i.e., converges to a poor local optimum). To overcome this drawback, one technique that was considered was to apply the local search technique with multiple initial solutions. Although the probability of obtaining better local optimum increased, this technique was computationally costly but performed only slightly better. However, strategies, which use a local search technique that allowed accepting non-improving neighboring solutions, were considered and performed well. This is the idea behind the SA heuristic and other meta-heuristics. In other words, the idea of annealing is used to accept non-improving moves (or neighboring solutions) to avoid getting trapped at a poor local optimum. In SA, the probability of accepting non-improving moves initially is high, but as the search proceeds (and the temperature is reduced), the probability of accepting non-improving moves reduces.

B. Parameters:

The most important parameters of the simulated annealing (SA) Meta heuristic are the probability of acceptance and the annealing schedule.

C. Annealing Schedule:

The annealing schedule, also called the cooling schedule is the parameter settings for the SA heuristic, which is used to reduce the current temperature.

1) *Temperature function:* The current temperature is determined by the following equation:

$$T_c = T_0 \alpha^{r-1}, \quad r = 1, 2, \ldots, R,$$

Where T_0 is the initial temperature, α is called the cooling ratio and is usually set at 0.90, and R − 1 is the number of temperature reductions.

2) *Epoch length:* Before reducing the temperature, a number of accepted pair-wise exchanges need to be performed in order to ensure that the system is at a steady state. However, when the temperature is low, a large number of attempted pair-wise exchanges may be performed, since only a few pair-wise exchanges may be accepted. Therefore, the temperature should be reduced after a certain number of attempted exchanges (A) known as epoch length.

D. Probability of Acceptance

The probability of acceptance is defined as the probability of accepting a non-improving solution as the current solution. This is determined based on the following probability:

$$P(\Delta TC) = \exp(-\Delta TC / T_c),$$

Where T_c is the current temperature and ΔTC represents the change in total cost (i.e., the cost of the neighboring solution minus the cost of the current solution).

$\Delta TC = f(y') - f(y)$

If x is a randomly generated number between 0 and 1, and

$x < P(\Delta TC)$,

Then accept the non-improving neighboring solution y ' as the current solution (i.e., set y = y '). Otherwise reject the non-improving solution, and keep the current solution y. Initially, the probability of accepting a non-improving solution is higher, and this should be considered when determining the initial temperature. However, as the temperature is reduced, the probability of

.Simulated Annealing (SA) Algorithm

A straightforward simulated annealing Meta heuristic for the facility layout is given below.

Step 1: Input Data

The flow matrix.

Distance matrix. and

Unit material handling costs between each pair of facilities are given as input data.

Step 2: Define the SA parameters:

T_0 is the initial temperature, α is the cooling ratio, A the attempted number of moves at each temperature and T_{min} the minimum allowable temperature.

Step 3: Initialize the temperature change counter: r = 1.

Step 4: (a) Generate an initial solution y_0 and assign it to the current solution (i.e., set $y = y_0$).

(b) Obtain the cost of the current solution, f (y).

(c) Set the following parameters: Best-sol = y and Best-cost = f (y).

Step 5: Initialize counter for the number of attempted moves at each temperature: i = 0, and set the current temperature according to the annealing schedule, $T_c = T_0 \alpha^{r-1}$. If $T_c < T_{min}$, then explore the entire neighborhood of the Best-sol (i.e., use the steepest-descent pair-wise exchange heuristic), and return Best-sol and Best-cost.

Step 6: (a) Perform an iteration of the random descent pair-wise exchange heuristic. In other words, randomly select a period t, and then randomly select two departments' u and v in period t. Exchange the locations of departments' u and v in period t, and denote the neighboring solution as y '. Also, update i = i + 1.

(b) Calculate the change in total cost, $\Delta TC = f(y') - f(y)$.

Step 7: If ($\Delta TC < 0$) accept this solution

Or

If $\Delta TC > 0$ Then

and $x = \text{random}(0, 1) < P(\Delta TC) = \exp(-\Delta TC/Tc)$

Then set y = y ' and if Best-cost>f(y), then Best-cost = f (y) and Best-sol = y.

Step 8: If i = A, then update r = r + 1, and go to Step 3. Else, go to Step 4.

Initially, the heuristic parameters α, A, and T_{min} are defined and obtained experimentally. In other words, α and A were obtained using experimental techniques and T_{min} is set to value 0.01 (i.e., $T_{min} = 0.01$).

Furthermore the initial temperature is determined such that the probability of accepting a neighboring solution with a cost of 10% above the cost of the initial solution is 0.25, which gives the equation

$$T_0 = -\Delta TC / \ln(P(\Delta TC)) = -0.10\, f(y_0) / \ln(0.25)$$

Since $P(\Delta TC) = \exp(-\Delta TC / T_c)$ and $T_c = T_0$ for r =1.

In Step 2, $y_0 = [ax_0(1), ax_0(2) \ldots ax_0(T)]$, is generated and is assigned to the current solution or layout plan, y. The n-component vector $ax_0(t)$ in the initial solution vector represents the initial layout for period t, where t = 1, 2 . . . T. Also, $ax_0(t) = [x_0(1), x_0(2) \ldots x_0(N)]$ such that the element $x_0(i)$ in the initial assignment vector represents the location of department i, where i =1, 2 . . . N.

In Steps 2 and 3, the heuristic parameters and counters are initialized. Also, if the stopping criterion as been reached (i.e., $Tc < Tmin = 0.01$), in Step 3, the heuristic is terminated after the entire neighborhood of the Best-sol is explored, and the best solution obtained is given. Otherwise in Step 4, the random descent pair-wise exchange heuristic is used to obtain a neighboring solution y ', and the change in total cost ΔTC is obtained. Also, the counter used to count the number of attempted pair-wise exchanges at the current temperature is updated. In Step 5, if $\Delta TC < 0$, then the neighboring solution y ' is accepted as the current solution y since f (y ')< f(y). Also, the Best-cost and Best-sol is updated if necessary. If $\Delta TC > 0$ (i.e., f (y ') > f(y)) and $x < P(\Delta TC)$, where x is a randomly generated number between 0 and 1, then y ' is accepted as the current solution (i.e., set y = y ') although y ' is worse than y. Otherwise, the current solution y does not change. In Step 6, for the current temperature, the number of attempted pair-wise exchanges is compared to A.

If less than, then the local search technique is implemented, in Step 4, and continues from there. Otherwise, the temperature is increased in Step 3. This process is repeated until the current temperature T_c drops below 0.01 (i.e., $T_c < T_{min} = 0.01$).

E. Flow chart of Simulated Annealing (SA) for FLP

The flow chart of the SA for facility layout problem is shown in the figure

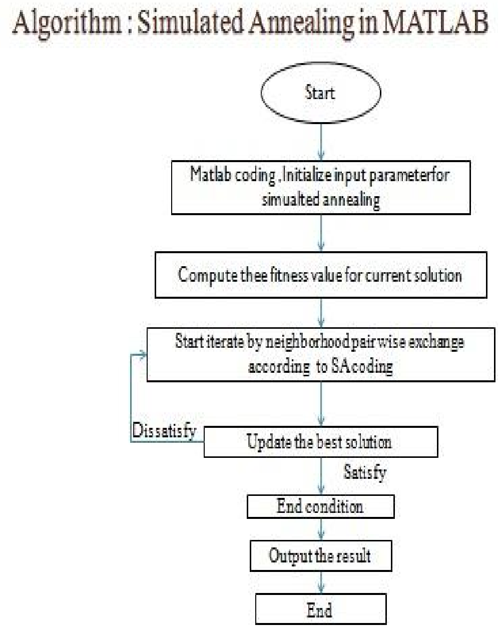

Algorithm : Simulated Annealing in MATLAB
Start
Matlab coding ,Initialize input parameterfor simualted annealing
Compute thee fitness value for current solution
Start iterate by neighborhood pair wise exchange according to SA coding
Dissatisfy
Update the best solution
Satisfy
End condition
Output the result
End

Fig 4. SA algorithm

V. RESULTS AND DISCUSSION

SA results

A. *Optimization through Simulated annealing (SA)*

The mathematical model for facility layout problem is to minimize the total distance between various facilties. We optimize the model with help of simulated annealing algorithm A programming code for Simulated annealing algorithm was written in MATLAB software. The latest version of MATLAB used for programming is R2010a.

Initial Temperature for SA T_o =1 Cooling ratio =.95 T_{min}=0.01

Input parameter

1. Distance matrix (D_{ij})

2. Flow matrix (F_{ij})

3. Unit material handling cost (C_{ij})

MATLAB version used for programming is R2010a.

shows the original co ordinates and optimized co ordinate obtained by the algorithm..

TABLE 5

COMPARISON OF ORIGINAL AND OPTIMIZED CO ORDINATES

Facility No.	**Original Coordinates**	**Optimized Coordinates**
1	2.25,14.10	13.4,12.9
2	8.4,11.70	13.4,18.65
3	15.3,4.35	20.45,20.2
4	19.5,4.35	6.65,20.2
5	2.25,4.45	7.1,13.45
6	2.25,10.00	6.75,5.2
7	10.5,4.35	13.4,5.2
8	27.0,6.0	23.7,5.2
9	20.55,15.0	2.6,5.2

By running simulated annealing (SA) MATLAB program, we get the centroids of each facility of the layout in the result. By using these centroids we can draw the optimized layout. Optimized layout obtained is shown in the fig

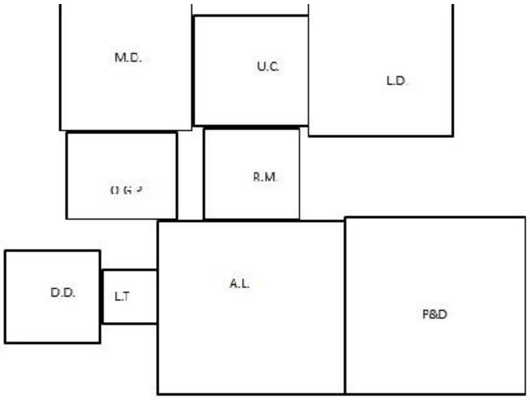


Fig 5. optimized layout

B. *Proposed Layout*

The optimized facility layout obtained by running simulated annealing (SA) MATLAB program is adjusted according to the aspect ratios of various facility within layout and new modified layout is prepared. Table 6.2 shows the existing and optimized co ordinates after adjustment.. Table 1.4 shows the existing coordinates and optimized coordinates after adjustment.

TABLE 6.

COMPARISON OF ORIGINAL AND PROPOSED CO ORDINATES

Facility No.	**Original Coordinates**	**Optimized Coordinates**
1	2.25,14.10	12.675,9.034
2	8.4,11.70	14.25,11.284
3	15.3,4.35	15.1,15.25
4	19.5,4.35	4.75,15.25
5	2.25,4.45	3.075,9.25
6	2.25,10.00	5.325,3
7	10.5,4.35	13.635,4
8	27.0,6.0	25.57,4.24
9	20.55,15.0	2.25,3

After modification the shapes of the facilities change and hence the coordinates, which alter the distance between the facilities. The figure 5.2 shows the proposed layout.

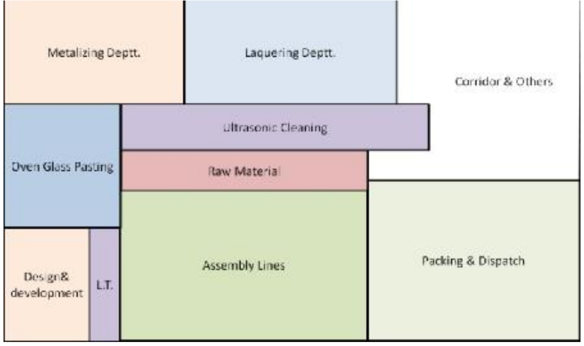


Fig. 6 proposed layout

C. *Distance optimization*

After the reshaping the facilities new dimensions and centroids are available. Now we can calculate the facility to facility distance. The main aim of minimizing the material handling cost depends on minimizing the distance between the facilities having material flows between them. The distance matrix obtained from the algorithm differs from the modified solution, because the reshaping changes the inter facility distance. We compare the distance matrix obtained from modified solution with the existing one. The table 1.5 shows the earlier (existing) & proposed (optimized) facility to facility distance values (in meters) for all the facility pairs between which the material flow takes place.

TABLE 7

COMPARISON OF ORIGINAL AND OPTIMIZED DISTANCE

Facilities *(i-j)*	**Existing distance** (m)	**Optimized distance** (m)
1-2	8.55	3.825
1-5	9.65	9.816
1-7	18	5.994
2-3	6.9	4.816
3-4	11.55	10.35
4-5	17.35	7.675
5-6	5.55	8.5
5-7	8.35	15.81
6-7	13.9	9.31
7-8	18.15	12.175
TOTAL	117.95	88.271

Figure 7 shows the statistical comparison between the existing (old) and proposed (optimized) distances between various facilities.

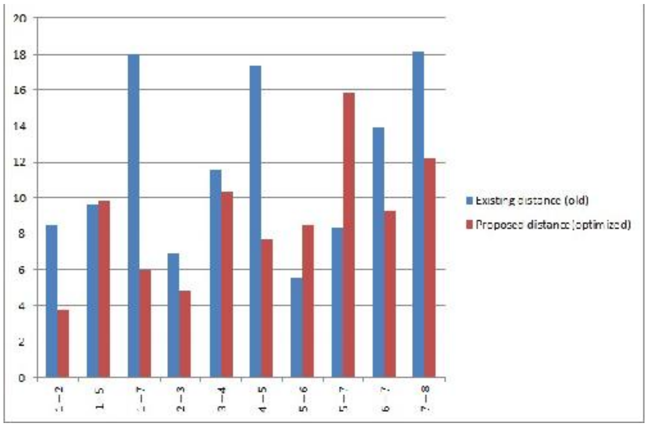


Fig. 7 Statistical comparisons of the existing and the proposed (optimized) distances

The red blocks represents the proposed (optimized) facility to facility distance value and blue blocks represents the existing (old) facility to facility distance value. Summing up all proposed distances we get total 88.271meters. So total 29.679 (117.95-88.271) meters. These proposed distances contribute towards the minimization of material handling cost (MHC).

VI. CONCLUSIONS

This paper conclude that Facility layout directly affects the productivity of the firm, so it is very important solve it carefully. Facility layout problem can be defined as optimization problem and a mathematical model way to solve. The main objective of facility layout problem is to minimize the total material handling cost by minimizing the total distance travel by material within firm.

The problem taken from an automotive industry is solved using simulated annealing (SA) algorithm by coding in MATLAB software. MATLAB program is run for simulated annealing algorithm by defining input parameters. Solution obtained by running program is obtained in the form of centroids of square as we modelled our problem by taking square facilities. The solution obtained is readjusted using aspect ratios.

REFERENCES

[1] Matai R. et al., “Modified simulated annealing based approach for multi objective facility layout problem”, International journal of production research, vol.51, issue no.51, pages 4273-4288, 2013.

[2] Sharma P. et al., “A review of meta heuristic approaches to solve facility layout problem”, International journal of emerging research in management and technology, vol.2, issue no.10, 2013.

[3] Matai et al., “A new heuristic approach to solve the facility layout problem”, International journal of advanced operations management, vol.5, pages.137-158, 2013.

[4] Reddy S.N. et al.. “Optimization of multi objective facility layout using non traditional optimization technique”. International journal of engineering science and technology, vol.4 Issue no.2, 2012.

[5] Matai et al., “Solving multi objective facility problem: modified simulated annealing approach”, European journal of management, vol.12, issue no.2, 2012.

[6] Kundu A. and Dan P.K., “Met heuristic in facility layout problems: current trend and future direction” Int. J. Industrial and Systems Engineering, Vol. 10, No. 2, 2012.

[7] Lin Lin and Fei Chen, "The simulated annealing algorithm implemented by the MATLAB", International journal of computer science, vol.9, issue no.6, 2012.

[8] Matai R. et al., "Facility layout problem: A state of the art review", XIMB journal of management, vol. 7, issue no. 2, pages 81-106, 2010.

[9] Keivani A. et al., "A simulated annealing for multi floor facility layout problem", Proceedings of the World Congress on Engineering and Computer Science, vol.2 , October 20-22, 2010.

[10] Dirira A. et al.. "Facility layout problem: A Survey", Annual review in control 31, www.elsevier.com pages 255-267, 2007.

[11] Singh S.P. and Sharma R.R.K., "A review of different approaches to facility layout problem", Int. journal of advance manufacturing technology, vol.30, pages.425-433, 2006.

[12] McKendall AR and Shang J., "Simulated annealing heuristics for the dynamic facility layout problem", Computers & Operations. Research, vol. 33, pages 2431-2444, 2006.

[13] Suman B. and Kumar P., "A survey of simulated annealing as a tool for single and multi objective optimization", Journal of operation research society vol.57, pages. 1143-1160, 2006.

[14] Chwif L. et al., "A solution to the facility layout problem using simulated annealing," Computers in Industry, vol. 36, pages 125-132, 1998.

[15] Meller R.D. and Bozer, Y.A., "A new simulated annealing algorithm for facility layout problem", International journal of production research, vol.34, issue no.6, pages.1675-1692, 1996.

[16] Tain Peng. et al., "Simulated annealing for the quadratic assignment problem : a further study", in proceedings of 18th International conference on computers and industrial engineering, vol.31, pages. 925-928, issue 3-4, December 1996.

[17] Heragu S.S., "Recent model and technique for solving the layout problem", European journal of operational research, vol.57, pages. 136-144, 1992.

[18] Heragu S.S. and Alfa A.S., "Experimental analysis of simulated annealing based algorithms for the layout problem", European journal of operational research, vol.57, pages.190-202, 1992.

[19] Connolly D.T., " An improved annealing scheme for the QAP", European journal of operation research,vol.46, issue no.1, pages 93-100, 1990.

[20] Kusiak A. and Heragu S.S., "The facility layout problem", European journal of operational research,vol.29, pages. 229-251, 1987.

[21] Wilhelm M.R. and Ward T.L., "Solving quadratic assignment problems by simulated annealing", IIE Transactions, vol.19(1), pages. 107-119, 1987.

[22] Arikaran P et al., "Analysis of Unequal Areas Facility Layout Problems", International Journal of Engineering (IJE), vol.4, issue no.1, pages 44-51, 2010.

[23] Azadivar F. and Wang J., "Facility layout optimization using simulation and genetic algorithms", International journal of production research, vpl.38, issue no.17, pages. 4369-4383, 2000.

[24] Alvarenga A.G.D. et al., "Meta hueristic method for class of the facility layout problem", Journal of intelligent manufacturing-11, pages.421-430, 2000.

[25] Tompkins J.A. et al., "Facilities planning", 3rd edition, Wiley, New York, 2003.

[26] Kirpatrick S. et al., "Optimization by simulated annealing", Science 220, pages.671-680, 1983.

[27] Kouvelis P. et al., "Simulated annealing for machine layout problems in the presence of zoning constraints", European journal of operational research, vol.52 (2), pages. 203-223, 1992.

[28] Suresh G. and Sahu S., " Multiobjective facility layout using simulated annealing", Internation journal of production economics, vol.32, issue no. 3, pages. 239-254, 1993.

[29] Heragu S.S. and Alfa A.S., "A simulated annealing based approach to solve the facility layout problem", in proceedings of the Fourth Advanced Technology Conference, Washington DC, Pages.489-499, 1990.

[30] Heragu S.S. and Kusiak A.S., " Efficient models for the facility layout problem", European journal of operational research, vol.53, pages. 1-13, 1991.

[31] Koopmans T.C. and Beckmann M., "Assignment problems and the location of economic activities", Econometrica, vol.25, pages. 53-76, 1957.

Optimization of Tie-Line Power In Automatic Generation Control Of Interconnected Thermal-Hydro Power System Using (BFO+PSO)

Ashish Chouhan[1], Ram Avtar Jaswal[2]

[1,2]*Department of Electrical Engineering, UIET, Kurukshetra University Kurukshetra INDIA*

***Abstract*:- A maiden attempt is made to examine and highlight the effective application of bacteria foraging particle swarm optimization (BFO+PSO) to optimize the tie-line power variation in automatic generation control of interconnected two area thermal-hydro power system. The variation in a tie-line power can be reduced to a nominal value or zero value by using application of bacteria foraging particle swarm optimization (BFO+PSO). It is a combination of bacteria foraging optimization and particle swarm optimization to settle down the variation in tie-line power to nominal value in reduced settling time as compared to bacteria foraging and particle swarm optimization. Bacteria foraging particle swarm optimization (BFO+PSO) not only give much reduced settling time but also give best dynamic response.**

Keywords:- Automatic generation control (AGC), Bacteria foraging particle swarm optimization (BFO+PSO) algorithm, Sensitivity analysis.

I. INTRODUCTION

In actual power system operations, the load is changing continuously and randomly. As a result the real and reactive power demands on the power system are never steady, but continuously vary with the rising or falling trend. The real and reactive power generations must change accordingly to match the load perturbations. Automatic generation control is essential for successful operation of power systems, especially interconnected power systems. Without it the frequency of power supply may not be able to be controlled within the required limit band. To accomplish this, it becomes necessary to automatically regulate the operations of main steam valves in accordance with a suitable control strategy, which in turn controls the real power output of electric generators. Thus the main objective of the power system is to maintain continuous supply of power with an acceptable quality, to all the consumers in the system. In case of an interconnected power system having two or more areas connected through tie lines, each area supplies its control area and tie lines allow electric power to flow among the areas. However, a load perturbation in any of the areas affects output frequencies of all the areas as well as the power flow on tie lines. Hence the control system of each area needs information about transient situation in all the other areas to restore the nominal values of area frequencies and tie line powers. The information about each area is found in its output frequency and the information about other areas is in the deviation of tie line powers. For example, for a two area interconnected power system, this information is taken as

$$B_i \delta f_i + \delta P_{tie} \quad (i = 1,2,\ldots S) \quad \ldots\ldots(1)$$

Where, B = tie line frequency bias, f = nominal frequency, Ptie = tie line power

Equation1.Refers the area control error (ACE) and the same is fed as input to the integral controller of corresponding area. Thus an AGC scheme for an interconnected power system basically incorporates suitable control system, which can bring the area frequencies and tie line powers back to nominal or very close to nominal values effectively after the load perturbations. A lot of literature is available on load frequency control of isolated and interconnected electrical power systems using various classical and intelligence technique like pi, pid, fuzzy, neural network, genetic algorithm, particle swarm optimization, bacteria foraging optimization etc. For any optimization technique both the convergence and optimal value achieved are important. When we apply a hybrid combination of both bacteria foraging optimization and particle swarm optimization to interconnected thermal-hydro power system then it give not only more reduced settling time to settle power variation in tie-line power to a nominal value but also give best dynamic response as compared to BFO and PSO technique alone.

II. BACTERIA FORAGING OPTIMIZATION

This technique is based upon the foraging behavior of e.coli bacteria. In this technique four main step are done which are chemotactic, swarming, reproduction and elimination & dispersal step.

A. Bacteria foraging algorithm:-

Step 1 Initialization

1. Number of parameters (p) to be optimized;
2. Number of bacteria (S) to be used for searching the total region;
3. Swimming length (Ns) after which tumbling of bacteria will be undertaking in a chemotactic;
4. Nc is the number of iterations to be undertaken in a chemo tactic loop (Nc > Ns)
5. Nre is the maximum number of reproduction to be undertaken;
6. Ned is the maximum number of elimination and dispersal events to be imposed over the bacteria;
7. P_{ed} the probability with which the elimination and dispersal will continue.
8. The location of each bacterium P(1-p,1-S,1) which is specified by random numbers on [1, 1];
9. The value of C(i) which is assumed to be constant in our case for all of the bacteria.

Step 2 Iterative Algorithms for Optimization

This section models the bacterial population chemo taxis, swarming, reproduction, elimination, and dispersal (initially, j=k=el=0). For the algorithm updating θ^i automatically result in updating of "P".

1. Elimination-dispersal loop : el=el+1
2. Reproduction loop : k=k+1
3. Chemotaxis loop : j=j+1
   - i. For i=1, 2, 3,---S take a chemotactic step for bacteria I as follows.
   - ii. Compute cost function, j (i, j, k, el).
   - iii. Let, J(i, j, k, el) = J(i, j, k, el) + $J_{cc}(\theta^i$ (j, k, el),P(j, k, el)) (i.e. add on the cell to cell attractant-repellant profile to simulate the swarming behavior) where J_{cc} is the objective function value to be added to the actual objective function value to be minimized.
   - iv. Let, J_{last} =J(i, j, k, el) to save this value since we may find a better cost via a run.
   - v. Tumble: generate a random vector δ(i) with each element $\delta_m(i)$, m= 1,2,…,p.
   - vi. Move: let

     Θ^i (j+1, k, el) = θ^i (j, k, el) + C(i)δ(i)/√δ(i) $\delta(i)^*$

     This result in a step of size C(i) in the direction of tumble for bacterium i.
   - vii. Compute J(i, j+1, k, el) and let,

     J(i, j+1, k, el) = J(i, j, k, el) + J_{cc} (θ^i (j+1, k, el),P(j+1, k, el))
   - viii. Swim:
     - Let m=0 (counter for swim length).

       While m<N_s
     - Let m= m+1

       If J (i, j+1, k, el) < J_{last} and let J_{last} =

       J (i, j+1, k, el) and let

       Θ^i(j+1, k, el) = θ^i(j, k, el) + C(i)δ(i)/√δ(i) $\delta(i)^*$

       And use this Θ^i (j+1, k, el) to compute the new J (i, j+1, k, el)

       Else, let m = Ns, this is the end of while statement.
   - ix. Go to next bacterium (i+1) if i± S (i.e., go to (ii) to process the next bacterium.
4. If J<Nc go to step 3. In this case continue chemotaxis since the life of bacteria is not over.
5. Reproduction:
   - I. For a given k and el , and for each I = 1, 2,…,S , let
     - i. J_{health} $\sum_{j=1}^{Nc+1} J(i,j,k,el)$
     - ii. Be the health of bacteria i. Sort bacteria and chemotactic parameter C(i) in order of ascending cost J_{health} (higher cost means lower health).
   - II. The S_r bacteria with the highest J_{health} value die and the remaining S_r bacteria with the best value split .
6. If k<N_{re}, go to step 2. In this case we have not reached the number of specified reproduction step , so we start the next generation of the chemotactic loop.
7. Elimination-dispersal: For i = 1, 2…..,S with probability p_{ed} , eliminate and disperse each bacterium To do this if a bacterium is eliminated , simply disperse another one to a random location on the optimization domain. If el < Ned then go to step 2; otherwise end.

III. PARTICLE SWARM ALGORITHM

A basic variant of the PSO algorithm works by having a population (called a swarm) of candidate solution (called particles). These particles are moved around in the search-space according to a few simple formulae. The movements of the particles are guided by their own best known position in the search-space as well as the entire swarm's best known position. When improved positions are being discovered these will then come to guide the movements of the swarm. The process is repeated and by doing so it is hoped, but not guaranteed, that a satisfactory solution will eventually be discovered. Formally, let $f: \mathbb{R}^n \rightarrow \mathbb{R}$ be the cost function which must be minimized. The function takes a candidate solution as argument in the form of a vector of real number and produces a real number as output which indicates the objective function value of the given candidate solution. The gradient of f is not known. The goal is to find a solution **a** for which f(**a**) ≤ f(**b**) for all **b** in the search-space, which would mean **a** is the global minimum. Maximization can be performed by considering the function $h = -f$ instead.

Let S be the number of particles in the swarm, each having a position $\mathbf{x}_i \in \mathbb{R}^n$ in the search-space and a velocity $\mathbf{v}_i \in \mathbb{R}^n$. Let $\mathbf{p}_i$ be the best known position of particle i and let **g** be the best known position of the entire swarm. A basic PSO algorithm is then

1. For each particle $i = 1, ..., S$ do:
   - a. Initialize the particle's position with a uniformally distributed random vector: $\mathbf{x}_i \sim U(\mathbf{b}_{lo}, \mathbf{b}_{up})$, where $\mathbf{b}_{lo}$ and $\mathbf{b}_{up}$ are the lower and upper boundaries of the search-space.
   - b. Initialize the particle's best known position to its initial position: $\mathbf{p}_i \leftarrow \mathbf{x}_i$
   - c. If $(f(\mathbf{p}_i) < f(\mathbf{g}))$ update the swarm's best known position: $\mathbf{g} \leftarrow \mathbf{p}_i$
   - d. Initialize the particle's velocity: $\mathbf{v}_i \sim U(-|\mathbf{b}_{up}-\mathbf{b}_{lo}|, |\mathbf{b}_{up}-\mathbf{b}_{lo}|)$
2. Until a termination criterion is met (e.g. number of iterations performed, or a solution with adequate objective function value is found), repeat:
   - a. For each particle $i = 1, ..., S$ do:
     - i. Pick random numbers: $r_p, r_g \sim U(0,1)$
     - ii. For each dimension $d = 1, ..., n$ do:
       1. Update the particle's velocity: $\mathbf{v}_{i,d} \leftarrow \omega\, \mathbf{v}_{i,d} + \varphi_p r_p (\mathbf{p}_{i,d}-\mathbf{x}_{i,d}) + \varphi_g r_g (\mathbf{g}_d-\mathbf{x}_{i,d})$
     - iii. Update the particle's position: $\mathbf{x}_i \leftarrow \mathbf{x}_i + \mathbf{v}_i$
     - iv. If $(f(\mathbf{x}_i) < f(\mathbf{p}_i))$ do:
       1. Update the particle's best known position: $\mathbf{p}_i \leftarrow \mathbf{x}_i$

2. If (f($\mathbf{p}_i$) < f($\mathbf{g}$)) update the swarm's best known position: $\mathbf{g} \leftarrow \mathbf{p}_i$

3. Now **g** holds the best found solution.

The parameters ω, φ_p, and φ_g are selected by the practitioner and control the behaviour and efficacy of the PSO method.

The optimal position of bacteria obtained by bacteria foraging optimization (BFO) is used as a local position of bacteria population which is also called candidate solution in particle swarm optimization in search space. The local position of bacteria population is initial position of bacteria position in search space which is updated using particle swarm optimization algorithm to find the best known position of bacteria in search space, if the best position of bacteria swarm is less than the global best known position of bacteria swarm then we update the position of bacteria position in search space to obtain global best position of bacteria swarm in search space.

For automatic generation control the objective function is taken as:-

$$J = \int_0^T \{(\Delta Fi)^2 + (\Delta Ptie - j)^2\}\, dt$$

IV. TABLE AND FIGURE

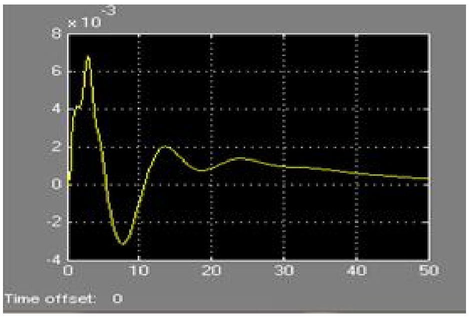


Fig.1 Shows the Relation b/w Δ P_{tie} and time for Thermal power plant PI Controller only

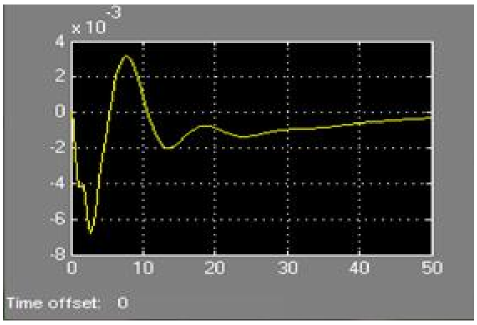


Fig.2 Show the Relation B/w Δ P_{tie} and time for hydro power plant PI Controller only

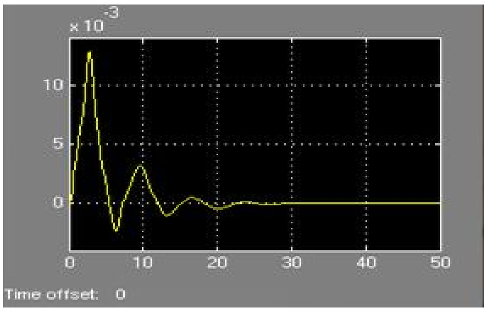


Fig.3 Shows the Relation B/w Δ P_{tie} and time for Thermal Power Plant Using PI controller and BFO

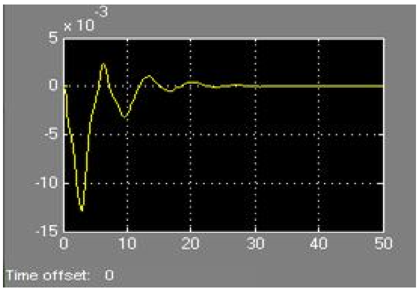


Fig.4 Shows the Relation B/w Δ P_{tie} and time for Hydro power plant Using PI Controller and BFO

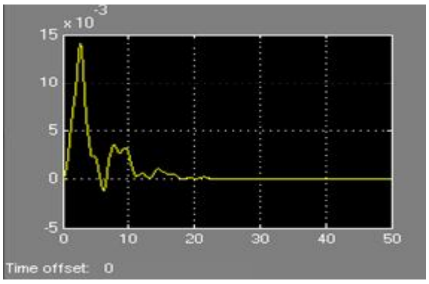


Fig.5 Shows the Relation B/w Δ P_{tie} and time for thermal Power Plant using PI Controller and (BFO+PSO)

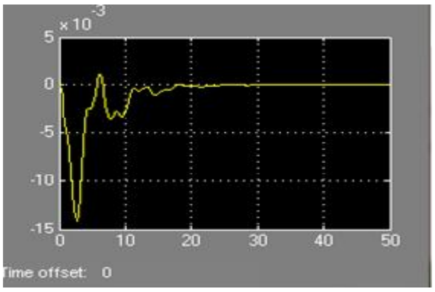


Fig.6 Showsthe Relation B/w Δ P_{tie} and time for Hydro Power Plant using PI Controller and (BFO+PSO)

Table 1

PARAMETER	PI CONTROLLER	BFO	BFO+PSO
CONTROLLER GAIN (Ki1)	0.1010	1.5575	2.1510
CONTROLLER GAIN (Ki2)	0.0510	0.1301	0.1001
SETTLING TIME (TS)	50(S)	25(S)	18(S)
INTEGRAL SQUARE ERROR	7.41(max)	0.0021(max)	0.0027(max)

V. CONCLUSION

When we apply the application of bacteria foraging particle swarm optimization (BFO+PSO) algorithm to an interconnected thermal-hydro power plant then the result reveal that tie-line power variation (ΔP_{tie}) can be reduced to nominal value or zero value in less consumption time as compared to bacteria foraging optimization and particle swarm optimization alone. The performance index (J) is also reduced to lower value and controller gains of thermal and hydro power plant are optimized in such a way that AGC give less variation in tie-line power and load frequency.

REFERENCES

[1]. Dr.C.Srinivasa Rao," Implementation of Load Frequency Control of Hydrothermal System under Restructured Scenario Employing Fuzzy Controlled Genetic Algorithm" IJAREEIE, Vol. 1, Issue 1, July 2012

[2]. J .Syamala, I.E.S. Naidu," Load Frequency Control of Multi-Area Power Systems Using PI, PID, and Fuzzy Logic Controlling Techniques" International Journal of Innovative Research in Science, Engineering and Technology, Volume 3, Special Issue 1, February 2014

[3]. Sachin Khajuria Jaspreet Kaur," Load Frequency Control of Interconnected Hydro-Thermal Power System Using Fuzzy and Conventional PI Controller" IJARCET, Volume 1, Issue 8, October 2012

[4]. Janardan Nanda, S. Mishra and Lalit Chandra," Maiden application of bacteria foraging optimization technique in multiarea automatic generation control ʼʼ IEEE Member.

[5]. Ratnesh Chaturvedi, Dr. Bharti Dwivedi," Comparative Analysis of PI & Fuzzy Based Cntroller For Load Frequency Control of Thermal-Thermal & Thermal: Hydro System" IJARCST Vol. 1 Issue 1 Oct-Dec 2013

[6]. Surya Prakash and Sunil Kumar Sinha," Performance Evaluation of Hybrid Intelligent Controllers in Load Frequency Control of Multi Area Interconnected Power Systems" World Academy of Science, Engineering and Technology Vol:7 2013-05-26

[7]. Aditi Gupta," Frequency Regulation Of Deregulated Power System Having Grc Integrated With Renewable Source" IJRET Volume: 02 Issue: 11 Nov-2013

[8]. B. Anand," Load Frequency Control of Hydro-Hydro System with Fuzzy Logic Controller Considering DC Link" Life Science Journal 2013

[9]. N. Cohn, "Some aspects of tie-line bias control on interconnected power systems," Amer. Inst. Elect. Eng. Trans., vol. 75, pp. 1415–1436, Feb. 1957.

[10] S. Farook, P. Sangameswara Raju, "AGC controllers to optimize LFC regulation in deregulated powersystem", International Journal of Advances in Engineering & Technology, IJAET ISSN:2231-1963, Nov 2011, Vol. 1, Issue 5, pp. 278-289.

[11]. Janardan Nanda, Mishra. S. , Lalit Chandra Saikia, "Maiden Application of Bacterial Foraging-Based optimization technique in multi-area Automatic Generation Control", IEEE Transaction on Power System, 24(2), (2009), 602-609.

[12]. B. Paramasivam and I. A. Chidambaram, "Bacterial Foraging Optimization Based Load-Frequency Control of Interconnected Power Systems with Static Synchronous Series Compensator", International Journal of Latest Trend in Computing, Vol 1, Issue 2, pp. 7-15, 2010.

[13]. M. Shanthakumar, Computer Based Numerical Analysis, Khanna Publishers, New Delhi, 1999.

[14]. Ghoshal, "Application of GA/GA-SA based fuzzy automatic control of multi-area thermal generating system", Electric Power System Research, 70, (2004), 115-127.

Performance Metrics in Wireless Sensor Network

Joni Birla [1]

[1] *Department of Computer Science & Engineering, Ganga Institute of Technology and Management, Kablana, Jhajjar, Haryana, INDIA*

Abstract— In last few years there has been significant growth in the area of wireless communication. Quality of Service (QoS) has become an important consideration for supporting variety of applications that utilize the network resources. These applications include voice over IP, multimedia services like video streaming, video conferencing etc.. This paper aims on performance Metrics as implemented by Ad-hoc networks. In real life we use voice call, video streaming which are set up through Wireless Sensor Network. We use many parameters for quality of service and these are: throughput, packet loss, average jitter and average delay. WSN is the part of Adhoc Network in which we don't have intelligent nodes. Wireless Sensor Networks (WSNs) are self-organizing, infrastructure less and multi-hop packet forwarding networks.

Index Terms—Improvement over WSN, Quality of services in Ad-hoc Network, Performance Metrics used in Adhoc Network, Characteristics of WSN

I.INTRODUCTION

Wireless Sensor Networks (WSNs) are self-organizing, infrastructure less and multi-hop packet forwarding networks. There is no concept of fixed base station. So, each node in the network acts as a router to forward the packets to the next node. Wireless networks are capable of handling of topology changes and malfunctions in nodes. It is fixed through network reconfiguration. For instance, if the node leaves the network and causes link breakages, affected nodes can request new routes and problem will be solved. This will slightly increase the delay, but the network will still be operational. It is the technology aimed to provide broadband wireless data access over long distances. This technology provides basic Internet Protocol (IP) connectivity to the user. The variety of applications used in IP networks has increased tremendously in the recent years. Various multimedia applications along with the common email, file transfer and web browsing applications are becoming increasingly popular. These applications send large audio and video streams with variable bandwidth and delay requirements. On the other hand, remote monitoring of critical services such as E-commerce and banking applications which do not need strict bandwidth guarantees due to the good nature of the data transfer. Instead, these applications require reliable and prompt packet routing. The presence of different kinds of applications in a network, results in heterogeneous traffic load. The traffic from different applications may require certain type of quality of service. In this paper, the Performance Metrics as prescribed in the Wireless Sensor networks is studied.

As packets travel within a wireless network such as WSN, they experience the following problems: Delay, jitter, out-of-order delivery, packet loss or error.

Quality of Service refers to the probability of the telecommunication network meeting a given traffic contract. In the field of packet-switched networks and computer networking it is used informally to refer to the probability of a packet succeeding in passing between two points in the network. Although the name suggests that it is a qualitative measure of how reliable and consistent a network is, there are a number of parameters that can be used to measure it quantitatively. These include throughput, transmission delay or packet delay, delay jitter, percentage of packets lost etc.

Quality of service enables end-to-end IP based QoS. Among other things, the MAC layer is responsible for scheduling of bandwidth for different users. The MAC layer performs bandwidth allocation based on user requirements as well as their QoS profiles. The standard is designed to support a wide range of applications. These applications may require different levels of QoS. To accommodate these applications, the WSN has defined many service flow classes.

These service flows can be created, changed, or deleted by the issuing Dynamic Service Addition (DSA), Dynamic Service Change (DSC), and Dynamic Service Deletion (DSD) messages. Each of these actions can be initiated by the Subscriber Station (SS) or the Base Station (BS) and are carried out through a two or three-way-handshake.

Wireless Sensor Networks (WSNs) are self-organizing, infrastructure less and multi-hop packet forwarding networks. These applications send large audio and video streams with variable bandwidth.

The services classes defined by Wireless Sensor Network are given below:

SERVICE CLASSES DEFINED BY WSN

	Description	Applications
Unsolicited Grant	For Constant Bit Rate (CBR) and	VOIP
Real-Time Polling	For Variable Rate and delay	Streaming audio, Streaming Video
Extended Real	For Variable Rate and delay	VOIP with silence Suppression
Non-real-time	Variable rate and non-real time	FTP
Best Effort	Best Effort	E-mail, web traffic

Fig:1

This paper focuses on the performance Metrics in Wireless sensor networks.. To analyze the QoS parameters simulation based on the popular network simulator ns-2 is used. Various parameters that determine QoS of real life usage scenarios and traffic flows of applications is analyzed. The goal is to compare different types of service flows with respect to the QoS parameters such as throughput, average jitter, average delay and packet loss, end to end delay, energy, Packet delivery fraction.

A WSN module written for ns-2 is used to simulate real life situations and analyze the effect of various network conditions and load on QoS parameters. We have many QoS Parameters like Throughput, Average delay, Average Jitter etc. The effect of the service flow on the quality of service parameters such as throughput, average jitter and packet loss is studied.

II. CHARACTERISTICS OF WSN

The following are the characteristics of wireless sensor networks.

- Dynamic topology: Due to the node mobility, the topology of wireless sensor networks changes continuously and unpredictably. The link connectivity among the terminals of the network dynamically varies in an arbitrary manner and is based on the proximity of one node to another node. It is also subjected to frequent disconnection during node's mobility. WSNs should adapt to the traffic and propagation conditions as well as to the mobility patterns of the mobile network nodes. The mobile nodes in the network dynamically establish routing among themselves as they move about, forming their own network on the fly. Moreover, a user in the WSNs may not only operate within the network, but may require access to a public fixed network.

- Bandwidth: WSNs have significantly lower bandwidth capacity in comparison with fixed networks. The used air interface has higher bit error rates, which aggravates the expected link quality. Current technologies suitable for the realization of WSNs are IEEE 802.11(b,a) with bandwidth up to 54Mbps and Bluetooth providing bandwidth of 1Mbps. The nature of high bit-error rates of wireless connection might be more profound in WSNs. One end-to-end path can be shared by several sessions. The channel over which the terminals communicate is subjected to noise, fading and interference, and has less bandwidth than a wired network. In some scenarios, the path between any pair of users can traverse multiple wireless links and the links themselves can be heterogeneous.

- Energy: All mobile devices will get their energy from batteries, which is a scarce resource. Therefore the energy conservation plays an important role in WSNs. This important resource has to be used very efficiently. One of the most important system design criteria for optimization may be energy conservation.

- Security: The nodes and the information in WSNs are exposed to the same threats like in other networks. Additionally to these classical threats, in WSNs there are special threats, e.g. denial of service attacks. Also mobility implies higher security risks than static operations because portable devices may be stolen or their traffic may insecurely cross wireless links. Eavesdropping, spoofing and denial of service attacks should be considered.

- Autonomous: No centralized administration entity is required to manage the operation of the different mobile nodes. In WSNs, each mobile terminal is an autonomous node, which may function as both a host and a router. So usually endpoints and switches are indistinguishable in WSNs.

- Distributed Operation: Since there is no background network for the central control of the network operations, the control and management of the network is distributed among the terminals. The nodes involved in a WSNs should collaborate among themselves and each node acts as a relay as needed, to implement functions e.g. security and routing.

- Multi-hop Routing: Basic types of ad hoc routing algorithms can be single-hop and multi-hop, based on different link layer attributes and routing protocols. Single-hop WSNs is simple in comparison with multi-hop WSNs in terms of structures and implementation. When delivering data packets from a source to its destination out of the direct wireless transmission range, the packets should be forwarded via one or more intermediate nodes.

- Light-Weight Terminals: In most cases, the WSNs nodes are mobile devices with less CPU processing capability, small memory size and low power storage.

- Infrastructure less and Self Operated: A wireless sensor a network includes several advantages over traditional wireless networks, including: ease of deployment, speed of deployment and decreased dependence on a fixed infrastructure. WSN is attractive because it provides an instant network formation without the presence of fixed base stations and system administrators.

III. NETWORK SIMULATOR

The network simulator 2 (ns-2) is a popular tool for the simulation of packet-switched networks. It provides substantial support for simulation of TCP, routing, and MAC protocols over wired and wireless networks. The simulator core is written in C++. It has an OTcl (Object Tool Command Language) interpreter shell as the user interface and allows input models written as Tcl (Tool Command Language) scripts to be executed. Most network elements in ns-2 simulator are developed as classes, in object-oriented fashion. It is freely distributed and all the source code is available.

Figure shows basic structure of ns-2. The network topology and traffic agents etc are specified in the TCL file. It is parsed by the oTCL interpreter. The C++ library has all the implementation details. When ns-2 is run, the resulting data could be obtained in a trace file format. The trace file contains time stamp and information about each packet that is sent, received or dropped. It also has information about the packet size, type of packet etc. A base station and a subscriber station can be set up as a node in ns-2. As the number of nodes in the simulation increase, the packets that are sent and received increases. This makes the trace file very large.

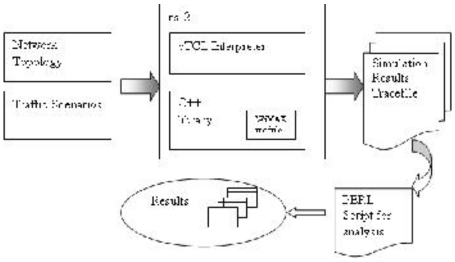


Fig:2 NS-2 Architecture

IV. PERFORMANCE METRICS

Performance Metrics encompasses Quality of Service to the end user in terms of several generic parameters. The perceived quality of service can be quantitatively measured in terms of several parameters. In the analysis, the throughput, average delay, average jitter, packet loss, end-to-end delay, Packet delivery fraction and energy were considered.

Throughput

Throughput is a measure of the date rate (bits per second) generated by the application. Equation shows the calculation for throughput TP, where PacketSize is the packet size of the i^{th} packet reaching the destination, PacketStart is the time when the first packet left the source and PacketArrival is the time when the last packet arrived.

$$TP = \sum PacketSize/(PacketArrival - PacketStart)$$

From the trace file, based on the packet ID, each data packet was kept track of. The time a packet is sent, the time when the packet was received and the packet size was stored for all packets that reached the destination. To calculate throughput, the size of each packet was added. This gave the total data that was transferred.

The total time was calculated as the difference between the time the first packet started and the time the last packet reached the destination. Thus throughput is equal to the total data transferred divided by the total time it took for the transfer.

Average Delay

Delay or latency would be time taken by the packets to transverse from the source to the destination. The main sources of delay can be further categorized into: source-processing delay, propagation delay, network delay and destination processing delay. Equation 2 show the calculation for Average Delay, where $PacketArrival_i$ is the time when packet "i" reaches the destination and $PacketStart_i$ is the time when packet "i" leaves the source. "n" is the total number of packets.

Average delay= (Packet Arrival- Packet Start)/n

Average Jitter

Delay variation is the variation in the delay introduced by the components along the communication path. It is the variation in the time between packets arriving. Jitter is commonly used as an indicator of consistency and stability of a network. Measuring jitter is critical element to determining the performance of network and the QoS the network offers.

Average Jitter= ((Packet Arrival+1)- (Packet Start+1))-((Packet Arrival)-(Packet Start))/n-1

Packet loss or corruption rate

Packet loss affects the perceived quality of the application. Several causes of packet loss or corruption would be bit errors in an erroneous wireless network or insufficient buffers due to network congestion when the channel becomes overloaded.

Packet Loss= (∑(Lost Packet Size/∑Packet Size)*100

Packet Delivery Fraction

The ratio of the data packets delivered to the destinations to those generated by the CBR sources is known as packet delivery fraction.

End-to-End Delay

Network delay is the total latency experienced by a packet to traverse the network from the source to the destination. At the network layer, the end-to-end packet latency is the sum of processing delay, packet, transmission delay, queuing delay and propagation delay. The end-to-end delay of a path is the sum of the node delay at each node plus the link delay at each link on the path.

Energy

The total number of energy consumed for packets transmitted and packet receiving during the simulation.

V.CONCLUSION

In this paper, the characteristics and service classes of wireless sensor networks were studied. We have concentrated here different performance metrics like PDF, end to end delay, energy, throughput, packet loss .

REFERENCES

[1] Reactive Routing Protocols of MANET using Group Mobility Model" International Journal of Computer Sciences, Vol 7, Issue 3, May 2010.

[2] [2] B.Chen, K.Jamieson, H.Balakrishnan, and R.Morris. "Span : An energy efficient coordination algorithm for topology maintenance in ad hoc wireless

[3] networks in Pro of the ACM/ IEEE International Conference on Mobile Computing and Networking, July 2001.

[4] [3] Performance Measurement of various Routing Protocols in Adhoc Network" International Multiconference of Engineers and computer scientists 2009 Vol 1,

[5] March 2009.

[6] [4] http://en.wikipedia.org

[7] [5] Study on Energy Conservation in MANET" journal of networks, vol 5, No 6, JUNE 2010.

[8] [6] Performance Comparison Of Manet Protocols"©2010 International Journal of Computer Applications (0975 – 8887) Volume 1 – No. 1.

Precast Concrete For Building Systems

Manoj Lakra[1], Sarita Dagar[2], Sheela Malik[3], Amit Singhal[4], Lokesh Yadav[5]

[1,2,3,4,5]*Department of Civil Engineering, Ganga Institute of Technology and Management, Kablana, Jhajjar, Haryana, INDIA*

ABSTRACT-The application of precast concrete structural systems has been attaining vast progress worldwide in the last few decades. This is due to the fact that the precast structural systems possess several advantages compared to monolithic systems, such as quality control, speedy construction, and suitable application to regularly modular systems.

The paper deals with the use and the application of precast concrete for various types of buildings. The paper also describes the earthquake performances of precast buildings, seismic-strengthening techniques and Benefits of Using Precast elements in Building Construction.

***Keywords*: Precast concrete, Building Structures**

I. INTRODUCTION

The concept of precast (also known as “prefabricated”) construction includes those buildings where the majority of structural components are standardized and produced in plants in a location away from the building, and then transported to the site for assembly. These components are manufactured by industrial methods based on mass production in order to build a large number of buildings in a short time at low cost.

The main features of this construction process are as follows:

- The division and specialization of the human workforce
- The use of tools, machinery, and other equipment, usually automated, in the production of standard, interchangeable parts and products

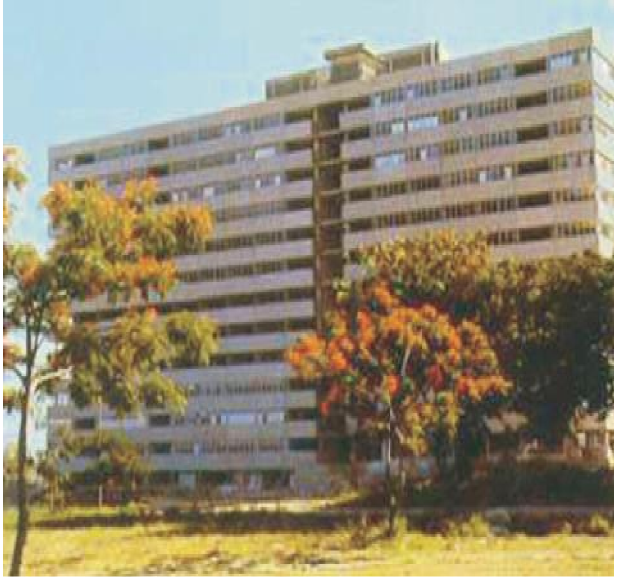


Figure 1: A typical precast slab-column building.

This type of construction requires a restructuring of the entire conventional construction process to enable interaction between the design phase and production planning in order to improve and speed up the construction. One of the key premises for achieving that objective is to design buildings with a regular configuration in plan and elevation. Urban residential buildings of this type are usually five to ten stories high (see Figure 1). Many countries used various precast building systems during the second half of the 20th century to provide low-income housing for the growing urban population. They were very popular after the Second World War, especially in Eastern European countries and former Soviet Union republics.

In general, precast building systems are more economical when compared to conventional multifamily residential construction (apartment buildings) in many countries. The reader is referred to the UNIDO report for detailed coverage on precast systems and their earthquake resistance.

Categories of Precast Building Systems

Depending on the load-bearing structure, precast systems described in the WHE can be divided into the following categories:

- Large-panel systems
- Frame systems
- Slab-column systems with walls
- Mixed systems

II. LARGE-PANEL SYSTEMS

The designation “large-panel system” refers to multi-storey structures composed of large wall and floor concrete panels connected in the vertical and horizontal directions so that the wall panels enclose appropriate spaces for the rooms within a building. These panels form a box-like structure (see Figure 2a, 2b). Both vertical and horizontal panels resist gravity load. Wall panels are usually one story high. Horizontal floor and roof panels span either as one-way or two-way slabs. When properly joined together, these horizontal elements act as diaphragms that transfer the lateral loads to the walls.

Depending on the wall layout, there are three basic configurations of large-panel buildings

- Cross-wall system. The main walls that resist gravity and lateral loads are placed in the short direction of the building.
- Longitudinal-wall system. The walls resisting gravity and lateral loads are placed in the longitudinal direction; usually, there is only one longitudinal wall.
- Two-way system. The walls are placed in both directions.

Thickness of wall panels ranges from 120 mm for interior walls to 300 mm for exterior walls. Floor panel thickness is 60 mm. Wall panel length is equal to the room length, typically on the order of 2.7 m to 3.6 m. In some cases, there are no exterior wall panels and the façade walls are made of lightweight concrete.

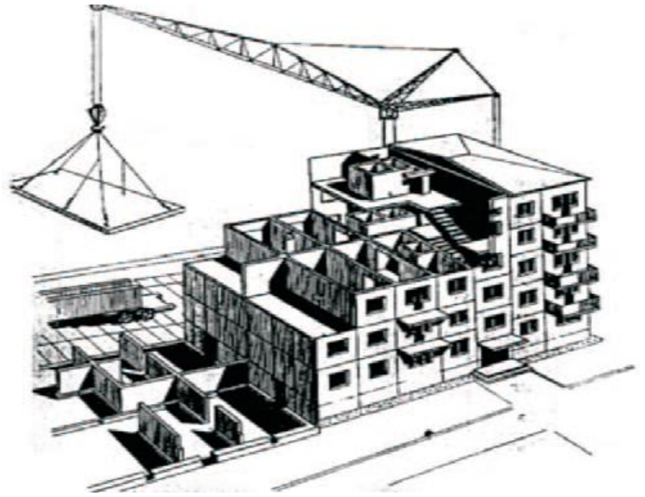


Figure 2a: A large-panel concrete building under construction

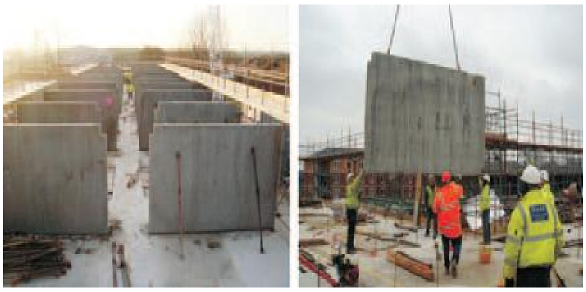


Figure 2b: Cross Wall construction

Lateral stability of a large-panel building system is provided by the columns tied to the wall panels. Boundary elements are used instead of the columns as “stiffening” elements at the exterior. The unity of wall panels is achieved by means of splice bars welded to the transverse reinforcement of adjacent panels in the vertical joints. Longitudinal dowel bars placed in vertical and horizontal joints provide an increase in bearing area for the transfer of tension across the connections. Wall-to-floor connection is similar to that shown in Figure 3.

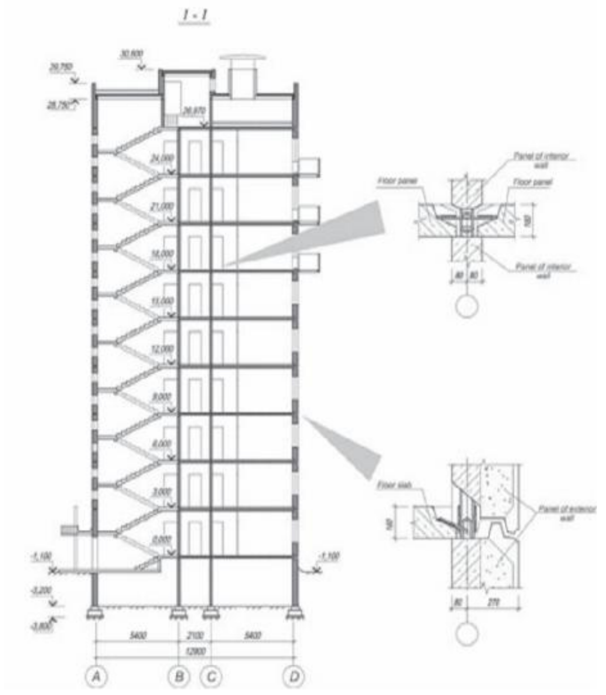


Figure 3: Plan of a large-panel building showing vertical connection details

III. Frame Systems

Precast frames can be constructed using either linear elements or spatial beam-column sub assemblages. Precast beam-column sub assemblages have the advantage that the connecting faces between the sub assemblages can be placed away from the critical frame regions; however, linear elements are generally preferred because of the difficulties associated with forming, handling, and erecting spatial elements. The use of linear elements generally means placing the connecting faces at the beam-column junctions. The beams can be seated on corbels at the columns, for ease of construction and to aid the shear transfer from the beam to the column. The beam-column joints accomplished in this way are hinged. However, rigid beam-column connections are used in some cases, when the continuity of longitudinal reinforcement through the beam-column joint needs to be ensured. The components of a precast reinforced concrete frame are shown in Figure 4.

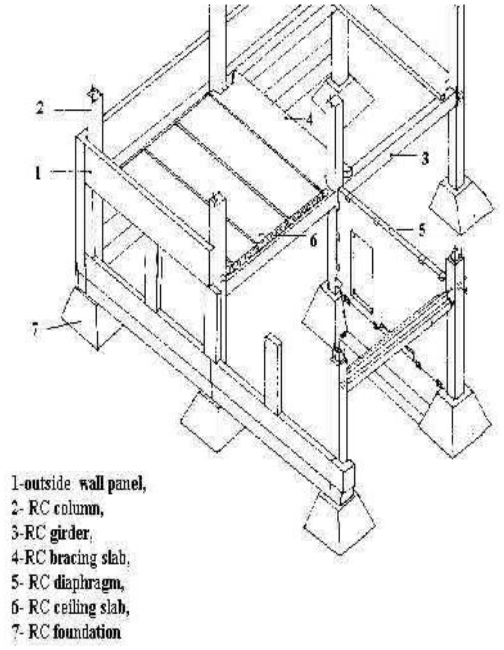


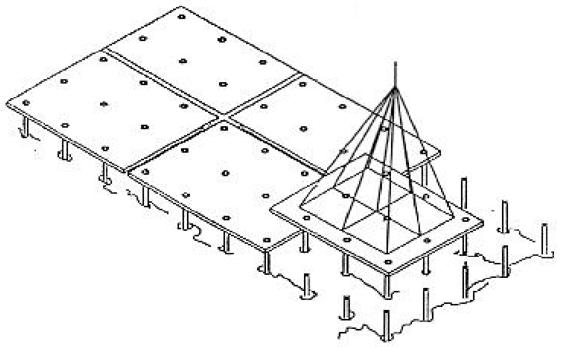
Figure 4: Components of a precast reinforced concrete frame system

IV. Slab-Column Systems with Shear Walls

These systems rely on shear walls to sustain lateral load effects, whereas the slab-column structure resists mainly gravity loads. There are two main systems in this category:

- Lift-slab system with walls
- Pre-stressed slab-column system

The load-bearing structure consists of precast reinforced concrete columns and slabs, as shown in Figure 6. Precast columns are usually two stories high. All precast structural elements are assembled by means of special joints. Reinforced concrete slabs are poured on the ground in forms, one on top of the other, as shown in Figure 5. Precast concrete floor slabs are lifted from the ground up to the final height by lifting cranes. The slab panels are lifted to the top of the column and then moved downwards to the final position. Temporary supports are used to keep the slabs in the position until the connection with the columns has been achieved.



The Large Precast Flat Slab System

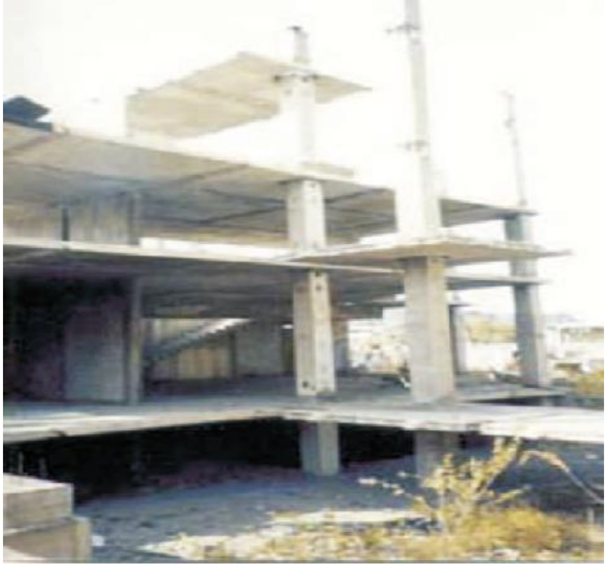


Figure 5: A lift-slab building under construction

V. Earthquake Performance

There is a general concern among the earthquake engineering community regarding the seismic performance of precast construction. Based on experience in past earthquakes in Eastern European and in Central Asian countries where these systems have been widely used, it can be concluded that their seismic performance has been fairly satisfactory. However, when it comes to earthquake performance, the fact is that “bad news” is more widely publicized than “good news.” For example, the poor performance of precast frame systems of Seria 111 in the 1988 Spitak (Armenia) (M7.5) earthquake is well known. However, few engineers are aware of the good seismic performance (no damage) of several large-panel buildings under construction at the same site, remained undamaged.

Due to their large wall density and box-like structure, large panel buildings are very stiff and are characterized with a rather small fundamental period. For example, a 9-story building in Kazakhstan has a fundamental period of 0.35 to 0.4 sec (WHE Report 32). In general, large-panel buildings performed very well in the past earthquakes in the former Soviet Union, including the 1988 Armenia earthquake and the 1976 Gazly earthquakes (Uzbekistan). It should be noted, however, that large-panel buildings in the area affected by the 1976 Gazly earthquakes were not designed with seismic provisions. Most such buildings performed well in the first earthquake (M 7.0), but more damage was observed in the second earthquake that occurred the same year (M 7.3), as some buildings had been already weakened by the first earthquake

VI. Seismic-Strengthening Technologies

According to WHE reports, no major efforts have been reported regarding seismic strengthening of precast concrete buildings. However, seismic strengthening of precast frame buildings was done in Uzbekistan . The techniques used include the installation of steel straps at the column locations (see Figure 6) and reinforcing the joints with steel plates to provide additional lateral confinement of the columns.

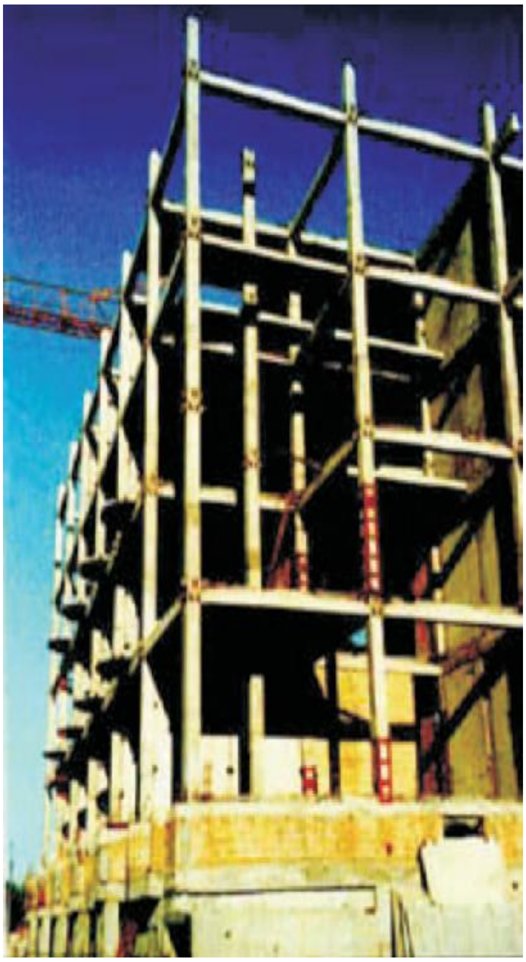


Figure 6: Seismic strengthening of precast columns with steel straps

VII. Benefits of Using Precast elements in Building Construction

A. *Hotels*

Precast Structures uses a system of precast elements which link together to form a cross-wall format. Panels can be formed in solid or twin wall styles to suit the design requirements of the structure. Whichever solution is selected the selections are produced in high quality finish which is suitable for direct decoration, with minimal preparatory work, obviating the need for plaster finishes, leading to cost and programme savings.

The philosophy of PCS is to produce a design which will provide the most cost effective solution, utilising the most appropriate materials for the project. This can include such items as hot rolled steel sections and cold rolled steel infill panels as appropriate.

Benefits of Using Precast Concrete Structures Include

1) High quality concrete designed for direct decoration or exposure.

2) Architectural and structural quality components.
3) Large volume supply capacity.
4) Dedicated experience project management.
5) In house Erection by trained and qualified erection personnel.
6) Solid room size slabs
7) Prefinished for direct ceiling decoration.
8) Suitable for direct carpet application.
9) Reduced structural zones free from downstands.
10) Erection of stair and lift cores as erection progresses allowing safe access for subsequent trades.
11) Pre-fitted windows option.

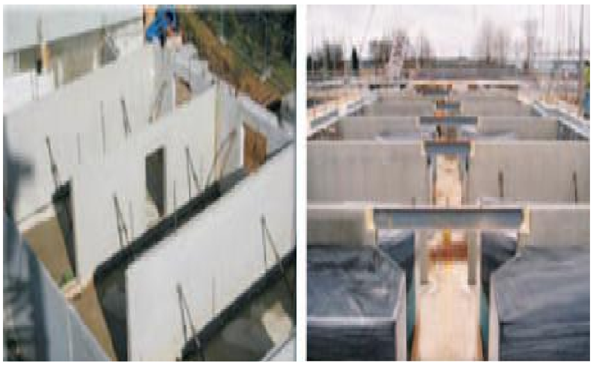


Figure 7: Use of precast concrete in hotel construction

Precast Concrete Structures Ltd specialise in the fast efficient delivery of the building structure, where minimal wet trades and high quality finish are essential to follow on trades. PCS strive to be market leaders in quality of finished product and offer an innovative and non-contractual approach to building structures. Some typical hotels made of precast concrete shown in Figure7.

B Student Accommodation

Cross-Wall Construction The use of cross-wall construction in student accommodation (See Figure 8) gives significant benefits for short-term build projects where a deadline for opening is critical. Precast concrete construction offers extremely durable accommodation, capable of sustaining even the toughest conditions of student living. By the use of direct finishing techniques to the walls and ceiling, together with solid room-sized slabs, and the pre-installation of bathroom pods, cross-wall construction offers speed of construction together with economy.

Key requirements for economical construction in student accommodation include:

- Repetition of room layout.
- Consistency of vertical alignment to division walls.
- Repetition of elevational treament.

By adhering to these basic principles, Precast Concrete Structures Ltd will provide advice and innovative solutions on the most economical means of manufacturing the components and sequencing the erection to the maximum benefit of the client. These benefits include:

- Fast-build programme within term-time constraints.
- Direct decoration to walls and ceilings, with only minor pre-decoration treatment.
- Pre-installation of windows.
- Early “dry-box” working for subsequent trades.
- A variety of elevational treatments using non-load bearing cladding systems (loads are transferred via the cross-walls and do not rely upon external walls for support).
- Reduced structural zone without downstands.

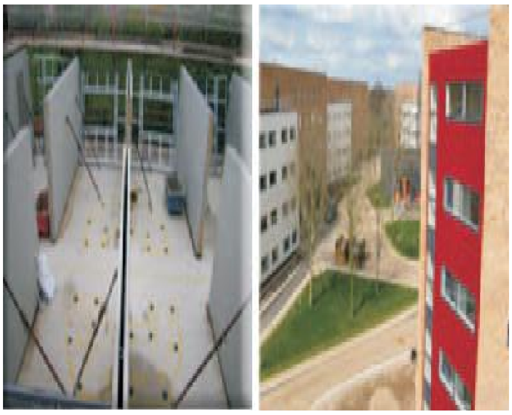


Figure 8: Use of precast concrete in hostel construction

C Apartments

Apartment construction has become increasingly popular as a modular build (Refer Figure 9) alternative to traditional steel and in-situ concrete frame methods. The system adopted uses cross-wall construction in a similar method to the hotel construction system, but differs in that the variability of room layouts and external elevations require differing techniques and innovative thinking to produce fast-build economical solutions. The options for apartments are both extensive and flexible providing key criteria in design are met. Precast Structures Ltd has broad experience in developing solutions for alternative construction, particularly suited to the Design & Build market.

Benefits include

- Direct decorative finish to walls with only minor pre-decoration treatment, negating the requirements for wet plaster.
- Optional methods of floor construction, allowing flexibility for individual client requirements, including:
  1) Traditional hollow-core.
  2) Wide slab composite flooring.
  3) Pre-finished solid slabs.
  4) Direct soffit finishing in replacement of suspended ceilings, significantly reducing construction build costs
  5) Reduced structural zone without down stands.
  6) Construction of common stairs and lift cores as the erection progresses, permitting early access for subsequent trades.
  7) Pre-fitted windows.
  8) External pre-finished cladding panels, grey concrete inner leaf only, or curtain-walling / metal stud permitting total flexibility in elevational treatment.

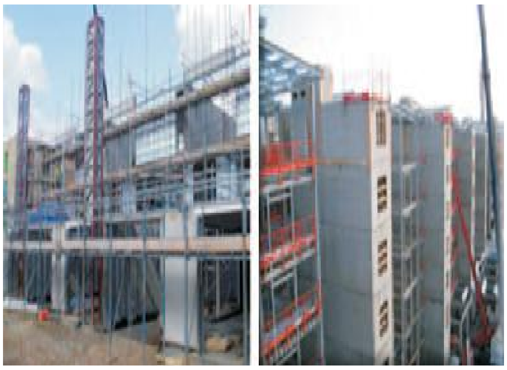


Figure 9: Use of Precast concrete technology in apartment construction

Apartment construction is usually designed with traditional building solutions which are subsequently modified during the design process to obtain a competitive edge in Design & Build solutions. The benefits of early consultation with Precast Structures will result in significant savings in both cost and time, resulting from economical manufacture solutions and reduced erection periods.

D Architectural Concrete

Precast Concrete Structures has extensive use in manufacture and erection of architectural and structural building components. Sections are bespoke and can be manufactured within the programme for our standard materials with a wide range of finishes and colours including:

- Brick.
- Wet cast reconstituted stone cladding and dressings.
- Composite Architectural / Structural insulated columns.
- Exposed structural elements.

Buildings are considered on an individual basis and assessed for integration of structural components to reduce programme and to ultimately drive down costs.

VII. PROGRESSIVE COLLAPSE

Concrete building structures whether, insitu or precast, is required to perform in the event of accidental damage or explosion by meeting the design criteria for progressive collapse.

Within the building structure, ties are incorporated to resist calculated forces determined by a variety of factors, including:

- Number of stories
- Centres of walls / size of spans
- Total loads carried

These are achieved by the use of the following ties incorporated into the precast cross-wall design:

- Vertical ties
- Horizontal ties
- Peripheral ties
- Internal ties

Joints between panels are tied together using pre-shuttered in-situ-fill to create a robust joint with minimal finishing required. The joints use wire ties designed to meet the specific tie-force criteria, but also to allow flexibility in assembly tolerances during erection. Peripheral and internal ties use high strength steel strand within the nominal in-situ joints at cross-wall locations and around the perimeter of the building to create a continuous tie arrangement. Building design is analysed for structural stability by Precast Structures consultants who have extensive knowledge in the design stability of cross-wall building structures.

VIII. CONCLUSION

By producing precast concrete in a controlled environment (typically referred to as a precast plant), the precast concrete is afforded the opportunity to properly cure and be closely monitored by plant employees. Utilizing a Precast Concrete system offers many potential advantages over site casting of concrete. The production process for Precast Concrete is performed on ground level, which helps with safety throughout a project. There is a greater control of the quality of materials and workmanship in a precast plant rather than on a construction site. Financially, the forms used in a precast plant may be reused hundreds to thousands of times before they have to be replaced, which allow cost of formwork per unit to be lower than for site-cast production. The use of precast concrete in Indian construction industry will definitely enhance the efficiency of the contractor in terms of quality, safety and time of project completion. In developing country like India, adoption of this technology for building construction will boost the Government's development plans, as this gives really faster way of construction and also quality of work far better than onsite casting concrete which is really value for money.

REFERENCE

[1] http://www.precaststructures.com

[2]N. Krishnaraju, Prestressed concrete,Tata McGraw-Hill, New Delhi-2004.

Preventing Abuse of Cookies Stolen by XSS

Sachin[1], Yashpal[2]

[1, 2] *Department of Computer Science &Engineering, Ganga Institute of Technology and Management, Kablana, Jhajjar, Haryana, INDIA*

Abstract—Cross Site Scripting (XSS) makes victims execute an arbitrary script and leaks out personal information from victims' computers. An adversary can easily get victim's cookies by the XSS attack. If the adversary cannot use the stolen cookies to impersonate the victim, stealing cookie has no meaning. Therefore, we propose a method to prohibit the abuse of stolen cookies in order to make it ineffective to steal cookies through the XXS attack. The proposed method uses onetime password and challenge-response authentication to identify whether a person is a valid owner of the cookie.

***Keywords*:- Cookies, Cross Site Scripting, HTTP, Web Application**

I. INTRODUCTION

Today the Internet is widely used all over the world. More the Internet is used, more the security of computer is demanded. Especially protecting personal information is one of major concerns because of the advent of various kinds of Internet services such as SNS and online shopping. Such various kinds of services often use a function called "cookie".

Cookie is a small piece of data sent from a website and stored in a user's web browser while a user is browsing the website [1],[2]. browsing It can be read out by web server whenever needed. Cookie provides websites with a reliable mechanism for remembering their state and user's activities. Cross Site Scripting (XSS) is a typical web application vulnerability[3] and an attacker of XSS can steal cookies by setting up the execution of malicious scripts after crossing several websites. This attack finally enables the adversary to do illegal access or session hijack. Nowadays, XSS dominates the largest percentage of all web application vulnerabilities [4]. Unfortunately, there is no effective way to prevent it [5], [6]. A secure cookie system and a method to prevent XSS attack are highly demanded.

In this paper, we propose a secure cookie protocol which prevents the abuse of cookies stolen by XSS. If an adversary cannot abuse the cookies, accounts of the victims remain safe. This paper is organized asfollows. After the introduction, we explain background knowledge of HTTP, Cookies and XSS including a fundamental method to invalidate a malicious script contained in HTTP request in section II. In addition to the fundamental method, previous methods are described in section III. Then we describe a new method to prevent abuse of stolen cookies with enough usability in section IV. After that, we discuss in comparison with previous methods in section V. Conclusion is given in section VI.

II. BACKGROUND

A. Session Management of HTTP

Hyper Text Transfer Protocol (HTTP) is a protocol which is constructed for exchanging data between a web browser and a web server at World Wide Web (WWW). HTTP is a request-response type protocol such that a client, web browser, sends a server a HTTP request containing URL and method, and receives a HTTP response. The set of request and response is called session. When the session is completed, connection between the client and the server is disconnected. The connection is stateless. That is, the erver treats each request as an independent connection: The server does not hold the information of the previous client and cannot reflect the state of the previous session. This kind of stateless protocol is not suitable for online operations such as online shopping. In order to solve this problem, there is an idea of session management which provides statefull protocol that is able to hold the state of the connection. Session management means that the server recognizes the session with the clients and grasps the progress of processing. If session starts, messages between the server and the client share the same session ID. They recognize each other by checking the session ID [7].

B. Cookie

The technology which enables the session management over the HTTP protocol is called cookie. Cookie is widely used for storing the session ID and personal information handled in web applications. It is a small size of data stored in a text file of the user's computer and exchanged between the server and the client [1], [2]. There are six parameters in the cookie called attribute.

1. Name of the cookie
2. Value of the cookie
3. Deadline of the cookie
4. Path of the server which the browser sends the cookie
5. Domain of the server where the browser sends the cookie
6. The demand for a secure connection between the browser and the server.

Cookie is given to a web browser from the server and is held at the browser until it expires. There are two types of cookies, a session cookie and a persistent cookie. The session cookie is used temporarily and discarded when the browser closes. The value of a session cookie is a random value and renewed every time a new session starts. On the other hand, a persistent cookie is stored in the browser for a definite period of time. Once a persistent cookie is given to the browser, it can be reused for any number of times, which improves the performance of web services.

C. Cross Site Scripting (XSS)

An attack of XSS [3] inserts a malicious script while a user is browsing web pages. If the attack succeeds, the adversary makes a victim to execute an arbitrary script which is sent from the server to the browser without any translation. The adversary does not attack a vulnerable server directly, but uses the vulnerability to lead a target user to a phishing page.

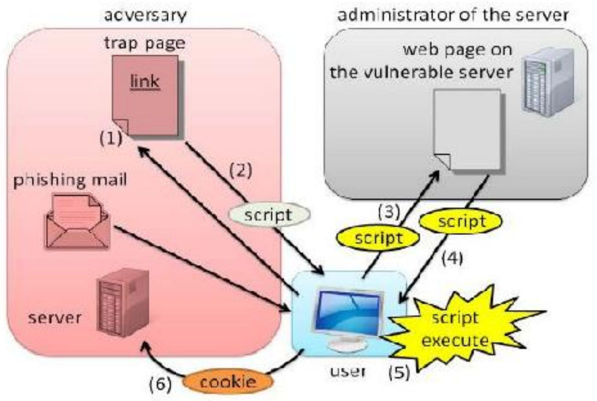


Fig 1. Procedures of XSS

The figure 1 shows the concept and procedures of XSS. An attacker follows the following procedures to launch the XSS attack.

1. An adversary prepares a web site (trap page) and puts a link to other web site which has vulnerability. The link contains a malicious script, that sends cookie to the adversary in step 6).
2. When a user comes to the trap page, he receives the HTTP response which contains malicious script. At this stage, the script has not been invoked.
3. When a user clicks the link, the malicious script is sent to the vulnerable server as a part of HTTP request.
4. The server returns the malicious script to the user's browser without any process because of the vulnerability.
5. The browser executes the malicious script because the browser falsely regards the script is required not from the adversary but from the server.
6. Because of the execution of the malicious script, the browser sends cookie or personal information to the adversary.

If the vulnerable server exists, it enables the adversary to commits various kinds of attack by crossing a trap page and embeds a malicious script. It means that after the success of the XSS attack the adversary can get personal information to impersonate a valid user or session hijack.

XSS vulnerability often exists in the web page which has a text field and operates dynamically according to the input character. Therefore web pages which deal with the personal information such as resister page or login page are more likely to have XSS vulnerability. The cause of XSS vulnerability is that a web browser executes all scripts received from any server. Of course a browser has option to prohibit the execution of all the scripts that the browser receives. However, it spoils the convenience of cookies. One of the reasons why XSS is still a major issue is low level awareness of people who manage the web server. People who are not an expert of computing can make web pages easily today and get damage of XSS. Meanwhile, server administrators are less likely to take an active action against XSS because they do not get damage directly. Also, taking measures against XSS needs a lot of cost and XSS seems to be ignored in spite of its damages.

A fundamental method to invalidate a malicious script contained in the HTTP request is escaping special characters by using CGI script. In the method, servers regard a script in the HTTP request as a script embedded by an adversary. The CGI script replaces special characters such as ”&” and ”<” of the HTTP request with equivalent characters shch as ”&amp;” and ”&lt;”, respectively, before it is sent to the user's browser as a HTTP response. A malicious script is never executed after escaping special characters. Unfortunately, there are still many sites which do not take this counter measure. From these reasons, XSS is still a major attack in computer networks that we must prevent.

III. PREVIOUS WORK

A. *Using Session Cookie*

Cookie is stored at a browser until it expires. If we are able to remove the cookie before the adversary successfully steals it, the leakage of cookie never happens. The valid period of cookie can be determined by setting the deadline of cookie described in section II-B. In the session cookies, the period is set at the past time so that these cookies will be removed every time the session terminates. This method [5] disables the adversary to abuse the stolen cookie, but it ruins the advantage of cookie which does not require the valid user to input his personal information every time he logs in to his account. Also it cannot prevent replay attack which reuse the password stored in the session cookie.

B. Dynamic Cookies Rewriting Technique

Rewriting the value of cookies is effective for precluding the adversary to use stolen cookies [8]. When the server sends a cookie to the browser, a web proxy changes the values of the cookie into randomized values before stored in the browser. As the browser's database does not have the original values of the cookies, the adversary does not get the true values even if the XSS attack succeeds. The proxy has a table which stores the attributes of the cookie and randomized values. When a server requests the browser to send a cookie, the randomized cookie is rewritten to the original value by the proxy and send to the server. A user can reuse the same cookie again. So the user can enjoy the benefit of the cookie. However there are two types of adversaries for which this method does not work; (1) If an adversary and valid users are in the same LAN and the adversary steals the randomized cookies, the adversary succeeds in impersonation by sending these cookies through the same proxy in the LAN. (2) When an adversary steals cookies after the proxy writes them back to the original values, these stolen cookies contain true values. This method is secure only if the adversary cannot use the same web proxy as a valid user uses. Concerning replay attack, both of adversaries described above can perform replay attack easily.

IV. PREVENTING ABUSE OF STOLEN COOKIES

A. Outline

As explained in section II-C, direct anti-XSS methods such as escaping special characters is not secure enough. In this section, we discuss indirect anti-XSS methods. In our approach, we pay attention to decreasing the effect of stealing cookies by XSS. That is, an adversary cannot abuse stolen cookies even if they have leaked out. Stolen cookies are often used for session hijacking and prohibiting abuse of the stolen cookies allows us to prevent session hijacking. When someone accesses to a login page with a stolen cookie, the system regards him as a valid user and impersonation succeeds. From this point of view, distinguishing a regular user from an adversary possessing stolen cookies is effective for invalidating the XSS. In the next section, we propose a method for indirect anti- XSS using the challenge-response authentication.

B. Synchronize State Cookie Protocol

We propose a method that uses one-time password and challenge-response authentication. In our method, a server and a user have the same password which is renewed every fixed time. The user keeps the password in the persistent cookie and uses it when he needs to log in to his account. The password the user uses and the password the server keeps need to be synchronized at all times. There are various kinds of one-time password schemes [9]. If a new password is generated by an algorithm using a secret value, the value should not be stored in any cookie.

We also use challenge-response authentication in our method. In response to an authentication request, the server sends a challenge value to the user. We use a PHP session ID as a challenge value. A user calculates the response value by hashing the concatenation of his password and the challenge value. Then the user sends the response value to the server, and the server checks whether the value matches with the value calculated by the server or not. When it matches, the user is able to access his account.

V. CONSIDERATION

In this section, we discuss properties of the proposed method. There are some advantages in our method. Even if an adversary succeeds in stealing a password contained cookie by XSS, the adversary cannot abuse the cookie after its expiry. In other words, the adversary cannot impersonate a valid user when a fixed time has passed. However, before the cookie expires, the adversary can succeed in impersonation. From this reason, we have to set an appropriate short interval to renew the password. Challenge-response authentication avoids the reuse of intercepted values. Even if an adversary gets the response value sent from a valid user to the server, the adversary cannot use it later because a different challenge is sent to the adversary in the succeeding authentication. Our method can prevent the replay attack.We compare our method with previous work. The table I shows the summary of the comparison. As described in section III-B, the Dynamic Cookies Rewriting Technique is vulnerable to several types of adversaries, and the abuse of cookies is prevented depending on the type of adversaries. Using proxy to rewrite the cookie causes latency of communication between the server and the user. Our method also makes latency because of a challenge-response authentication. The Dynamic Cookies Rewriting Technique rewrites the cookies and keeps the original values of the cookies at proxy. So when it fails to write them back to original values, even the valid user cannot properly access to the server. Our method needs to synchronize a password between the user and the server. When the synchronization fails, the authentication fails. Both methods have a possibility to induce errors such that cookies do not properly operate. As for usability, using session cookie in section IIIA requires valid users to input their login information every time they login to their account. In contrast, users are required to input their login information only once in our method.

Table I: COMPARISON OF THREE PROTECTIVE METHODS

	SectionIII-A Session Cookie	SectionIII-B Cookie Rewriting Technique	Our Method Synchronized State Cookie
Cookie Abuse Prevention Before Expiry	×	*	×
Cookie Abuse Prevention After Expiry	√	*	√
Anti-Replay Attack	×	×	√
Low Latency	√	×	×
Possibility of No Error	√	×	×
Usability	×	√	√

√ : satisfied , × : not satisfied ,

* : Not satisfied against adversaries described in section III-B

VI. CONCLUSION

When a server has XSS vulnerability, an adversary can obtain user’s cookies. To minimize the influence of XSS indirectly, we introduced a method for preventing abuse of stolen cookies. It uses one-time password and challenge-response authentication to judge whether an accessing user is valid or not. With keeping usability, it can prevent the abuse of stolen cookies after their expiry and offers anti-replay attack property. We plan to implement our proposed method and evaluate its feasibility including latency

ACKNOWLEDGMENT

A part of this paper is supported by JSPS A3 Foresight Program.We would like to appreciate the support.

REFERENCES

[1]. Joon S. Park, Ravi Sandhu, Secure Cookies on the Web, 3rd ed. IEEE INTERNET COMPUTING, pp.36-44, JULY - AUGUST 2000.

[2]. Vorapranee Khu-smith, Chris Mitchell, Enhancing the Security of Cookies, ICICS 2001, LNCS 288, pp.132- 145, 2002.

[3]. JNV (Japan Vulnerability Notes) iPedia, CWE-79, Cross Site Scripting, http://jvndb.jvn.jp/ja/cwe/CWE-79.html.

[4]. IPA Security Center, Report on Vulnerability-related Information of Software, http://www.ipa.go.jp/files/000009160.pdf

[5]. D. Kristol, L. Montulli, HTTP State Management Mechanism, IETF Documents IETF Tools, http://tools.ietf.org/html/rfc2965.

[6]. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, ISBN: 0-8493-8523-7, 1997.

Problem Analysis in Concrete Repair and Maintenance of Civil Engineering Structures

Pankaj Parashar[1], Sitender[2], Jasbir[3]

[1,2]*Department of Civil Engineering, Ganga Institute of Technology and Management, Kablana, Jhajjar, Haryana, INDIA*
[3]*Department of Civil Engineering, CBS Group of Institutions, Jhajjar, Haryana, INDIA*

Abstract: This study deals with experimental investigation for finding the causes of distressed concrete and their effects which reduces the load bearing capacity of the structures. The rehabilitation of existing reinforced cement concrete (RCC) bridges and building becomes necessary due to ageing, corrosion of steel reinforcement, defects in construction/design, demand in the increased service loads, and damage in case of seismic events and improvement in the design guidelines. Today, concrete repair is a major industry, supporting the need of virtually every concrete structure. Each structure requires routine repair and maintenance, ranging from simple protective coatings to repair of spalling concrete to strengthening of under-designed components. Developing effective repair strategies requires an understanding of what caused the undesirable behavior. Understanding the cause allows the repair strategy to address both the cause and the effect. The result is successful long lasting repair. The purpose of this study is to present concrete behavior under embedded metal corrosion, disintegration mechanisms, alkali-aggregate reaction (AAR), moisture effects, thermal effects, load effects and faulty workmanship.

Keywords: FRP, GFRP, AAR, RCC, C/D, ASTM, MMA.

I. INTRODUCTION

Sometimes in late 1970's, it finally was recognized that there was a major problem with the infrastructure in United States. In 1970's an alarm signal went off to let us know that more than 60% of our bridges were failing and need some form of repair. There was big uproar and considerable funds were pumped in to promote research and development in fixing them. The first Symposium (1981) on repair, rehabilitation and investigations was held in Mumbai as an attempt to bring talents from the west and east together to discuss the problem of universal nature. The deterioration of civil engineering infrastructures such as buildings, bridge decks, girders, offshore structures, parking structures are mainly due to ageing, poor maintenance, corrosion, exposure to harmful environments. These deteriorated structures cannot take the load for which they are designed. A large number of structures constructed in the past using the older design codes in different parts of the globe are structurally unsafe according to the new design codes and hence need up gradation. Using internally placed moving hinge, external post-tensioned straps, dowel shear devices, drilled hole shear transfer devices, grouted subgrade, cantilever shear arm, installing new expansion joint, section enlargement, shear collars, externally post tensioned reinforcement, bonded steel plates and concrete overlays we can strengthen and stabilized the different types of cracking in the reinforced cement concrete structures. The concrete jacketing also improves the load carrying capacity of the pile foundation of bridges. Portland cement mortar, Portland cement concrete, microsilica modified Portland cement concrete, latex modified Portland cement concrete, polymer modified Portland cement mortar with non-sag fillers, magnesium phosphate cement concrete, epoxy mortar, methylmethacrylate (MMA) concrete and shotcrete may be used as repair and overlay materials.

II. OBJECTIVE OF THE PRESENT WORK

In the light of the literature survey presented above, the following objectives of are identified for the present work: 1) To study the embedded metal corrosion in concrete structures. 2) To study the disintegration mechanism of concrete structures. 3) To investigate the effect of moisture in concrete. 4) To study thermal effects in concrete structures. 5) To study load effects in concrete structures. 6) To study effect of faulty workmanship on concrete structures.

III. TESTING METHODS FOR CONCRETE EVALUATION

A thorough and logical evaluation of the current condition of the structure is the first step of any repair project. Concrete in a structure has a number of functions. Concrete is designed to carry loads. Disfunction of concrete structures usually occurs in some form of visible cracking, leaching, spalling, scaling, stains, disintegration, wear, settlement, or deflection. The evaluation of concrete structures can be either a reactive or proactive process. Concrete evaluation is not limited to studies of its physical conditions, mechanical properties, chemical make-up and external manifestation. Understanding its interaction with the environment is equally important. Any thorough investigation starts with a visual review of condition.

1) Acoustic emission and thermography methods are used for locating delaminated concrete.
2) Corrosion activity can be detected by placing a copper-copper sulfate half-cell and using a voltmeter.
3) Chloride content in concrete can be calculated using chloride analyzer.
4) To determine the depth of carbonation, a solution of phenolphthalein is sprayed over the surface of concrete.
5) Petrographic analysis is used to determine the formation and composition of concrete and to classify its type, condition and serviceability.
6) Impact echo method is a reliable method of locating voids, cracks, honeycomb, and other flaws.
7) Ultrasonic pulse velocity methods may be used to locate voids, cracks, and honeycomb.

8) Fiber optics (borescope), video cameras, and periscopes are the tools that allow for remote viewing inside a structure. Remote viewing technique requires larger drilled holes.
9) The monitoring of cracks can be conducted with various tools including optical comparitors, glued glass strips, glued-in-place crack gauge, electrical transducers, and extensometers.
10) One useful in situ test is pull-off test, which measures the bond between two layers.
11) Rebound hammer method is used to measure the surface hardness of concrete.

TABLE 1: Standard Test Methods for Evaluating Concrete

S. No.	Designation	Title
1	ASTM C 42	Obtaining and testing drilled cores and sawed beam of concrete
2	ASTM C 805	Rebound number of hardened concrete
3	ASTM C 803	Penetration resistance of hardened concrete
4	ASTM C 597	Pulse velocity through concrete
5	ASTM C 496	Splitting tensile strength of cylindrical concrete
6	ASTM C 78	Flexural strength of concrete (with third-point loading)
7	ASTM C 293	Flexural strength of concrete (with center-point loading)
8	ASTM C 418	Abrasion resistance of concrete by sandblasting
9	ASTM C 876	Half cell potentials of uncoated reinforcing steel in concrete
10	ASTM D 3633	Electrical resistivity of Membrane-Pavement System
11	ASTM C 856	Standard practice for petrographic examination of hardened concrete
12	AASHTO T 259	Resistance of concrete to chloride ion penetration
13	AASHTO T 260	Sampling and testing for total chloride ions in concrete
14	AASHTO T 277	Rapid determination of the chloride permeability of concrete
15	ASTM C 457	Microscopial determination of parameters of the air void system in hardened concrete
16	ASTM C 666	Resistance of concrete to rapid freezing and thawing
17	ASTM C 671	Critical dilation of concrete specimens subjected to freezing

IV. REPAIR MATERIALS AND PLACEMENT METHODS

Different kinds of defect, repair methods and materials are explained in the table below:

TABLE 2: Repair Materials and Placement Method

Defects	Repair Methods	Materials
• Live Cracks	- Caulking - Pressure injection with ‘flexible’ filler - Jacketing: * Strapping * Overlaying - Strengthening	Elastromeric sealer ‘Flexible’ epoxy filler Steel wire or rod Membrane or special mortar Steel plate, post tensioning, stitching, etc
• Dormant Cracks	- Caulking - Pressure injection with ‘rigid’ filler - Coating - Overlying - Grinding and Overlay - Dry-pack - Shotcrete/Gunite - Patching - Jacketing - Strengthening - Reconstruction	Cement grout or mortar, Fast-setting mortar. ‘Rigid’ epoxy filler Bituminous coating, tar Asphalt overlay with membrane Latex modified concrete, highly dense concrete Dry-pack Mortar, Fast-setting mortar Cement mortar, Epoxy or Polymer concrete Steel rod Post tensioning, etc.
• Voids • Hollows and • Honeycombs	- Dry pack - Patching - Resurfacing - Shotcrete/Gunite - Preplaced aggregate - Replacement	Dry-pack Portland cement grout, mortar, cement Epoxy or Polymer concrete Fast-setting mortar Coarse aggregate and grout as

		needed
• Scaling Damage	- Overlaying - Grinding - Shotcrete/Gunite - Coating - Replacement	Portland cement concrete, Latex modified concrete, Asphalt cement, Epoxy or polymer concrete Fast-setting mortar, Cement mortar Bituminous, Linseed oil coat, Silane treatment as needed
• Spalling Damage	- Patching - Shotcrete/Gunite - Overlay - Coating - Replacement	Concrete, Epoxy, Polymer, Latex, Asphalt Cement mortar, Fast-setting mortar Latex modified concrete, Asphalt concrete, Concrete Bituminous, linseed oil, Silane, etc. as needed

V. CONCLUSION

In this experimental investigation the causes and effects of undesirable behavior of concrete members are studied. The test results illustrated in the present study showed that the external strengthening with GFRP composites can be used to increase the shear capacity of RCC structures, but the efficiency varies depending on the test variables such as fiber orientations, wrapping schemes, number of layers and anchorage scheme.

Based on the experimental and theoretical results, the following conclusions are drawn:

1) The pH of newly produced concrete is usually between 12 and 13.

2) In good quality concrete the corrosion rate will be very slow.

3) Accelerated corrosion will take place if the pH is lowered.

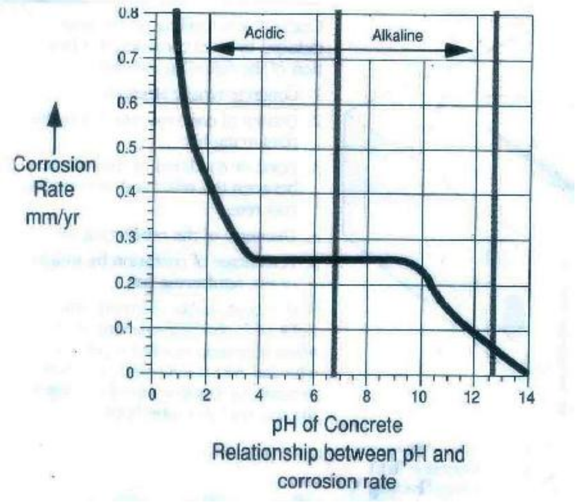
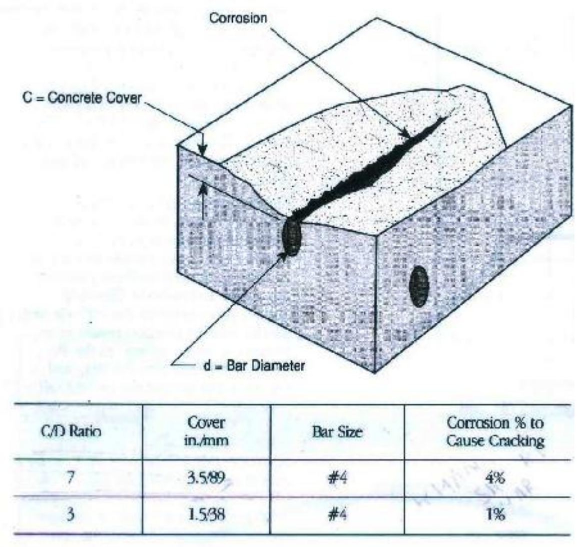


Fig. 1 Embedded Metal Corrosion Process

4) With a cover-to-bar diameter ratio (C/D) of 7, concrete cracking starts when corrosion reaches 4 percent.



C/D Ratio	Cover in./mm	Bar Size	Corrosion % to Cause Cracking
7	3.5/89	#4	4%
3	1.5/38	#4	1%

Fig. 2 Corrosion Induced Cracking and Spalling

5) With a cover-to-bar diameter ratio (C/D) of 3, concrete cracking starts when corrosion reaches 1 percent.

6) The research conducted on flexural beams found that in steel more than 1.5 percent corrosion, the ultimate load capacity began to fall, and at 4.5 percent corrosion, the ultimate load was reduced by 12 percent .

7) It was demonstrated that a threshold level of 8000 ppm of chloride ions was required to initiate corrosion when the pH was 13.2 and when pH was lowered to11.6, corrosion was initiated with only 71 ppm of chloride ions.

8)Carbonation will not occur when concrete is constantly under water .

9) Normal weight concrete shrinks from 400 to 800 microstrains.

10) A change of 38° C in a 30.5m length will change the overall length by 22mm.

11) A precast double T-shaped structured member with a 18m span can move 19mm upward at midspan from normal diurnal solar heating, causing the ends to rotate and stress the ledger beam bearing pads and concrete.

12) Hinges open and close with daily temperature changes.

13) The cement mortar converts to quicklime at temperature of 400° C , thereby causing disintegration of the concrete.

14) High slump mixes, incorrect methods of handling concrete, and over-vibration are the causes of segregation.

VI. FUTURE SCOPE

Perhaps in the years to come, we may be able to reduce the large expenses involved in repairs and rehabilitation of our structures and change the public image of our profession. Based on the finding and conclusions of the current study the following recommendations are made for future research in FRP shear strengthening:

1) Strengthening of RCC bridges under IRC loading.

2) Strengthening of existing residential building without interrupting residents.

3) Strengthening of columns using jacketing same as in pile foundation.

4) Strengthening of flexure member using external bonded steel plates at lower cost.

5) To lower the final cost of repair of existing buildings.

6) To improve the asthetic conditions of the bridges, T-beams and existing buildings.

7) FRP strengthening of RC T-beams with different types of fibers such as carbon, aramid & basalt.

8) Study of bond mechanism between CFRP, AFRP and BFRP and concrete substrate.

9) Strengthening of RC L-beams with FRP composite.

10) Strengthening of RC L-section beams with web opening.

11) Effects of web openings of different shape and size on the shear behavior of T & L-beams.

12) Effects of shear span to depth ratio on shear strengthening of beams.

13) Numerical modelling of RC T & L-beams strengthened with FRP sheets anchored at the end.

REFERENCES

[1] Clifton, J.R, Predicting the Remaining Service Life of concrete, National Institute of Standards and technology Report NISTIR 4712.

[2] Bousselham A., and Chaallal O. (2006), “Behaviour of Reinforced Concrete T-beams strengthened in shear with carbon fiber-reinforced polymer – An Experimental Study”, ACI Structural Journal, Vol. 103, No. 3, 339-347

[3] M.A. Shahawy, M. Arockiasamy, T. Beitelman, R. Sowrirajan “Reinforced concrete rectangular beams strengthened with CFRP laminates” Composites: Part B 27B (1996) 225-233

[4] Victor N. Kaliakin, Michael J. Chajes and Ted F. Januszka “Analysis of concrete beams reinforced with externally bonded woven composite fabrics” Composites: Part B 27B (1996) 235-244

[5] Koji Takeda, Yoshiyuki Mitsui, Kiyoshi Murakami, Hiromichi Sakai and Moriyasu Nakamura “Flexural behaviour of reinforced concrete beams strengthened with carbon fibre sheets” Composites: Part A 27A (1996) 981-987

[6] Ahmed Khalifa, Antonio Nanni “Improving shear capacity of existing RC T-section beams using CFRP composites” Cement & Concrete Composites 22 (2000) 165-174

[7] Thanasis C. Triantafillou and Costas P. Antonopoulos “Design of concrete flexural members strengthened in shear with FRP” Journal of Composites for Construction, Vol. 4, No. 4, November, 2000. 198-205

[8] Hausmann, D. A, Steel Corrosion in Concrete Material Protection, November 1967, pp. 12-23.

[9] Sergio F. Brena, Regan M. Bramblett, Sharon L. Wood and Michael E. Kreger “Increasing Flexural Capacity of Reinforced Concrete Beam Using Carbon Fiber Reinforced Polymer Composites” ACI Structural Journal/January-February 2003. 36-46

[10]Bimal Babu Adhikary, Hiroshi Mutsuyoshi, and Muhammad Ashraf “Shear Strengthening of Reinforced Concrete Beams Usmaing Fiber-Reinforced Polymer Sheets with Bonded Anchorage” ACI Structural Journal/September-October 2004. 660-668

[11] Vaysburd, A. M., Sabnis, G. M and Sorokko, R., Theoretical Aspects and Testing Methods of Concrete Carbonation, Proceedings, International Conference on Life Prediction of Corrodible Structures, Hawaii, 1991, pp. 34/1-34/16

[12] American Concrete Institute, SP-102, Steel Corrosion in Concrete: Cause and Restraints, Detroit, 1987.

[13] ACI 201.2R-77, Guide to Durable Concrete.

[14] ACI 318-83, Corrosion of Metals in Concrete.

[15] Chloride Corrosion of Steel in Concrete, ASTM STP 627, American Society for Testing and Materials, Philadelphia, PA, 1977.

[16] Peter H. Emmons and Gajanan M. Sabnis, “Concrete Repair and Maintenance”, Galgotia Publication, 2012.

[17] L.J. Li, Y.C. Guo, F. Lui, J.H. Bungey “An experimental and numerical study of the effect of thickness and length of CFRP on performance of repaired reinforced concrete beams” Construction and Building Materials 20 (2006) 901-909

[18]Yung Chih Wang, Kai Hsu “Design recommendations for the strengthening of reinforced concrete beams with externally bonded composites plates” Composite Structures Articles in press. [16] IS: 456-2000, “Plain and Reinforced Concrete – Code of Practice”, Bureau of Indian Standards.

[19] Al-Sulaimani, Kaleemullah, Basunbal and Rasheed , “Influence of Corrosion and Cracking on Bond Behaviour and strength of Reinforced Concrete Members,” ACI Structural Journal, March-April 1990, p220.

Author Profile

Pankaj parashar B.Tech., M. Tech. Scholar in Civil Engineering (Structural Design) from Ganga Institute of Technology and Management, Kablana, Jhajjar, Haryana (India) affiliated to Maharshi Dayanand University, Rohtak, Haryana (India).