3rd National Conference on

ITBT'15

INFORMATION TECHNOLOGY for BUSINESS TRANSFORMATION

20th & 21st March, 2015

Technical Sponsors

in association with

IEEE Computer Society Delhi Section

Computer Society of India Ghaziabad Chapter

Ghaziabad Management Association

Editors

Prof. R.P Saw
Dr. Anu Chaudhary
Mr. J.K Seth

Organised by

AJAY KUMAR GARG ENGINEERING COLLEGE

AKGEC

AJAY KUMAR GARG ENGINEERING COLLEGE

Ghaziabad, Uttar Pradesh

ITBT'15

3rd National Conference
on
INFORMATION TECHNOLOGY
for BUSINESS TRANSFORMATION

20th & 21st March, 2015

Editors

Prof. R.P Saw
Dr. Anu Chaudhary
Mr. J.K Seth

Organised by

AJAY KUMAR GARG ENGINEERING COLLEGE
Ghaziabad, Uttar Pradesh

Technical Sponsors

IEEE Computer Society
Delhi Section

Computer Society of India
Ghaziabad Chapter

in association with

Ghaziabad Management
Association

CHIEF PATRON

Dr. R.K. Agarwal
Director, AKGEC

PATRONS

Prof. M.P. Dave
M.Tech Coordinator

Prof. P.K. Chopra
HoD ECE

Prof. I.P. Sharma
HoD ME

Prof. S.L. Kapoor
HoD MCA

Prof. B.M. Kalra
HoD CSE

Prof. V.K. Parashar
HoD EN

Prof. P.K. Sharda
HoD AS&H

Prof. B.B. Prasad
HoD Civil Engg.

ORGANISING COMMITTEE

Prof. R.P Saw
Convener

Prof. Ashiv Shah
Co-Convener

Ms. Anupama Sharma
Member

Mr. Sumit Sharama
Member

Mr. Narendra Kr. Tewatia
Member

Dr. Anu Chaudhary
Co-Convener

Mr. J.K. Seth
Member

Mr. Ruchin Gupta
Member

Mr. Pancham Singh
Member

Ms. Yogita Chhabra
Member

TECHNICAL & ADVISORY COMMITTEE

Prof. R.C Joshi
Chancellor, Graphic Era University

Mr. Daman Dev Sood
IEEE Delhi Section

Prof. Bhim Singh
IIT, Delhi

Mr. Saurabh Agrawal
Chairman CSI, Ghaziabad Chapter

Dr. Arun Sharma
Asocc Prof- IGDTUW and
Vice Chairman- CSI Ghaziabad Chapter

Dr. Satish Chandra
JIIT, Noida

Dr. Rajesh Tyagi
JIMS, Noida

Dr. Deepak Garg
Secretary, IEEE Computer Society

Dr. D.K. Lobiyal
JNU, New Delhi

Dr. D.P. Vidyarthi
JNU, New Delhi

Dr. Emmanuel S. Pilli
NIT, Jaipur

Mr. Anil Ji Garg
Enterpreneur and Hony Secretary
-CSI Ghaziabad Chapter

Dr. Satish Peddoju
HoD MCA

Dr. Maitreyee Dutta
NITTTR, Chandigarh

Contents

Session – 1

Session – 2

16. Security on Mobile Agent Based Web Crawlers
Manisha Singh Raghav, Dev Gupta, Ayushi Chaudhary

17. Emperical Validation of OO Metrics for Change Proneness Prediction Using Open Source Software Systems
Anushree Agrawal

18. Analysis and Performance Evaluation of MPLS Network over Conventional IP Network
Shilpi Garg, Dr. Anu Chaudhary

19. A Review Paper on Data Mining Techniques and its Applications
Mohammad Aamir, Prashant Kamal Mishra, Shivangi Garg

20. Theory on Age Invariant Face Recognition System
Aman Kumar

21. Analysis of Wormhole Attack in AODV based MANET using OPNET SIMULATOR
Achint Gupta, Mohit Khandelwal

22. AVANT-GARDE CPU SCHEDULING ALGORITHM
Priyam Maheshwari, Akanksha Saxena, Shivesh Gupta

Session – 3

23. Improving Hadoop MapReduce Performance by Optimizing Programs and Configuration
Ajay Mohan Verma

24. An Approach – TURN TOUCH
Shikha Jain, Bhawna Sachdeva

25. Survey on Large Scale Networks based on Software Defined Networking (SDNs)
Sumit Sharma

26. Performance Enhancement through Adaptive Queue Management in MMDSR for MANET
Anupama Sharma, Abhay Bansal, Vinay Rishiwal

27. Artificial Neural Networks for Pattern Recognition
Parul Gupta, Rashi Tyagi

28. Face recognition an application of Artificial Neural Network and its solution
Rupal Grover, Ritu Nigam

29. Accuracy Evaluation of Recommender System Models
Vidushi, Rahul Dagar

30. Hierarchical Routing Protocols in Wireless Sensor Networks : A Survey
Tahira Mazumder, Sushruta Mishra

31. Video Analytics using Hadoop and MapReduce
Satyam Agrawal , Saurabh Tripathi, Shivam Agrawal, Ankur Tripathi

Application Of Genetic Programming

An application to symbolic regression

Ms. Shailee Lohmor
Bharathiar University, Coimbatore, India
shailee.mrce@mrei.ac.in

Dr. B B Sagar
Birla Institute of Technology, Mesra- Ranchi, India
drbbsagar@gmail.com

Abstract **- Genetic programming deals with parse tree (a diagrammatic representation of the parsed structure of a sentence or string) of symbols and operators. The symbols may be variables or constants while the operators are basic mathematical operators. This parse tree can be processed to generate a expression or a program which serve a required purpose or is near to the desired purpose .The basic set of GP operation are crossover, selection, mutation etc .The paper broadly divided into four sections. Section I is the introduction the genetic programming, section II consisting of Genetic programming terminology section III correspond to Genetic programming based for symbolic regression, while section IV is Experimentation and section V shows the result obtained.**

Keywords—Genetic Algorithm, Genetic Programming

INTRODUCTION

Prior genetic programming, genetic algorithm was popular optimization technique. Limitation of genetic algorithm like fixed length chromosome and syntax free approach does not make it suitable for applicable for program generation. Genetic programming follow regression methodology where in a relationship among variables is used to reach to a concluding parse tree. Following is basic GP algorithm.

The Basic terminologies used to understand the basic GP algorithm are

- **The terminal set**[1]: A set of input variables or constants.
- **The Operator set**[1]: A set of domain specific functions used in conjunction with the terminal set to construct potential solutions to a given problem. For symbolic regression this could consist of a set of basic mathematical functions, while Boolean and conditional operators could be included for classification problems.

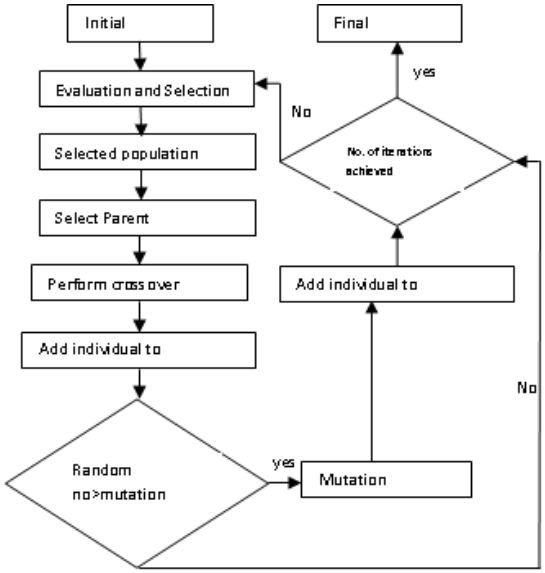


Figure1: Basic GP Algorithm

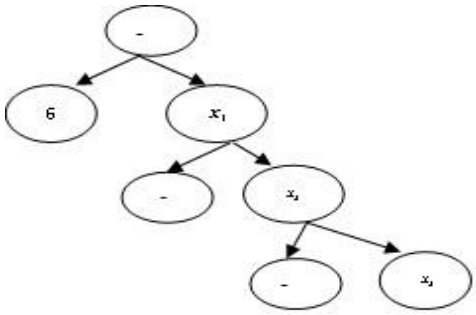
II. Basic Terminology

- **The fitness function**: Fitness is a numeric value assigned to each member of a population to provide a measure of the appropriateness of a solution to the problem in question.
- The algorithm **control parameters**[2]: This includes
  - **Population size**: A larger population allows for a greater exploration of the problem space at each generation and increases the chance of evolving a solution. In general, the more complex a problem the greater the population size needed.

Maximum number of generations: The evolutionary process needs to be given time; the greater the maximum number of generations the greater the chance of evolving a solution. However, further evolution of a population does not guarantee a solution will be found—it may be better to start again with a different initial population. So if, after a user-defined number of generations, a sufficiently successful individual has not evolved then the process should halt.

III. Genetic Programming: Symbolic Regression

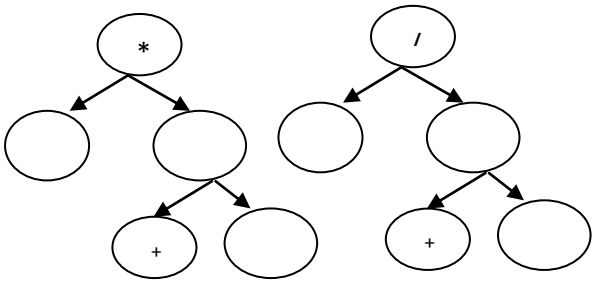
Like Genetic algorithm, chromosomes do occur in Genetic Programming too, with a difference that chromosome is a tree consisting of symbols which may be terminals/constants and operators. The genotype is the here is the tree while phenotype is the solution that correspond to the expression generated after parsing the tree. For our example the tree which could be formed is



The symbols that are taken for our problem are operator set {'+','-','*','/'} and terminals { , },thus these are used to generate a tree. The following are the steps in genetic Programming:

A. Population Initialization

The population is initialized with random generation of tree of depth provided with maximum of 2^{depth} -1 node. The sample individual consists of a tree and fitness value assigned, which is 0 for during initialization. Some of the random individual tree may be

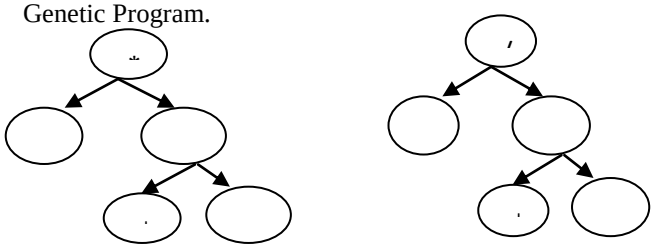


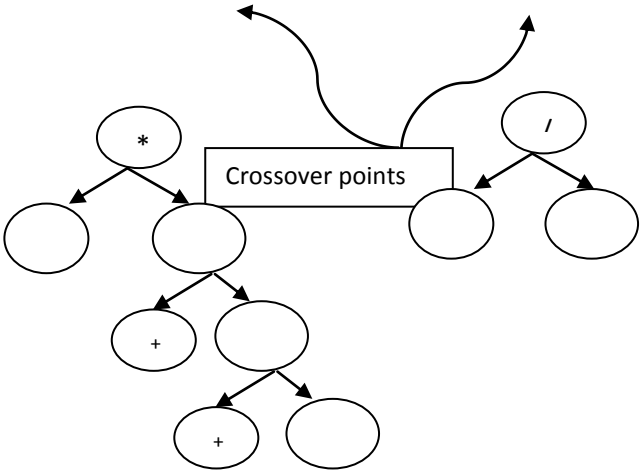
B. Population evaluation

The Population is then evaluated by parsing the tree. During parsing the generates an expression which is evaluated for the given set of input domain which results in the fitness value for each individual of population .For example above tree generates expression and .

C. Cross Over

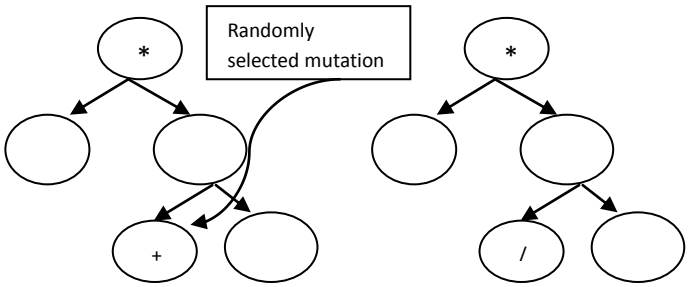
Cross over in a tree could a single point or multipoint as case of genetic algorithm, difference lies in the chromosome length, which is variable in case of Genetic Program.





D. Mutation

Mutation is a chance change of a operator/terminal in the individual chromosome. The node modified is replaced with the symbol of similar kind i.e. operator is replaced with a element from operator set and terminal node from a terminal set.



E. Selection

Selection is based on fitness value which is reevaluated once a crossover and/or a mutation is made to the individual. The selection method varied from roulette, tournament, stochastic uniform, uniform. The experimentation performed uses roulette selection where fitness value is associated with a probability factor.

The above steps B, C, D, E are repeated for number for iteration.

EXPERIMENT

The Experimentation was done using MATLAB where Genetic algorithm was coded fully, while genetic Programming used GPols tool of MATLAB. There were certain changes made in the m-files of tool to fit into the requirement to solve the quadratic equation. Bound is being used to set the range of the input variables [-2, 3] [-2, 4] and [-1, 1] for both the approaches.

Gpols tool is a Genetic programming tool with some inbuilt m files for handling tree which is the basic requirement to perform genetic programming. However

some m-files were modified in order to evaluate a quadratic equation and to produce MSE.

Mean square error (MSE) is used as a approximation for correctness of the result produced. MSE is average of the square of the difference between the desired response and the actual system output (the error).The lesser the value of MSE the more the result is appropriate.

The experiment here started with generation of random value set for X .The values set produced for are in range as discussed before, which are input to the equation thus giving a set of desired output.

Once done with it operator set {'+','-','*','/'} and terminal set { } are defined. The above set is used to generate tree for initial population. The tree produced has above symbols as node in some random manner, with mean square error and fitness value equal to 0.The evaluation starts with parsing of tree and generating an expression which is evaluated. The evaluated expression is fed with the same set of input variable set produced at the starting of experimentation and actual result is produced.

MSE is calculated for each individual of the population. Fitness value is calculated on the basis of correlation [3] coefficients, which demonstrate how closely two values are related. MATLAB provide a inbuilt function corrcoef (actual value, desired value), whose value lies between 0 and 1 where 1 says they match exactly and 0 vice versa.

Once we have fitness value for each individual in the population, section (roulette in our case) can be applied to get the best individual for cross over and/or mutation. Crossover and mutation phenomenon occurs in accordance to concept discussed earlier. The process of selection, cross over and/or mutation repeats

RESULTS

The following is the table showing various parameters used, which are common in both our approach

Entity	Value
population size	10
Selection Mode	Roulette
No. of iteration	20
Cross over	Single point
Mutation rate	0.05

Table 1:

In Figure2, the graphs generated using genetic programming. It is clearly visible from the graph as with each iteration correlation between the desired value and actual values increases which demonstrates the fit individual with time. It may also be noticed that mean square error which is the measure of closeness to the result is just compliment of fitness value/iteration graph, which make it clear that lesser the MSE value the more optimized the result is

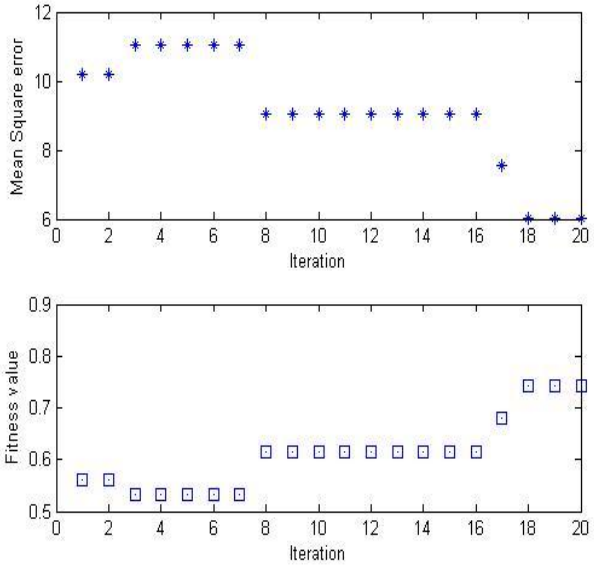


Figure 2 : Graphs generated using GP

Future Scope

- **Document Images Segmentation and Classification** [1]: In computer vision, **image segmentation** is the process of partitioning a digital image into multiple segments (sets of pixels, also known as superpixels). The goal of segmentation is to simplify and/or change the representation of an image into something that is more meaningful and easier to analyze.
- **Automatic Programming** [2]: Genetic programming (GP) is an evolutionary algorithm which explores a program space rather than a solution space which is typical of other evolutionary algorithms such as genetic algorithms. GP finds solutions to problems by evolving a program, which when implemented will produce a solution.
- **Software Reliabilty growth modeling** [3] :Reliability models are very useful to estimate the probability of the software fail along the time. Several different models have been proposed to estimate the reliability growth, however, none of them has proven to perform well considering different project characteristics. In this work, we explore genetic programming (GP) as an alternative approach to derive these models. GP is a powerful machine learning technique based on the idea of genetic algorithms and has been acknowledged as a very suitable technique for regression problems.

References

[1] M.J. Willis*, H.G Hiden*, P. Marenbach+, B. McKay* and G.A. Montague* Genetic Programming: An Introduction And Survey Of Applications

[2] Gray, J., Murry-Smith, D.J., Yun, L. and Sharman, K.C., (1996b), 'Nonlinear model structure identificationusing genetic programming', Late Breaking Papers at the Genetic Programming 1996 Conference, Koza, J.R (ed.), Stanford University Bookstore, USA, pp.32-37.

[3] Enrique F Schisterman, Kirsten B Moysich, Lucinda J England and Malla Rao Estimation of the correlation coefficient using the Bayesian Approach and its applications for epidemiologic research, *BMC Medical Research Methodology* 2003, **3**:5 doi:10.1186/1471-2288-3-5

[4] Mulholland H., Tapamo J. R. and Pillay

N., Evolutionary Methods for Document Images

Segmentation and Classification, in proceedings of

PRASA 2006, 29 Nov-1 Dec 2006, Parys, South Africa,96-102.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892,pp.68-73.

[5] Igwe, K., Pillay, N. Automatic Programming Using Genetic Programming, in proceedings of proceedings of WICT 2013 (Nature Inspired Algorithms and their Applications Track), Hanoi, Vietnam, December 2013, 339-344, IEEE Press.K. Elissa, "Title of paper if known," unpublished.

[6] Costa, E.O. ; Dept. of Comput. Sci., Fed. Univ. of Parana, Curitiba ; Vergilio, S.R. ; Pozo, A. ; Souza, G.ISSRE 2005. 16th IEEE International Symposium on Software Reliability Engineering

Offline Signature Verification Using Chain Code and Wavelet Feature and Verification Method

Vimal Dwivedi
CDAC, Noida
vimal.bncet@gmail.com

Tushar Patnaik
CDAC, Noida
tusharpatnaik@cdac.in

Abstract - **Signature verification is a topic which is being discussed among the researchers for long time .Off-line signature data is 2-D image representation. Offline signature verification is a process of verifying the signature on the basis of feature of signature either it is genuine or forged. The purpose of Offline Signature Verification is to authenticated signature. A robust system has to be designed which should also detect various types of forgeries .The system should neither be too sensitive nor too coarse. It should have an acceptable trade-off between a low False Acceptance Rate (FAR) and a low False Rejection Rate (FRR). So we present a new approach which yields more accurate result as compared to the already existing algorithms. The application of Offline Signature Verification is to identity theft, signature in retail, banking etc.**

The Algorithms are based on the chain code and Wavelet feature which are called as Feature points in our thesis. As Feature points increases results will be more accurate but complexity and time require for testing will be more. So we have taken 64 feature points which improves security and maintains same complexity level. All calculations are done on the basis of these feature points. Results are expressed in terms of FAR (False Acceptance Rate) and FRR (False Rejection Rate) and subsequently compare these results with other existing Techniques. Results obtained by this algorithm are quite impressive. Random and Simple forgeries are eliminated and skilled forgeries are also eliminated in greater extent. As signature image is tested rigorously so FRR is more in the Algorithm proposed by us.

Processing Off-line is complex due to the absence of stable dynamic characteristics. Difficulty also lies in the fact that it is hard to segment signature strokes due to highly stylish and unconventional writing styles. The non-repetitive nature of variation of the signatures, because of age, illness, geographic location and perhaps to some extent the emotional state of the person, accentuates the problem. All these coupled together cause large intra-personal variation.

Keywords- Chain code histogram, wavelet feature, FAR, FRR, SVM

INTRODUCTION

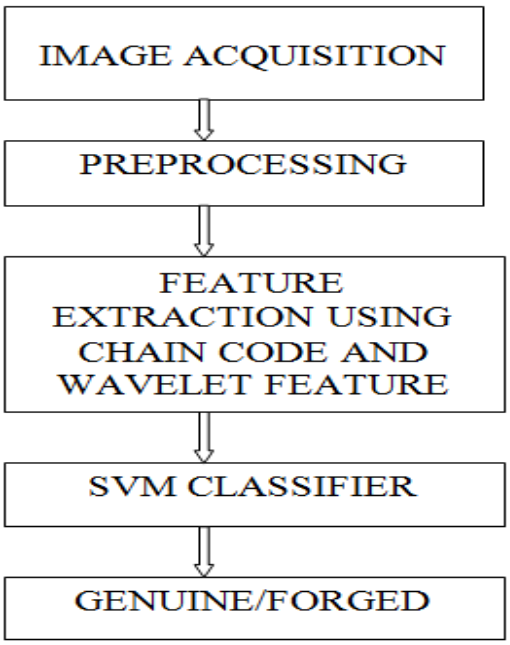
The objective of the signature verification system is to discriminate between two classes: the original and the forgery, which are related to intra and interpersonal variability. The variation among signatures of same person is called Intra Personal Variation. The variation between originals and forgeries is called Inter Personal Variation. Signature verification is so different with the character recognition, because signature is often unreadable, and it seems it is just an image with some particular curves that represent the writing style of the person.

Signature is just a special case of handwriting and often is just a symbol. So it is wisdom and necessary to just deal with a signature as a complete image with special distribution of pixels and representing a particular writing style and not as a collection of letters and words. A signature verification system and the techniques using to solve this problem can be divided into two classes: online and off-line. In an online system, a signature data can be obtained from an electronic tablet and in this case, dynamic information about writing activity such as speed of writing, pressure applied, and number of strokes is available. In off-line systems, signatures written on

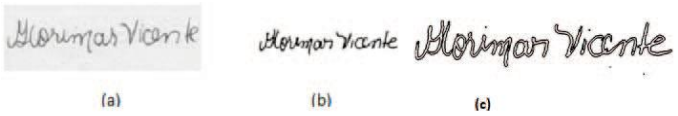
paper as has been done traditionally are converted to electronic form with the help of a camera or a scanner and obviously, the dynamic information is not available. In general, the dynamic information represents the main writing style of a person. Since the volume of information available is less, the signature verification using off-line techniques is relatively more difficult. Our work is concerned with the techniques of off-line signature verification. The static information derived in an off-line signature verification system may be global, structural, geometric or statistical. This paper is divided into four sections. Section II describes proposed method; Section III describes Test result and Section IV describes conclusion of a approach.

PROPOSED METHOD

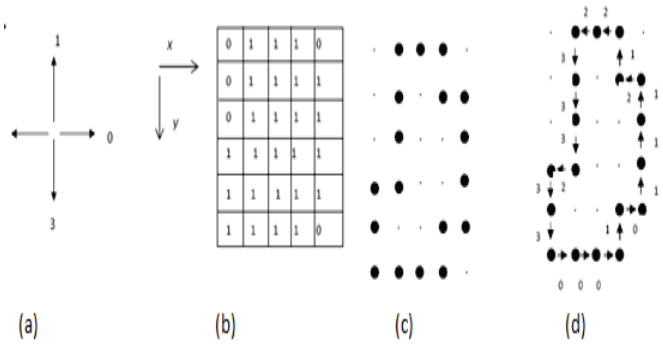
As more and more number of scanned signature increases, the existing technique does not work correctly means the accuracy of system decreases. Hence we require fast and more accurate signature verification technique which improves verification problem when number of signature increases. Most of the scanned signature after feature extraction, suffers from various types problem such as accurate classification, hence we used here SVM for accurate classification. Basic steps in this approach are



1. The first step of proposed approach is to get scanned image from scanned devices.
2. Preprocessing is a next step is used for removing noisy image to get final image for feature extraction.



3. We will apply wavelet feature with chain code feature which improves best signature pattern result.



Chain code feature of image2(c)

Global and local wavelet features are extracted from the image. The procedure employed in this stage is described in the following steps. First- the global features such as height, width and area are extracted from whole image. Second- DWT (Discrete Wavelet Transform) is applied on signature image and maximum vertical projection position and maximum horizontal projection position features are extracted from each of the three sub images.
4. Next step is to classify nature of signature with using Support Vector Machine which tells us either it is genuine or forged signature. The SVM classifier is widely used in bioinformatics (and other disciplines) due to its high accuracy, ability to deal with high-dimensional data such as gene expression, and edibility in modeling diverse sources of data. SVMs belong to the general category of kernel methods; a kernel method is an algorithm that depends on the data only through dot-products. When this is the case, the dot product can be replaced by a kernel function which computes a dot product in some possibly high dimensional feature space. This has two advantages: First, the ability to generate non-linear decision boundaries using methods designed for linear classifiers.

5. The comparison will also be drawn between proposed and the available methods by the use of following parameters:

a. FAR (false acceptance rate)
b. FRR (false rejection rate)

FAR-Actually, it is defined as the ratio of the no. of feature acceptances divided by the no. of identifications attempts. FRR-Actually it is defined as the ratio of the no. of false rejections identifications attempts.

TEST RESULTS

A database of about 130 signatures with 7 signatures per person was used for training. The signatures were scanned with a precision of 200 dpi. It was found experimentally that a value of 0.75 for γ gave good results. We used a threshold value of 1.5 for the distanceδ.

Publication	Extracted Feature	Verification Method	performance
Offline Signature Verification by using Pixel based Method	Chain code and Wavelet Feature	SVM	FRR-High FAR-Low
Off-line Signature Verification Using Contour Features	Length based and direction based	Euclidean distance based	EER-6.44%
A Multi-Hypothesis Approach for Off-Line Signature Verification with HMMs	States of signature	HMM	EER-4.9%
Fusion Of Static Image And Dynamic Information For Signature Verification	Contour Feature	Euclidean distance based	EER-0%

CONCLUSION

The algorithm uses simple wavelet and chain code features to characterize signatures that effectively serve to distinguish signatures of different persons. The system is robust and can detect random, simple and semi-skilled forgeries but the performance deteriorates in case of skilled forgeries. A larger database can reduce false acceptances as well as false rejections. Using a higher dimensional feature space and also incorporating dynamic information gathered during the time of signature can also improve the performance.

Our algorithm takes 64 feature points for threshold calculations, a small variation of a signature results in a large change in the values of threshold distance from the geometric center. Therefore in our algorithm the FRR value will not increased. So it is important for a user to sign his signature with utmost care so that there is not a large variation of his signature to his training signatures. Otherwise there is a probability of rejection of an original signature.

References

[1] R.K. Bharathi, B.H. Shekar "Off-line Signature Verification Based on Chain Code Histogram and Support Vector Machine" International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp 2063 – 2068, 2013

[2] *Urmila A.Jain,Nitin N.Patil* "A Comparative Study of Various Method for Offline Signature Verification", International Conference Issues and Challenges in Intelligent Computing Techniques (ICICT) , pp 760 – 764, 2014

[3] Amit Kishor Shukla, Pulkit Mohan, Gaurav Ojha, Manoj Wariya "Offline Signature Verification using Grid and Tree based Feature Extraction Machine" Issues and Challenges in Intelligent computing tech.(ICICT), IEEE@2014

[4] *S.A Angadi,Smita Gour* "Offline Signature Verification using Global and Local Wavelet "Signal and Image Processing(ICSIP),IEEE@2014

[5] Vaibhav Shah, Umang Sanghavi, Udit shah"Off-line Signature Verification Using Curve Fitting Algorithm with Neural Networks Machine" Advanced in Technology and Engineering(ICATE) IEEE@2013

[6] *K.N Pusplata,A,k Gautam* "Offline Signature Verification using Directional and Textural Feature"Circuit,Control and Communication(CCUBE) IEEE**@**2013

Cryptanalysis of Pass-Icons in 3d password authentication system

Vaishali Jain
IEC-College of Engineering & Technology
Greater Noida, U.P., INDIA
iamvaishalijain@gmail.com

Abstract **- As computing becomes pervasive, people increasingly rely on public computers to do business over the internet. Accessing today's web based services invariably requires typing a username and password to authenticate .Many authentication schemes has been used in the past such as textual password, graphical password, biometrics etc. 3D password is a multifactor and multi-password authentication scheme that combines two or more authentication schemes in one scheme. In this the user is presented with a 3D virtual environment where it navigates and interacts with the objects. 3D password is constructed by observing the actions and interactions by the users and by observing the sequence of such actions. This multifactor authentication scheme provides unlimited password possibility but shoulder surfing attack is possible in this scheme. In this paper, i have described the use of pass-icons in Convex Hull Scheme as countermeasure to shoulder-surfing attack in 3D password scheme.**

Keywords - Password, 3DPassword, Shoulder Surfing Attack, Convex Hull Click Scheme, Pass-icons

INTRODUCTION

Password is the mean to provide authentication which is the process of validating who you are to whom you claimed to be in any system. Password relies on two basic conflicting requirements as shown in fig below.

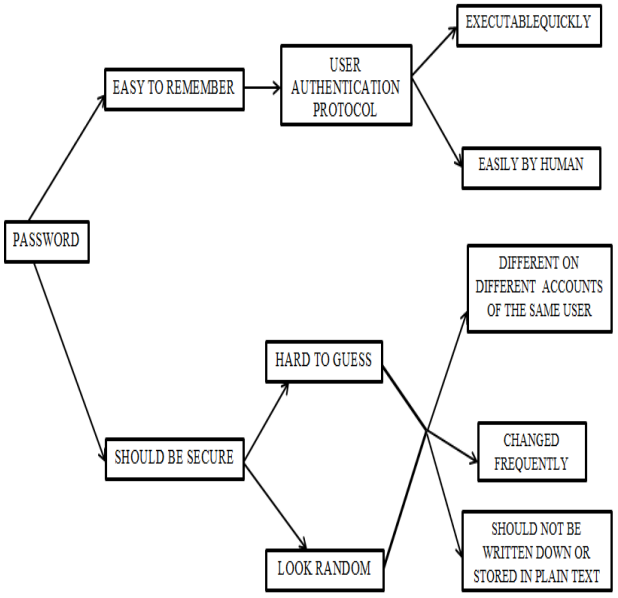


Fig.1.1. Password Requirements

To overcome the vulnerabilities of single factor authentication technique, a multifactor and multi-password authentication technique is used which is called as "3D Password Authentication Scheme". 3D password scheme is based on combination of recall and recognition based authentication techniques as well as biometrics and many other schemes. As recall based techniques requires the user to repeat or reproduce a secret that the user created before [2] [5] [7] [9]and recognition based technique requires the user to identify and recognize the secret, or part of it, that it has selected before [2] [5] [7] [9]. When these two techniques are combined to create 3D password, the user is presented with a virtual environment consisting of various virtual objects through which user interacts with. The interaction with 3D environment changes as per user changes and the

sequence of such actions is observed while constructing 3D password.

3D PASSWORD

3D password authentication scheme is a multifactor and multi-password authentication scheme which combines the benefits of two or more authentication scheme in one scheme. It is multifactor as it is a combination of more than one scheme and multi-password because multiple passwords can be created by combining two or more schemes such as textual and graphical authentication scheme.

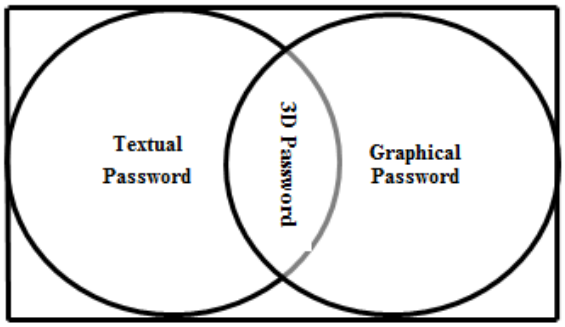


Fig.2.1. 3D Password (Multifactor and Multi-Password Authentication Scheme)

For creating 3D password a new virtual environment is introduced which is known as 3D virtual environment which consists of several virtual objects where user navigates based on the schemes which user chooses(Textual and Graphical). Biometrics is not chosen here because inclusion of biometrics may lead to several vulnerabilities in 3D password system such as hardware cost is more which increase the cost of overall system and biometrics is vulnerable to some attacks which decrease the efficiency and security of 3D password system. 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 3-D environment toward the virtual objects. The 3-D password is simply the combination and the sequence of user interactions that occur in the 3-D virtual environment

A. Objectives of 3D Password Scheme

1) To provide more secure authentication technique than existing one.
2) To design & develop more user friendly & easier authentication scheme and giving user to freedom of selecting more than one password scheme as single system.
3) To overcome the drawbacks & limitations of previously existing systems (textual password, graphical password etc.).
4) New scheme should be combination of recall-, recognition, biometrics, and token based authentication schemes.

B. 3D Password System Design

Designing a well-studied 3-D virtual environment affects the usability, effectiveness, and acceptability of a 3-D password system. Therefore, the first step in building a 3-D password system is to design a 3-D environment that reflects the administration needs and the security requirements. The design of 3-D virtual environments should follow guidelines such as real-life similarity, object uniqueness and distinction, 3D virtual environment size, number of objects and their types. The general flow of 3D password system is shown in figure below:

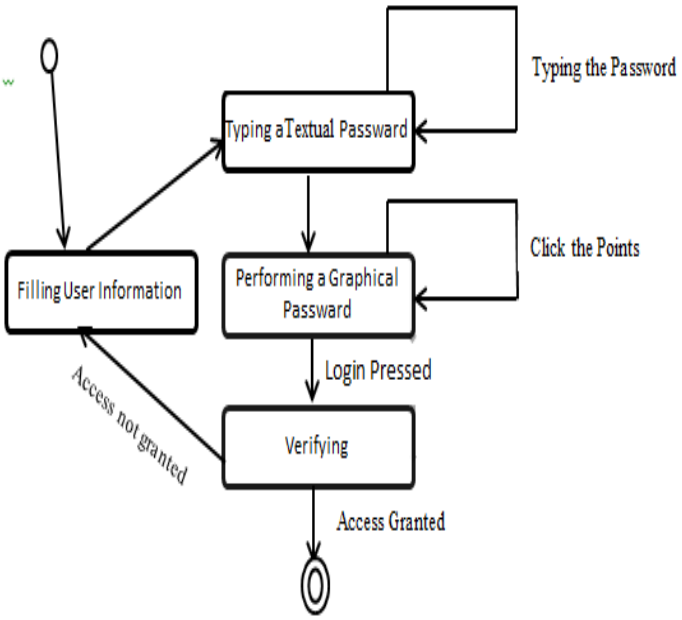


Fig.2.2 Flow of the System

C. Advantages Offered by 3D Password System

1) A 3D password gives the user the choice of modeling his 3D password to contain any authentication scheme that the user prefers.
2) Users have the choice to model their 3D password according to their needs and their preferences.
3) Users do not have to provide their fingerprints if they do not wish to.

4) It fails most of the brute force attacks and dictionary attacks.
5) As the authentication system is new and complex the hacker will have to study the new authentication schemes .It requires a study of the user's selection of objects for the 3D password which is quite difficult as the selection of object varies from individual to individual.
6) Provides strong security over critical servers. Now a day as all banking transactions are done on internet.so this module will provide a good security to e-commerce transactions.
7) As this system is based on human quality if recognition and recall, password cracking algorithms fail to crack these passwords.
8) The 3D virtual environment contains biometric recognition objects and token based objects. The attacker has to forge all probable biometric information and forge all the essential tokens. The cost of forging such information is very expensive; therefore cracking the 3D password is more challenging.
9) Easy to use as an end user.

SECURITY ANALYSIS OF 3D PASSWORD SYSTEM

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 [10]. As 3D password system gives the user the freedom of selection as to what type of authentication scheme will be included in their 3D password and ease provided by it in making infinite number of password by combining two or more schemes. The large number of objects in virtual environment will increase the possibility of large number of 3D password which makes it difficult for the attacker to crack the password. As 3D password authentication scheme is multifactor so in order to realize the security of it we have to consider all possible attacks on its all factors such as all possible attacks on textual and graphical authentication scheme. When combining two or more schemes together we have to consider attacks which are possible on individual scheme should not possible when combined with other schemes to create 3D password system. All possible attacks on combination of textual and graphical password authentication scheme are as follows:

1) Brute-Force Attack

Brute-Force attack is a trial and error method where attacker has to try all possible combination of 3D password. This attack is not possible in 3D password system because The total time needed for a legitimate user to login may vary from 20 s to 2 min or more, depending on the number of interactions and actions, the size of the 3-D virtual environment, and the type of actions and interactions done by the user as a 3-D password. Therefore, a brute force attack on a 3-D password is very difficult and time consuming.

2) Well-Studied Attack

In this attack, the attacker tries to find the highest probable distribution of 3-D passwords. Acquiring such knowledge is very difficult because the attacker has to study all the existing authentication schemes that are used in the 3-D environment. It requires a study of the user's selection of objects, or a combination of objects, that the user will use as a 3-D password. Moreover, a well-studied attack is very hard to accomplish since the attacker has to perform a customized attack for every different 3-D virtual environment design.

3) Timing Attack

In this attack, the attacker observes how long it takes the legitimate user to perform a correct sign-in using the 3-D password. This observation gives the attacker an indication of the legitimate user's 3-D 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 3-D virtual environment is poorly designed.

4) Keylogger

In this attack attacker install as software called key logger on system where authentication scheme is used. This software stores text entered through keyboard & those text are stored in text file. In this way this attacks is more effective & useful for only textual password, but as 3D password is multi password authentication scheme, So that this kind of attacks are not much effective in this case.

5) Shoulder-Surfing Attack

In this attack, an attacker uses a camera to record the user's 3-D password or tries to watch the legitimate user while the 3-D password is being performed [2] [7]. This attack is the most successful type of attack against 3-D passwords and some other graphical passwords. Shoulder surfing" or "peeping attacks" refers to stealing information (especially authentication information) by looking over the shoulder of an unsuspecting user and unauthorized observing of an authorized user's session on an electronic device in order to gain access to information. Most authentication methods involve pressing keys on a keyboard or selecting objects on a

screen, and both the screen and the keyboard are visible to the authorized user as well as to the shoulder surfer. Both textual and graphical passwords are vulnerable to this attack. The degree of threat depends on the situation. In this way 3D password is vulnerable to shoulder surfing attack. To make 3D password much more secure and non-vulnerable to shoulder surfing attack, pass-icons in convex hull scheme can be used.

CONVEX HULL CLICK SCHEME

Convex Hull Click scheme (CHC) is a graphical password and another multiple round challenge response authentication scheme proposed to lead off shoulder surfing[7] [10]. In this scheme the system uses a large portfolio consisting of several hundred icons. The icons are displayed using the image without text. The user will click on the set of icons and the sequence in which user clicked on the icons is recorded. After that user creates an imaginary hull mentally based on the sequence of clicks made by the user. Now, user made some clicks on some icons which are inside the imaginary hull. The combination of hull created by user and the clicks made inside the hull will be the user's graphical password.

Fig.4.1 Concept of Convex Hull Click Scheme (CHC)

A. Drawbacks of Convex Hull Click Scheme(CHC)

I. Increased Complexity
II. More chances of failure by authenticated user as imaginary hull can be wrong manipulated.
III. Password space is small, hacker get more chances of hacking the password
IV. Time taken is more in performing graphical password.

PASS-ICONS BASED 3D PASSWORD SYSTEM

The phenomenon of pass icons is used in convex hull scheme which is a shoulder-surfing attack defense scheme. Convex Hull scheme is a graphical password scheme that has been designed to guard against shoulder-surfing attack. The system uses a large portfolio consisting of several hundred icons. The user interacts with the system in the flow which is shown in the figure below:

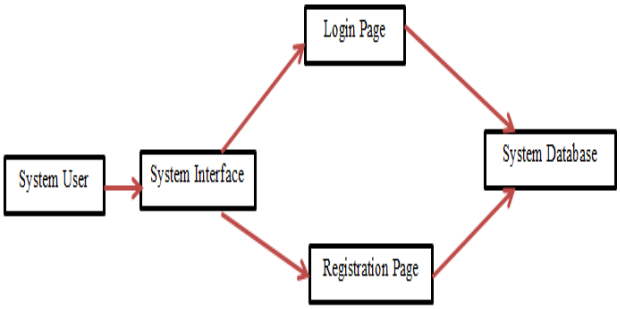


Fig 5.1 Flow of Pass-icons Based 3D Password System

The main features of this will be the user interface which will directly impact the usability of the system and the security of the system which will be directly impacted by the security procedures utilized in the system. The user will be primarily interacting with two interfaces login page and the registration page. The registration page is of significant importance as this is where the user will be able to create and set their password. First the user will be registering itself by giving its basic details along with a user-id and textual password.

Fig 5.2 Registration Page

After that user will set its graphical password by clicking on the icons displayed on a screen as shown in the figure below:

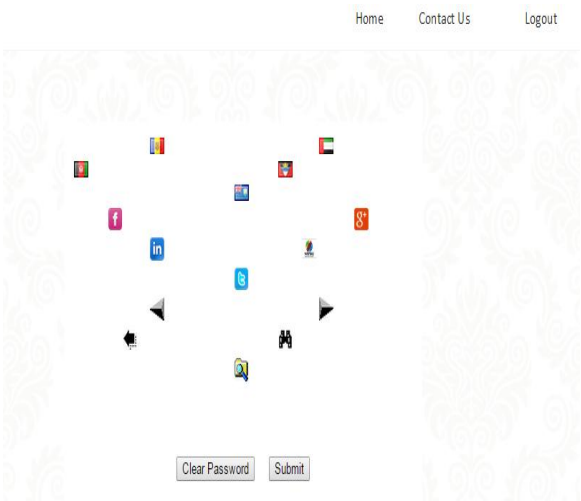


Fig 5.3 Graphical Interface

The icons clicked by the user are called the pass-icons which are shown in the figure below.

Fig 5.4 Pass-icons in Graphical Interface

The pass-icons along with the textual password and other details are saved into the database. The combination of textual password and pass-icons becomes the 3D password of the user. The second interface that the user will be interacting with is the login screen of the system. With this interface the user will be required to enter their user-id along with textual password, if both matched with the database the user is presented with the screen consisting of icons where he has to enter his graphical password. If the pass-icons clicked by the user matches from the database then the user are granted access to the system .If access is not granted, an error message is presented to the user informing them of the error. For both the login and registration pages, the users will be provided with a means to clear any errors they would have made with entering the password and given the opportunity to try again. Both the login and the registration page interact with the database. This database is responsible for the secure storage of the user's personal details including the user name, the pass-icons selected for the password. It is imperative that the database be secure to guarantee the security of the users' information.

CONCLUSION

3D Password is an authentication scheme which combines the benefits of all other authentication schemes in one scheme along with much more secure system. As this authentication scheme is feasible so any upcoming authentication scheme can also be added into this system. In this paper, i did the inclusion of textual and graphical authentication scheme to make 3D password authentication system. This combination is free from all kinds of attacks except shoulder surfing attack for which we have used the pass-icons based 3d password system. Pass-icons based system offers several benefits along with the non-vulnerability of shoulder surfing attack. In our observation if we implement pass-icons concept in 3D password authentication scheme, then this scheme will provide better results while choosing graphical password.

References

[1] Banita Chadha, Dr. Puneet Goswni,"3D Password-A Secure Tool", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), Volume 4, Issue 1, January 2014.

[2] Vishal Kolhe, Vipul Gunjal, Sayali Kalasakar, Pranjal Rathod, " *Secure Authentication with 3D Password*", International Journal of Engineering Science and Innovtive Technology(IJESIT), Volume 2, Issue 2, March 2013.

[3] Mr.Jaywant N. Khedkar, Ms.Pragati P. Katalkar, Ms.Shalini V. Pathak, Mrs.Rohini V.Agawane, "*Integration of Sound Signature in 3D PasswordAuthentication System*", International Journal of Innovative

Research in Computer and Communication Engineering,Vol. 1, Issue 2, April 2013.

[4] A Aswathy Nair, Theresa Rani Joseph, Jenny Maria Johny," *A Proficient Multilevel Graphical Authentication System*", Interanational Journal of Science, Engineering, and Technology Research (IJSETR), Volume 2, No 6, June 2013.

[5] R.N.Muneshwar, S.K.Sonkar, "*Virtual Environments Provide Mammoth Security for Critical Server*", International Journal of Engineering and Advanced Technology (IJEAT), Volume-2, Issue-3, February 2013.

[6] Shubham Bhardwaj, Varun Gandhi, Varsha Yadav, Lalit Poddar, "*New Era of Authentication: 3-D Password*", International Journal of Science, Engineering and Technology Research (IJSETR), Volume-1, Issue-5, November 2012.

[7] A.B.Gadicha , V.B.Gadicha , "*Virtual Realization using 3D Password*", International Journal of Electronics and Computer Science Engineering, ISSN 2277-1956/V1N2-216-222.

[8] Grover Aman, Narang Winnie,"*4-D Password: Strengthening the Authentication Scene*", International Journal of Scientific & Engineering Research, Volume 3, Issue 10, October-2012.

[9] Mr. Namdev A. Anwat, Mr. Dattatray S. Shingate, Dr. Varsha H. Patil, "*A Secure Authentication Mechanism using 3D Password*", International Journal of Advance Research in Science, Engineering and Technology, Vol.01, Issue 01, pp. 29-37.

[10] Fawaz A. Alsulaiman, Abdulmotaleb El Saddik,"*Three Dimensional Password for More Secure Authentication*", IEEE Transactions on Instrumentation and Measurement, Vol. 57, No. 9, September 2008.

[11] Harshil Shah, Chirag Lakhani, Sagar Haldankar,"*Graphical Password Authentication Based on Polygon Visualization*", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622.

2-tier Secure Communication between Smart devices

Lucknesh Kumar
Galgotias College of Engineering and Technology Greater Noida, India
Lucknesh.mnnit@gmail.com

Apoorv Agarwal
Galgotias College of Engineering and Technology Greater Noida, India
apoorvagarwal_2411@hotmail.com

Arpit Kumar Srivastava
Galgotias College of Engineering and Technology Greater Noida, India
arpityuuvraaj@gmail.com

Abhinav Mathur
Galgotias College of Engineering and Technology Greater Noida, India
abhinav23mat@gmail.com

Abstract - **The Internet of Things (IoT), an emerging global Internet-based technical architecture facilitating the exchange of information, goods and services in the internet world has an impact on the security and privacy of the involved stakeholders. Measures ensuring the architecture's resilience to attacks, data authentication, and access control and client privacy need to be established.**

This paper includes a survey of IoT and various security issues related to it. Furthermore, out of all security issues, concern over data authentication and transfer is taken into consideration. Here we will discuss the idea for two levels of security in form of two different approaches i.e. Advance Encryption Standards (AES) and the Steganography approach via an image and the simulating of these two logics in the MATLAB.

Keywords: Internet of Things (IoT), RFID, Advance Encryption Standard (AES).

INTRODUCTION

Internet of Things is everything. It can be defined in many different ways, depending upon what you are dealing with, how you manage them and what are your resources. It encompasses several aspects of life-from various components (such as refrigerator, oven, and washing machine) to well-equipped semi-detached homes, from travelling tools to sophisticated devices to track down from an individual's behavior to his extent of thinking and collecting relevant data and "apply services".

IoT [1-2] is the next step of digital data virtualization since it can be visualized as the interaction between several packets of data from various devices and their exchange between machines and objects. Internet of Things (IoT) is something that connects 100 millions of people as an emerging global Internet-based information architecture facilitating the exchange of data and information at global level.

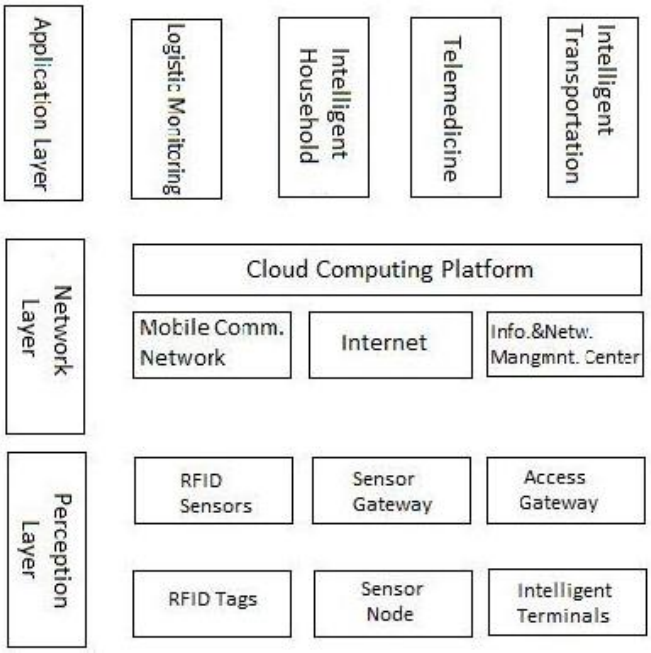


Fig. 1 Structure of IoT

The term of IoT was first used by Kevin Ashton in 1999 (though the concept has been discussed since 1991) in the context of supply chain management [3]. From the technical point of view, the structure is based on data communication tools, primarily RFID-tagged items and cloud-based support services. The IoT [4-6] has a purpose of providing an IT-infrastructure, providing the exchange of "things" in a safe and reliable manner.

Radio Frequency Identification (RFID) and sensor network technologies can be used to meet the new challenge of the next wave in the era of computing, in which information and communication system are invisibly embedded in the environment around us. This result in the generation of enormous amounts of data which need to be stored, processed efficiently and presented in a seamless and understandable form.

Security of the data, channels, medium etc. is an important aspect into which the IT organizations are most concerned about [7] Despite of the theoretical concept of the secured servers and smart devices, practical implementation of these security features are at minimal. [8-10]Following security and privacy requirements can be mentioned as:

- Terminal security issue of IoT: terminal devices are easily accessible and can cause damage or data modifications. Authentication and integrity of the data is prior concern. Since passive RFID tags cannot exchange too many message with the authentication servers, main problem existed in the perception terminal includes terminal of sensitive information leakage, tampering, copying, terminal virus and other issues.
- Sensor network security problem of IoT: sensors are not only responsible for the data transmission but also data acquisition, integrity and collaboration. Therefore malicious code attacks and security risk in information transmission may occur.
- Information transmission security of IoT: security related to the security risk of IoT and the protocol vulnerabilities defects.
- Information processing safety of the IoT reflected in the middleware layer
- Data which is needed to be transferred must be encrypted before transmission. It aims to protect the confidentiality and integrity of the information transmission and to prevent data tampering.

This research is opted because of several reasons. IoT is now becoming a world-wide technology, the potential users are exponentially increasing and the algorithm being used is cheap, easy to implement, can be easily reprogrammed and has good level of security.

This research paper is focused on the performance and the implementation of combined logic of AES and steganography. Here the data that is to be transferred between smart devices is required to undergo a set of process that includes sequential implementation of algorithms to enhance its security. Thereafter simulation of these algorithms is done on MATLAB environment.

RELATED WORK

To give more description about the implementation and analysis of this 2-tier security, this section show some other work from the related field.

In [11-13], authors analyzed the performance of DES, AES and Blowfish encryption algorithms. Furthermore there performance is compared over varying block size, key size and number of round of the encryption input file. And thus their performance is analyzed by computing various performance parameters such as execution time and memory required. The result showed blowfish algorithm consumes less execution time, memory usage and produce more throughputs. Blowfish algorithm performed approximately 4 times faster than AES and 2 times faster than DES.

Thereafter the blowfish algorithm is studied and enhanced and its function is modified [14]. In [15] author designed an algorithm that combines the process of bits from ancient cipher and substitution boxes from modern cipher. These research present the idea that either AES, DES, 3DES or Blowfish algorithms are good enough for securing the data

transmission between devices or terminals to some extent or they are even better in comparison to each other, but the level of security provided is limited to only one level.

DESIGN

Advance Encryption Standard: AES is based on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is fast in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. AES uses Rijndael cipher which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits and is defined in three versions 10, 12 and 14 rounds respectively.

Fig. 2 show the functional structure of the AES. The plaintext block size of 128 bits (16 bytes) is converted into cipher text using key of length 128, 192, or 256 bits (16, 24, 32 bytes). The algorithms is referred to as AES-128, AES-192 and AES-256, depending upon the key length.

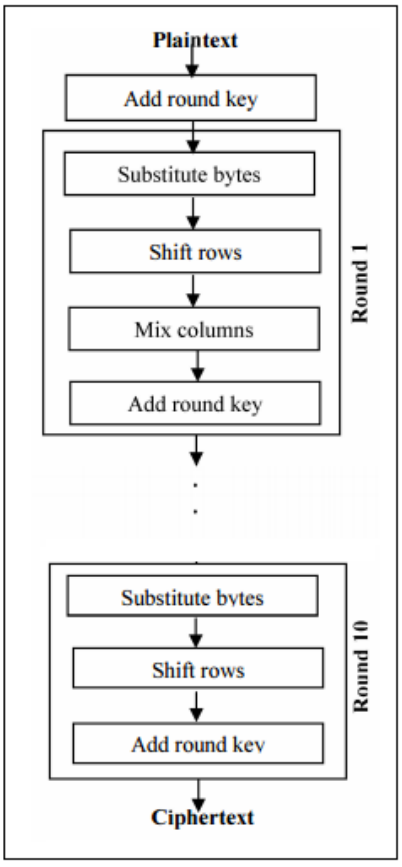


Fig. 2 Structure of AES

There are three steps performed in AES, i.e. encryption, decryption and key generation.

AES encryption
Step 1: Get the plain text and the key
Step 2: Perform the pre-round transformation using the plain text
Step 3: With 'n' key length, perform transformation for 'n' rounds
Step 4: cipher text achieved

AES decryption
Repeat the step followed in encryption in reverse order

Key Generation
Step 1: Get the key
Step 2: based upon number of round, calculate required number of words
Step 3: In an array of 4 bytes, first four words are made from the key
Step 4: Get the next word
Step 5: Repeat step 4 until required number of words are reached.

Steganography: Image steganography is the modern way of hiding the text in an image in such a way that the information hidden is secure and well away from the intruder. Apart from hiding the secret data, it is also useful in data authentication and availability of data ensuring proper usage, data monitoring, copyright protection, ownership identification, confidentiality and control of data piracy etc.

Fig.3 show flow chart of image steganography.

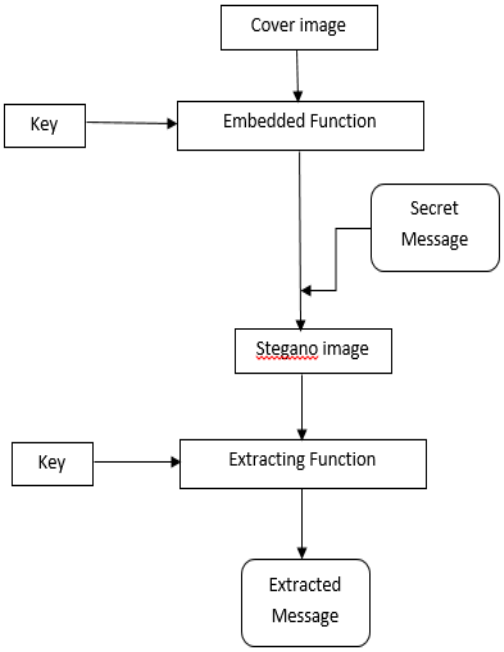


Fig. 3 Steganography workflow

WORKFLOW

Securing the data and information among the devices in organization is a serious issue especially when devices are connected to the internet. Using two simple and cheap encryption algorithms but implementing efficiently could help us to achieve a bigger goal. This research uses the AES algorithm followed by image steganography. The message that is needed to be transferred from one device to another (in case of IoT, it is smart devices), is first encrypted using AES encryption and the generated cipher text is hidden in an image using steganography technique. The generated stegano image is transferred in the communication channel where it is secured from the intruder. At receiver side the mentioned steps are followed in reverse order and ultimately the plain text is achieved.

Fig. 4 show how the implementation process of the approach actually takes place.

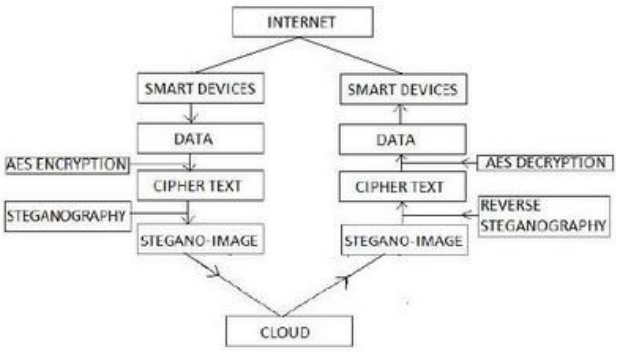


Fig. 4 Workflow

FUTURE WORK

This research is expected to provide us with security features and facilities that can be easily taken into consideration. The 2-tier secure channel that we are providing is not only cheap and efficient but will also enhance the integrity of the data. Smart devices now-a-days are vulnerable to many types of attacks and this approach can be helpful in distinguishing various intruders and can thus provide a broader area for analysis and data protection.

References

[1] Rajkumar Buyya, Jayavardhana Gubbi, Slaven Marusic, Marimuthu Palaniswami -Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions, University of Melbourne, Australia.

[2] Ashton, Kevin (22 June 2009). "That 'Internet of Things' Thing, in the real world things matter more than ideas". RFID Journal.

[3] The Internet of Things. International Telecommunication Union (ITU). ITU Internet Report, 2005

[4] Gonzalez G. Organero M, Kloos C. "Early in infrastructure of all Internet of Things in space for learning". 8th IEEE International Conference on Advance Learning Technologies, 2008:381-383

[5] Amardeo C, Sarma J. Identities in the future Internet of Things. Wireless Pers Commun, 2009, 49:353-363

[6] Security model and key technologies for the Internet of things, The Journal of China Universities of Posts and Telecommunications, December 2011

[7] Lan Li, Study on security architecture in the internet of things, International Conference on Measurement, information and Control (MIC), 2012

[8] Xu Xiaohui, Study of Security problem and Key Technologies of the Internet of Things, International Conference of Computation and Information Sciences, 2013

[9] Leusse D, Per Iorellis P, Dimitrakos P. ―Self-Managed Security Cell, a Security Model for the Internet of Things and Services Advances in Future Internet‖. 2009 First International Conference on Digital Object Identifier, 2009, pp. 47-52.

[10] Security model and key technologies for the Internet of things, The Journal of China Universities of Posts and Telecommunications, December 2011

[11] Ramesh.A, Suruliandi.A, "Performance Analysis of Encryption for Information Security", IEEE, 2013.

[12] G.N.Krishnamurthy, Ramaswamy.V, M.E.Ashalatha,"Performance Enhancement of Blowfish and CAST-128 Algorithms and Security of Improved Blowfish Algorithms Using Avelanche Effect", International Journal of Computer Science and Network Security, Vol.8 No.3, 2008.

[13] Ramesh.A, Suruliandi.A, "Performance Analysis of Encryption for Information Security", IEEE, 2013.

[14] K.Mayers Rusell, H.Desoky Ahmed," An Implementation of the Blowfish Cryptosystem", IEEE.2008.

[15] R.Sriram and K.Marimuthu,"Designing an Algorithm with High Avelanche Effect", International Journal of Computer Science and Network Security, Vol 11 No.1, 2011.

Degraded Document Image Binarization

Garima Chutani
CDAC, Noida
garima.chutani@gmail.com

Tushar Patnaik,
CDAC, Noida
tusharpatnaik@cdac.in

Abstract **- Degraded Document Image Binarization is usually performed in the preprocessing stage of different document image processing related applications such as optical character recognition (OCR). Purpose of Degraded Document Image Binarization is to convert poor quality grayscale or colored images with low quality i.e. noisy background to binary form to feed them into OCR system as a preprocessing module. Binarization is a process which is very useful in most of the image processing applications. Due to poor binarization most of the images after digitization, suffers from various types of document degradation such as poor contrast, noise, uneven illumination, shadows, bleed-through etc. Degraded Document Image Binarization is an active subject in image processing which addresses these problems. In this paper we present a local binarization approach which includes region localization and noise cleaning along with the hybrid thresholding method which yields more accurate result as compared to the already existing algorithms. Basic evaluation parameters used are precision, recall, F-measure, signal to noise ratio (SNR) and peak signal to noise ratio (PSNR).**

Keywords – Document image binarization ; Binarization evaluation; Preprocessing

INTRODUCTION

At present scenarios lot of research works are going on binarization since it is one of the basic feedbacks to Image processing applications. Hence many approaches and techniques were developed to enhance document image quality. Binarization is one of the techniques which improve the quality of an image.

Binarization is one of the most important pre-processing steps which separate foreground and background area of images. It converts a gray-scale image into a binary image. The extraction of main objects from an image sometimes becomes more challenging because of the presence of some noises like, ink bleed, variable background, non-uniform illuminations, shadow etc. Thresholding is a technique which separates an image into two meaningful regions: foreground and background, through a selected threshold value T.

Generally, thresholding have been classified into: Global Thresholding (Otsu), Local Thresholding (Sauvola).This paper is organized in 4 sections. In Section II we present the proposed approach. section III Describes about the Test results, section IV describes some possible extensions and future works.

PROPOSED METHOD

In this section we present our approach of binarization. We have integrated a prebinarization step in order to enhance the input image quality. Figure 1 shows an overview of the proposed binarization architecture. We have integrated different noise removal methods before binarization, in order to enhance the quality of the gray-scale image.

A. Noise Removal

Digital images are prone to various types of noise. Noise can be removed by using many filters. In this approach three filters are used: Mean filter, median filter and wiener filter

B. Region localization

We have integrated localization for the object-of-interest at the pre binarization step. Selected objects-of-interest are considered as the inputs of the method of binarization. We have used canny's edge detection for this task. We classify into two regions as object of interest and the background region. On the object of

interest region we apply binarization algorithm and separate into foreground and background region.

C. Binarization
We have used different binarization methods.

1) OTSU TECHNIQUE-

- Otsu's algorithm is based on maximizing the inter-class variance or minimizing intra-class variance.
- The intra-class variance is defined as weighted sum of variances of the two classes.

Outcome of this step is:

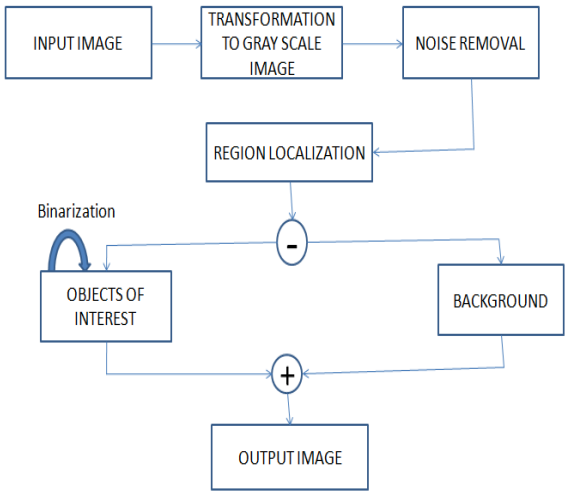
$$T(x,y) = \begin{cases} 255 \text{ if } I(x,y) > \\ I(x,y) \text{ if } I(x,y) \leq \end{cases}$$

T(x,y)- new value of pixel
I(x,y)-Intensity of original image pixel
Tg- Global threshold computed for entire image

- Local Thresholding- The original image is partitioned into smaller sub images and threshold is determined for each of the sub images.

2) SAUVOLA TECHNIQUE-

- Sauvola has introduced a binarization technique where the local threshold is computed by standard deviation.
- This method calculates pixel-wise threshold by sliding a rectangular window over the image.



TEST RESULTS

Evaluation Metrics-
The following parameters from 30 images (Total 210 images) from each image types are used to evaluate these degraded document images when compared with the reference images. Those parameters are:

1. Mean Square Error (MSE)
-Goal is to compare degree of similarity or level of error.
-Error is basically difference between the original and distorted image.

2. Peak Signal to Noise Ratio (PSNR)
-The PSNR is most commonly used as a measure of how an image is close to another using the mean square error (MSE) and a constant C as measure for the difference between foreground and background pixel intensities.

$$PSNR = 10 \cdot log_{10} \left(\frac{C^2}{MSE} \right)$$

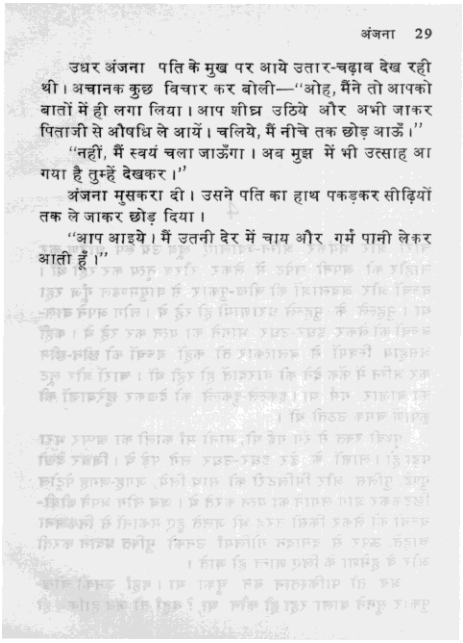
3. Signal to Noise Ratio (SNR)

-It is defined as the ratio of signal power to the noise power
-Expressed in decibels.

Comparison of images on the basis of these parameters-

IMAGE TYPE	MSE	PSNR	SNR
1-gaussian	0.0757	59.3403	10.7298
2-speckle	0.0965	58.2850	9.6745
3-localvar	0.0346	62.7421	14.4987
4-unevenly	0.0082	68.9821	20.6992
5-salt and	2.7618e+003	13.7188	-5.9211
6-shadow	1.4582e+004	6.4927	-13.2389
7-blurred	67.5121	29.8370	-2.6957

Table 1 Comparison of images on the basis of MSE, PSNR and SNR value



अंजना 29

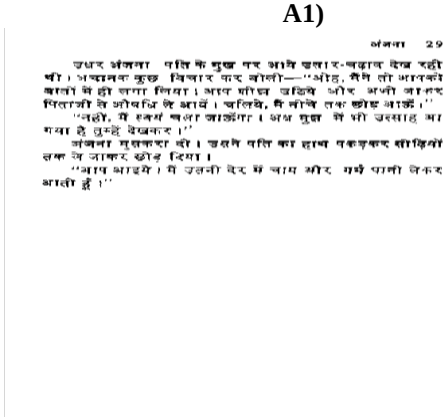
उधर अंजना पति के मुख पर आये उतार-चढ़ाव देख रही थी। अचानक कुछ विचार कर बोली—"ओह, मैंने तो आपको बातों में ही लगा लिया। आप शीघ्र उठिये और अभी जाकर पिताजी से औषधि ले आयें। चलिये, मैं नीचे तक छोड़ आऊँ।"

"नहीं, मैं स्वयं चला जाऊँगा। अब मुझ में भी उत्साह आ गया है तुम्हें देखकर।"

अंजना मुसकरा दी। उसने पति का हाथ पकड़कर सीढ़ियों तक ले जाकर छोड़ दिया।

"आप आइये। मैं उतनी देर में चाय और गर्म पानी लेकर आती हूँ।"

A1)



अंजना 29

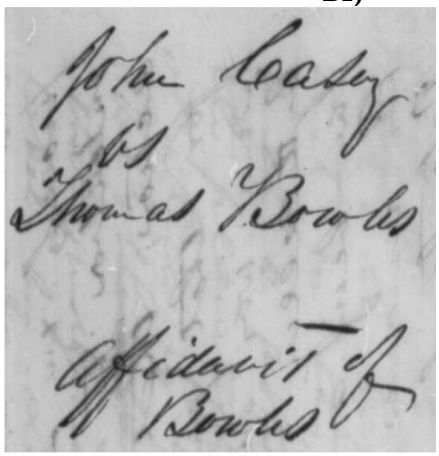
उधर अंजना पति के मुख पर आये उतार-चढ़ाव देख रही थी। अचानक कुछ विचार कर बोली—"ओह, मैंने तो आपको बातों में ही लगा लिया। आप शीघ्र उठिये और अभी जाकर पिताजी से औषधि ले आयें। चलिये, मैं नीचे तक छोड़ आऊँ।"

"नहीं, मैं स्वयं चला जाऊँगा। अब मुझ में भी उत्साह आ गया है तुम्हें देखकर।"

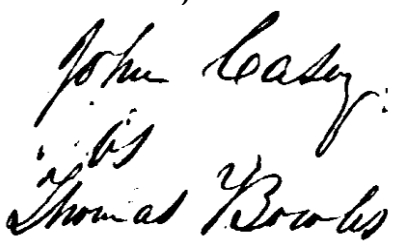
अंजना मुसकरा दी। उसने पति का हाथ पकड़कर सीढ़ियों तक ले जाकर छोड़ दिया।

"आप आइये। मैं उतनी देर में चाय और गर्म पानी लेकर आती हूँ।"

B1)



A2)



B2)

Figure. 2 Samples of the test dataset resulted from binarization (A) Degraded document (B) Binarized document

CONCLUSION

This research paper includes basic techniques of binarization, types of degradations and comparison of degraded documents in terms of peak signal to noise ratio (PSNR), signal to noise ratio (SNR) and Mean square error (MSE). We get better quality images when we binarize degraded documents using existing binarization techniques. In this new approach we have added region localization module which separates the image into two regions i.e. object of interest and background. The existing binarization technique will be applied on the object of interest region only and not on whole image thus improving the quality of image more and providing better result. The objective of our future work is to develop a technique that can detect the type of degradation which will significantly improve the result of binarization.

References

[1] Naveed Bin Rais , M. Shehzad Hanif and rmtiaz A. Taj *" Adaptive Thresholding Technique for Document Image Analysis"* Center for Advanced Studies in Engineering (CASE), © 2004 IEEE

[2] Seyed Amin Tabatabaei "A novel method for binarization of badly illuminated document images" MSc Student, University of Tehran, Tehran,

Iran © 2010 IEEE Proceedings of 2010 IEEE 17th International Conference on Image Processing

[3] Mohamed Zayed, Asma Ouari, Meriem Derraschouk and Youcef Chibani *"An Effective Hybrid Thresholding Technique for Degraded Documents Images Binarization"* Faculty of Electronics and Computer Science, University of Sciences and Technologies Houari Boumedienne Algiers, Algeria © 2011 IEEE 6^{TH} international conference on internet technology and secured transactions 11-14 December 2011 Abu Dhabi, United Arab.

[4] N. Chaki et al." *A Comprehensive Survey on Image Binarization Techniques Exploring Image Binarization Techniques"* Studies in Computational Intelligence © Springer India 2014

[5] Bolan Su, Shijian Lu and Chew Lim Tan *"Combination of Document Image Binarization Techniques"* Department of Computer Vision and Image Understanding Institute for Infocomm Research-© 2011 IEEE 2011 International Conference on Document Analysis and Recognition

[6] Soharab Hossain Shaikh, Asis Maiti, Nabendu Chaki *"Image Binarization Using Iterative Partitioning"*University of Calcutta, India- © 2011 IEEE 2011 International Conference on Recent Trends in Information Systems

Performance Evaluation of Hierarchal Protocols in Wireless Sensor Networks

Payal Jain
Mewar University Chittorgarh, Rajasthan
bhavayapayal@gmail.com

Dr. Anu Chaudhary
Ajay Kumar Garg Engineering College, Gzb
getanuchaudhary@yahoo.com

***Abstract* - Energy is the scarcest resource of WSN nodes, and it determines the lifetime of WSNs. In today's environment wireless sensor networks are used wildly, hence the measure concern is the efficiency of the sensor networks and the efficiency strongly depends on the routing protocols which are used in the sensor networks. In this paper, we will discuss two different types of routing protocol: LEACH and PEGASIS. Network simulator 2 is being used to analyze the result and found that PEGASIS performs better than LEACH.**

Keywords: Wireless sensor networks, Routing protocols, PEGASIS, LEACH, Energy consumption and Performance.

INTRODUCTION

Wireless Sensor Networks have emerged as an important new area in wireless technology. In the near future, the wireless sensor networks are expected to consist of thousands of inexpensive nodes, each having sensing capability with limited computational and communication power which enable us to deploy a large-scale sensor network.

A wireless sensor network is a group of specialized transducers with a communications infrastructure for monitoring and recording conditions at diverse locations. Commonly monitored parameters are temperature, humidity, pressure, wind direction and speed, illumination intensity, vibration intensity, sound intensity, power-line voltage, chemical concentrations, pollutant levels and vital body functions.

A sensor network consists of multiple detection stations called sensor nodes, each of which is small, lightweight and portable. Every sensor node is equipped with a transducer, microcomputer, transceiver and power source. The transducer generates electrical signals based on sensed physical effects and phenomena. The microcomputer processes and stores the sensor output. The transceiver receives commands from a central computer and transmits data to that computer. The power for each sensor node is derived from a battery.

The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding [9].

Sensor networks have a wide variety of applications and systems with vastly varying requirements and characteristics. The sensor networks can be used in Military environment, Disaster management, Habitat monitoring, Medical and health care, Industrial fields, Home networks, detecting chemical, Biological, radiological, nuclear, and explosive material etc. Deployment of a sensor network in these applications can be in random fashion (e.g., dropped from an airplane) or can be Planted manually (e.g., fire alarm

sensors in a facility). For example, in a disaster management application, a large number of sensors can be dropped from a helicopter. Networking these sensors can assist rescue operations by locating survivors, identifying risky areas, and making the rescue team more aware of the overall situation in the Disaster area [1].

SENSOR NETWORK CHALLENGES

Wireless sensor network uses a wide variety of application and to impact these applications in real world environments, we need more efficient protocols. Designing a new protocol or algorithm address some challenge which is needed to be clearly understood. These challenges are summarized below:

Physically Resource Constraints: The most important constraint imposed on sensor network is the limited battery power of sensor nodes. Limited computational power and memory size is another constraint that affects the amount of data that can be stored in individual sensor nodes. So the protocol should be simple and light-weighted.

Ad-hoc Deployment: Many applications are requires the ad-hoc deployment of sensor nodes in the specific area. Sensor nodes are randomly deployed over the region without any infrastructure and prior knowledge of topology. In such a situation, it is up to the nodes to identify its connectivity and distribution between the nodes

Fault-Tolerance: In a hostile environment, a sensor node may fail due to physical damage or lack of energy. If some nodes fail, the protocols that are working upon must accommodate this change in the network.

Scalability: Most of the applications are needed; the number of sensor nodes deployed must be in order of hundreds, thousands or more .The protocols must scalable enough to respond and operate with such large number of sensor nodes.

Quality of Service: Some real time sensor application are very time critical which means the data should be delivered within a certain period of time from the moment it is sensed, otherwise the data will be unusable. So this must be a QOS parameter for some applications.

Undeterred: The sensors nodes are not connected to any energy source. They have only a finite source of energy, which must be optimally used for processing and communication. To make optimal use of energy, communication should be minimized as much as possible.

Security: Security is very critical parameter in sensor networks. Security demands for secure data communication in the sensor networks [14].

HIERARCHICAL PROTOCOL

Hierarchical routing protocols also known as cluster-based routing, proposed in wireless networks. They are well known techniques having special advantages related to scalability and efficient communication. The concept of hierarchical routing is also utilized to perform energy efficient energy efficient routing in WSNs. Hierarchical routing is an efficient way to lower energy consumption within a cluster and by performing data aggregation and fusion in order to decrease the number of transmitted messages to the BS. Hierarchical routing is mainly two-layer routing where one layer is used to select cluster heads and the other layer is used for routing [11]. However, most techniques in this category are not about routing, rather on "who and when to send or process/aggregate" the information, channel allocation etc., this can be orthogonal to the multi-hop routing function [15].

LEACH PROTOCOL

LEACH is the hierarchal protocol stands for low energy adaptive clustering hierarchy. As the node is no longer in use when its battery dies but this protocol allows us to space out the lifespan of the nodes allowing it to do only the minimum work so that it can transmit the data. This is the reason why network protocol LEACH is used. The LEACH network is made up of nodes some of which are called cluster heads. The work of these cluster heads is to collect the data from their surrounding nodes and pass it to the base station. LEACH is dynamic because the job of cluster head rotates [5]. The nodes that have been cluster heads cannot become cluster head again for n rounds where n is the desired percentage of the cluster heads. Thereafter each node has a 1/n probability becoming a cluster head in each round at the end of each round each node that is not a cluster head and joins that cluster the cluster head then crates a schedule for each node in its cluster to transmit its data[6].

LEACH network has two phases:

1. The setup phase:
   Each sensor chooses a random number *m* between 0 and 1

If $m < T(n)$ for node n, the node becomes a cluster-head where

$$T(n) = \begin{cases} \dfrac{P}{1 - P[r * \bmod(1/P)]} & if\ n \in G \\ 0 & otherwise, \end{cases}$$

P : the desired percentage of cluster heads
r : the round number
G : the set of nodes that have not been cluster heads during the last $1 / P$ rounds
A cluster head advertises its neighbors using a CSMA MAC.
Surrounding nodes decide which cluster to join based on the signal strength of these messages
Cluster heads assign a TDMA schedule for their members [3].

2. The steady state[7]:
    a. All source nodes send their data to their cluster heads
    b. Cluster heads perform data aggregation/fusion through local transmission
    c. Cluster heads send them back to the BS using a single direct transmission
    d. After a certain period of time, cluster heads are selected again through the set-up phase

The key features of LEACH are:

1. Localized coordination and control for cluster setup and operation.

2. Randomize rotation of the cluster "base stations" on cluster heads and the corresponding clusters.

3. Local compression to reduce global communication [10].

Drawbacks:

1. It is not applicable to networks deployed in large regions

2. The idea of dynamic clustering brings extra overhead.

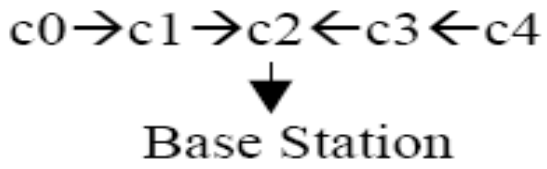
3. The protocol assumes that all nodes begin with the same amount of energy capacity in each election round, assuming that being a CH consumes approximately the same amount of energy for each node

PEGASIS PROTOCOL

PEGASIS is the improved protocol where only one node is chosen ahead node which sends the fused data to the Base station per round. This achieves factor of 2 improved compared to LEACH protocol. It is near optimal chain based protocol that is improvement over LEACH [2].

PEGASIS: Power-efficient gathering in censor information systems. In PEGASIS each node communicates only with the close neighbor and takes turns transmitting to the base station. The main idea in PEGASIS is to form a chain among the censor nodes so that each node will receive from and transmit to a close neighbor, gathered data moves from node to node, get fused and eventually a designated node transmit to the Base station[4]. To construct the chain in PEGASIS protocol we start from the furthest node from the Base station and the greedy approach is used to construct the chain. Leader of each node is selected randomly[12]. If n is number of nodes I mode n node is selected as head node for I round. Randomly selecting head node also provides benefit as it is more likely for nodes to die at random location thus providing robust network [13]. When a node dies chain is reconstructed to bypass that node and head nodes receives all the fused data and send it to the Base station.

Chaining in PEGASIS:



C0, C1, C3, C4 - Non-leader nodes

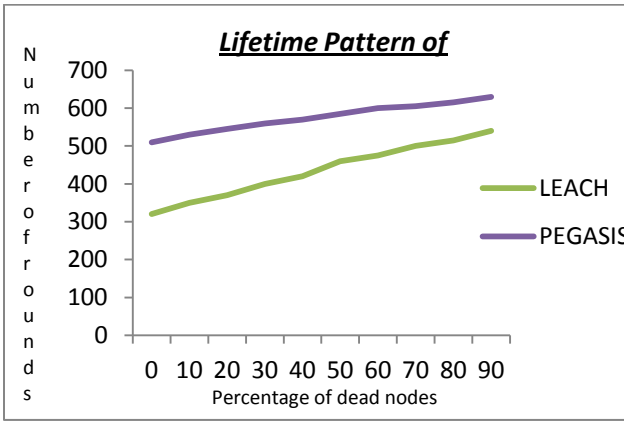
C2- Leader Node

- Each node communicates only with the closest neighbor[8]
- Gathered data moves from node to node, get fused and sent to the BS by the designated leader node

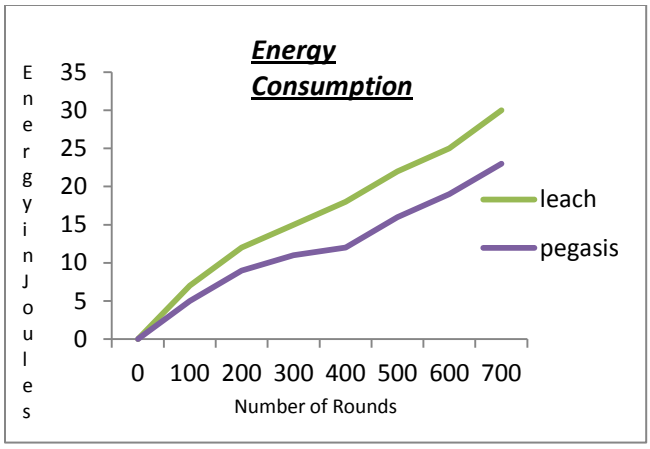
- Nodes take turns being the leader (I mod N)
- Chaining is done using the greedy approach
- When a node dies chaining is done again

SIMULATION RESULTS

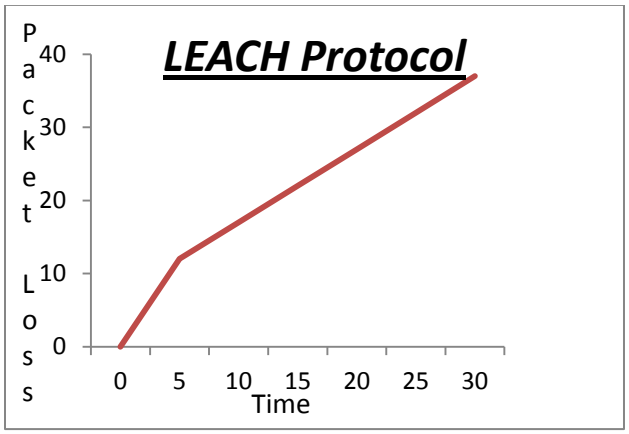
In order to compare the performances between LEACH and PEGASIS, we simulated both of them using network simulator 2. We used several random 100-node networks with each node having 0.5 Joules of initial energy. As measurement tools, we considered the liveliness of the sensors, energy consumed by the sensors and the time requirement to complete several hundred rounds. A node is considered to be dead when its energy becomes zero and excluded for the consecutive rounds. As shown in the Fig. round numbers are determined when 1%, 10%, 20%, 30%, 40%, 50%, 60%, 70% and 80% of nodes are died. From the graph we concluded that PEGASIS perform 35% better than LEACH in terms of system lifetime. This improvement is achieved by reducing the number of communication to distant BS to only single per round.

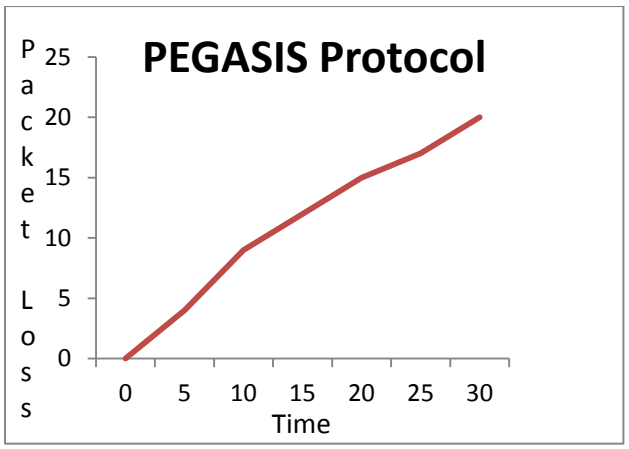


Lifetime pattern of randomly 100-node sensor network with each node having initial energy .5 joules.



Energy consumption of randomly 100-node sensor network with each node having initial energy .5 joules.





CONCLUSION

In this paper we analyzed the performance of the two hierarchical protocol LEACH and PEGASIS with respect to the network lifetime, energy consumption and packet failure. Network simulator 2(NS2) is used to compare the performance of two Hierarchical protocols Pegasis and Leach. The simulation results show that PEGASIS can greatly prolong sensor network's lifetime when the transmission range is limited.

References

[1] Laiali Almazaydeh, Eman Abdelfattah, Manal Al- Bzoor, and Amer Al- Rahayfeh," PERFORMANCE EVALUATION OF ROUTING PROTOCOLS IN WIRELESS SENSOR NETWORKS", International Journal of Computer Science and Information Technology, Volume 2, Number 2, April 2010

[2] S. Lindsay and C. Raghavendra, "PEGASIS: Power-Efficient Gathering in Sensor Information Systems", international Conf. on Communications, 2001. A new routing

[3] Shamsad Parvin and Muhammad Sajjadur Rahim," Performance Evaluation of LEACH and PEGASIS: Two Prominent Routing Protocols for Wireless Sensor Networks ".

[4] Owais Ahmed Ahthsham Sajid and Mirza Aamir Mehmood,"Comparision of Routing Protocols to Assess Network Lifetime of WSN",International Journal of Computer Science Issues,Vol. 8,Issue 6,No 3,November 2011.

[5] Probablistic Modeling of Leach Protocol and Computing Sensor Energy Consumption Rate in Sensor Networks", Song, Dezhen, Febraury 22, 2005 http://www.cs.tamu.edu/acadamics/tr/tamu-cs-tr-2005-2-2.

[7] "Low Energy Adaptive Clustering Hierarchy with Deterministic Cluster-Head Selection", M.J.Handy, M.Haas,D.Timmermann;2002;http//www.vs.inf.ethz.ch/publ/se/IEEE MWCN2002.pdf.

[8] W.Heinzelman, A.Chandrakasan and H.Balakrishnan,"Energy-Efficient Communication protocol for Wireless Microsensor Networks,"Proc.33rdHawaii int'l.conf.sys.sci.Jan.2000.

[9] S. Lindsey and C. Raghavendra, "PEGASIS: Power-Efficient Gathering in Sensor Information Systems," *IEEE Aerospace Conf. Proc.*, 2002, vol. 3, 9–16, pp. 1125–30.

9.http://en.wikipedia.org/wiki/Wireless_sensor_network.

[9] Raed M. Bani Hani and Abdalraheem A. Ijjeh," A Survey on LEACH-Based Energy Aware Protocols for Wireless Sensor Networks", *Journal of Communications Vol. 8, No. 3, March 2013.*

[10] L. J. G. Villalba, Ana L. S. Orozco, A. T. Cabrera, C. J. B. Abbas. "Routing Protocols in Wireless Sensor Networks",IEEE Transactions on Parallel and Distributed Systems, pp.919–931, 2007.

[11] Mukesh Prajapat, and N.C Barwar "Reduction of energy dissipation in wireless sensor network using multi-chain PEGASIS" in IJARCSSE 4(11),November 2014,pp.497-500.

[12] http://www.slideshare.net/ReenaShekar/leach-pegasis?related=1

[13] "Sensor node" available at http://en.wikipedia.org/wiki/Sensor_node,last accessed September, 2014.

.

[14] JAMAL N. AL-KARAKI, AHMED E. KAMAL," ROUTING TECHNIQUES IN WIRELESS SENSOR NETWORKS: A SURVEY**",** IEEE Wireless Communications • December 2004.

Theory on "Computing of impossible" & Idea of human correct age detection System

Aman Kumar
Golgotia's College of Engineering And Technology Greater Noida
varmaaman.mhb@gmail.com

Abstract - **The computing of impossible is same like the physics of impossible. In case of physics of impossible it contains the various theories of physics that is not possible in present like advance smart cars, time travel , supersonic speed and so on.**

It can be made possible in future by using the advance technologies or other theories , but the excuse about computing of impossible is that it is like a operation or execution of any problem with using the computer algorithms and it will be able to solve the problem by using other techniques. It shows that some types of impossible problems in present time like human correct age detection system, make advance intelligent machine (artificial intelligence), make quantum computer and other problems. In this research paper I have focused on that what kind of problems are in present time, and what type of disadvantage can occur in those types of problems, and how you can detect the correct age of any human body with the help of biological cell determination and with the help of many other systems. Basically there is a basic idea to detect the correct age of human being. It detect the initial body part like blood cells and measure that cell growth regarding the time and then save the data into storage. The system contains many part like sensing part that is able to detect the cell by using the rays and it also contain the biological cells infrastructure that will implement to recognize the human blood cell position. Means it clearly shows that this human body has the following growth rate regarding this time,[7][8] then we can calculate the Age according the growth of body cells of human and measure the cell position to detect thousands images and do filter according the status of algorithms. It can be used in various organizations that want correct data like in fields of education, police

department, for research areas, identification and passport testing.

Keywords: Current impossible facts, idea of human correct age detection system, biological sells growth facts, neural network.

INTRODUCTION

The computing of impossible contains the two terms first is computing and second is impossible, both terms shows the some type of advance or smart technologies that contains the some fact or theories that is not possible in present. It can be possible in future or after some years.

The computing works with computer algorithms or based on computer technology. In this paper I am trying to put idea of correct age detection of human using the following parameters.[11][12]

The system has some biological facts in initial state of newly born baby, and it detects the starting growth of cells, and measure cell growth regarding the time.[8]

Then we can estimate the approximate 80% correct age of human from this method.

CURRENT POSSIBLE FACTS

In fields of the impossible facts there are various theories such as field of artificial intelligence, image processing, Quantum computing, human mind and others.

Let us consider in fields of Artificial intelligence like making the more intelligent machine like human, insert the intelligent behavioural programming better than human then it is impossible in present time.

And about some impossible fact regarding the image processing in correct Human age detection system; there is no current system or current technology to detect the correct age of human.

And another excuse about the quantum computing is work with quantum number of electrons but this is very complex situation to controls the quantum phase of electrons.

So in present time there is no idea to make the best quantum computers with the help of quantum computing.

In fields of biology that contains the human mind approach. Basically the mind contains the billion number of neuron. And in present time we have used only less than 10% mind. In current time we don't have algorithms to measure the all number of neurons quantity in our mind.

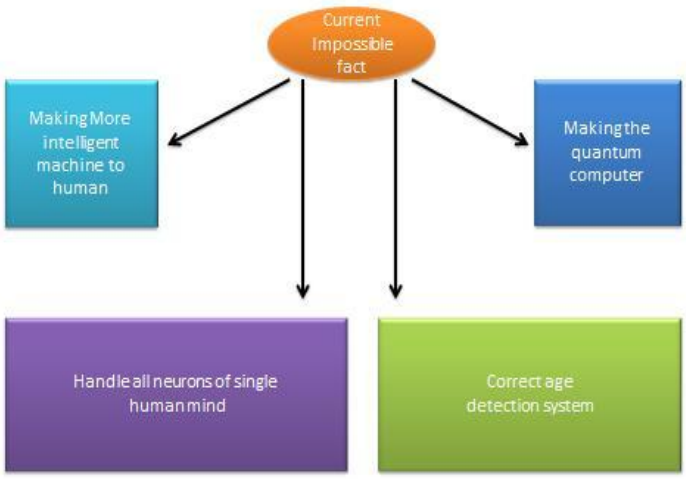


Figure: 1 some current impossible facts

3: Basic Idea to solve the human correct age detection system:

We know that the human body contains the various types of cells and each cell have unique function in growth of the human body.

In case of solving the problem of human to detect the correct age then in initial we have to search the unique cell in body blood and then measure its growth rate regarding the previous and current time.

Then with the use of the sensing system to detect the cell and measure the growth rate and comparison with fixed data pattern in storage.

It has the some mathematical algorithms that can calculate the cell growth rate with respect to the time.

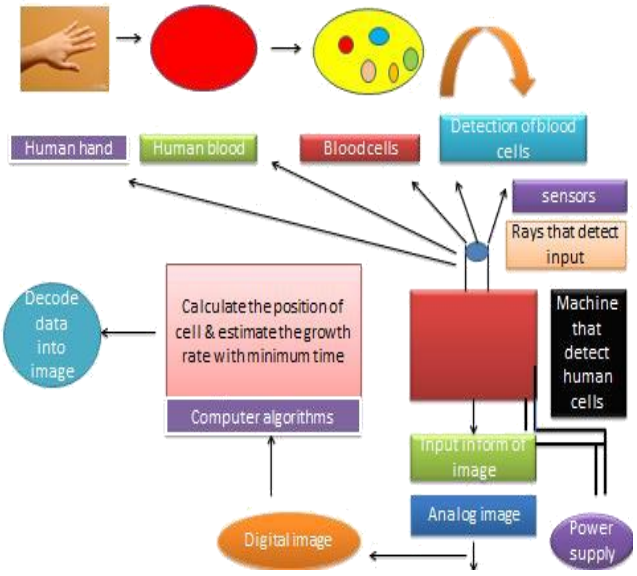


Figure: 2 basic architecture of correct age detection system

This system contains the following step to solve this problem.

3(a): Cell detection system

3(b): Sensing system architecture

3(c): Neural network Architecture [6]

3(a) Cell detection system: The cell detection is the important part of this system. It contains the following parameter.

3(a)1: Measure cell position

3(a)2: Measure cell time

3(a)3: Calculate initial Growth

second -> then minute -> then hour –and month and year..

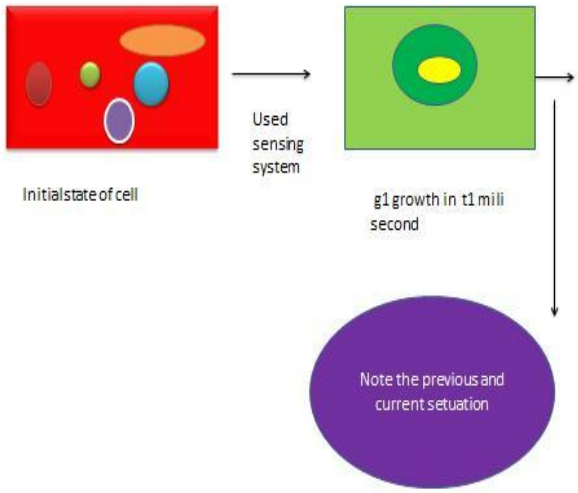


Figure 3: Measure cell position

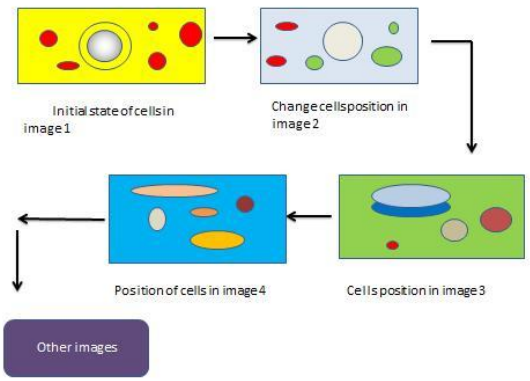


Figure 4 Cell positions with many images

3(b) Measure cell time:

To measure the cell time firstly you have to check the initial time and then check the starting small changing in cell.

3(a) 1 Measure The Cell Position

The human blood contains the various types of cell and each cell contains the unique functionality regarding the various reactions.We will prefers the sensing system to detect the cell using the rays like (x rays) and others then it checks the initial growth rate with minimum second then algorithms assume that its cell is growing following rate then we can calculate that what will growth rate after 10.

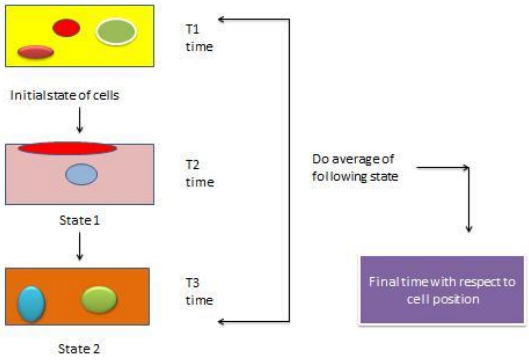


Figure 5: Calculate cell time **3(c)**

Measure cell growth:

The cell uses the various states like replication, mitosis, meiosis and others.The replication contains the binary fusion, than DNA replication, chromosome segregation than cytokinesis. And the mitosis contains the s- phase and s- phase will convert into the various states and then finally we find the gametes and Zygote. This is the basic cell growth in any baby. But it system contain the same cell growth rate.

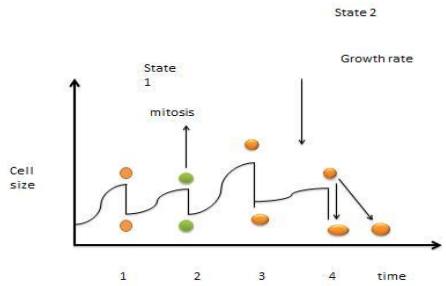


Figure 6 Growth rate in cells

The sensing system will have capacity to fetch the cell image in very fast speed.[5]

It also contains the wave length that can visible or invisible by user and it will operate with the help of some power supply AC/DC.

The sensing system also contain the controller of rays it have responsibility to control the power supply and wave length in emergency situation. [13][14][3]

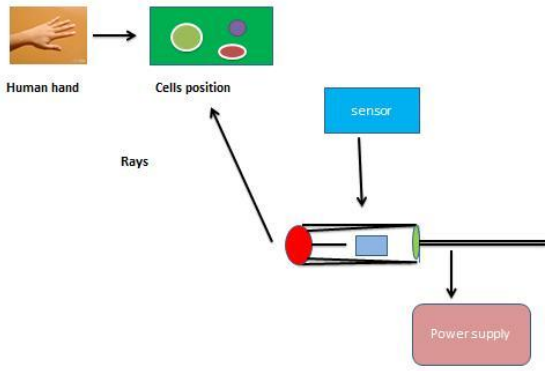


Figure 7: Basis sensing system

The cell growth is fully depend on the time means if we calculate the growth rate in following time then we can assume correct time by help of some mathematical operation.

The cell time and cell growth is also proportional to each other.[9]

3(b) Sensing System Architecture

The sensing system contains the all type of parameter that is same like physical machine and this machine is able to detect the cell position in the form of image.[14]

And image is detected by some rays or sensor. The sensor parameters have the following property like frequency of rays, measuring speed, and so on.

It uses some limited frequency that can able to detect the cell image from human body and can do calculation in system and can display the correct age.

3(c) Neural network architecture:

This system will sense the various images in seconds. If images are in large quantity then in this

situation we can use the neural network to handle the large data and can find the best solution.[1][6]

The neural network takes the various images in form of Analog image the digitalizer converts the digital image. Then after this operation it uses various mathematical algorithms to measure the cell time regarding the cell growth. And their numerical values will be analysed by neural network. It is used when you want to handle the large number of data.[15]

It contains the various learning algorithms that help to learn the data according to the performance. The neural network is also recovering the small problem that generate in execution.

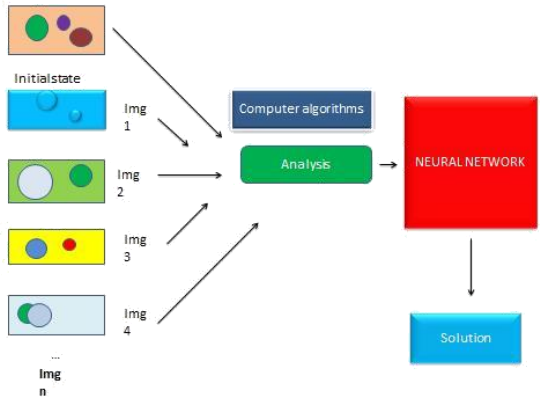


Figure8: Image handled by neural network

RESULT

Result of following detection system can gives not 100% sure result but it will match the 80% cell from body and can show the result on screen that following human have that age.[5][8]

Suppose due to any reason one time skin detection fails then we need to detect the skin more than one time.[2][4]

The output is totally based on the cell detection and its growth.[7]

If we detect the any cell from body that are changed with respect to time. If all system will connect the systematic manner then we can find the best result.[10]

APPLICATION

It contains the following application in real life implementation.

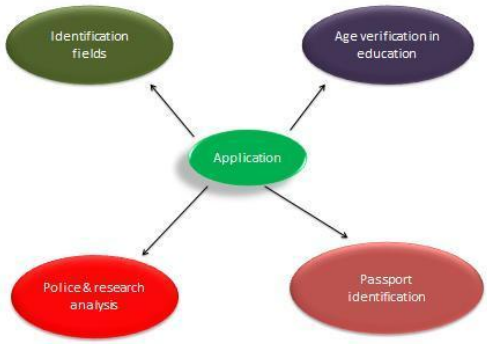


Figure9 Application of correct age detection system

LIMITATIONS

This system contains the following limitation.

I. This will contain large size and used medium complexity.
J. Its rays can be harmful for health or human skin.
K. If any user has cancers then they can generate problem to detect the cells.
L. System can low reliable to detect image pattern or analysis because it has huge amount of data.

FUTURE WORK

The human correct age detection system contains the complexity because when it measure the cell position then it generate huge amount of data for processing in form of images. It has low accuracy Accuracy can be enhanced in future and it can be able to give best result to current system.

The system size will also be very huge, in future its size, shape, complexity, accuracy, reliability, will become better.

References

[1] Artificial intelligence by Russell & Norving 3rd Edition.

[2] Dean , T. Allen , j. & Aloimonos, Y Artificial intelligence theory and practise.

[3] French, S. decision theory – an introduction to the mathematics of

rationality and application.
[4] Ekert , Arthur ,Quantum computing cryptoanalysis: an introduction
[5] Deutsch , david(1992-01-06) quantum computation physical.
[6] Harnd, stevan(2001) "Minds, machine and turing test
[7] Murrary , Andrew, and Tim hunt. Cell cycle: an introduction. New york: W. H. freeman and company, 1993.
[8] Hartwell, Leland H.,and T.A weinert. "check point: control that ensure the order of cell cycle events." Science 246(1989):629_634.
[9] Padte NN, Martin SG, Howard M,chang F(December 2006) " the cell end factor pom1p in specification of the cell division plane in fission yeast.
[10] Stephen hawkings "a brief history of time"
[11] Nahin, paul J.(2001) time machine: the time travel in physics:
[12] Physics of impossible by Micho kaku.
[13] Ackerman, Eugene,Biophysical science, prentice – hall 1962. Considerable material on vision from a medical point of view.
[14] Trpkovski, S.; Wade, S.A; Baxter, G.W; Collins, S.F(2003)."Dual emperature and strain sensor using a combind fiber Bragg grating and fluorescence intensity."
[15]Eaton, H.A.C and T.L Oliver (1992), learning coefficient dependence on training set size, neural network, volJ .5,and pp.28- . 288.

Comparative study of medical image segmentation techniques

Vartika Agrawal,
Jaypee Institute of IT Noida, India
vartika5290@gmail.com

Dr. Satish Chandra
Jaypee Institute of IT Noida, India
satish.chandra@jiit.ac.in

***Abstract* - Recent advances in imaging techniques have made it possible for the medical practitioners to view the details of abnormalities present in human body. Since last few years many techniques have been devised and implemented which can be used in conjunction with the imaging devices so as to diagnose automatically the medical problem existing a human body. There are many segmentation techniques which can be used in the analysis of a medical image. This paper presents a comparative study of such techniques.**

Keywords – Computed Tomography; Threshold based segmentation; Edge Based Segmentation; Region Based Segmentation; Atlas Based Segmentation;

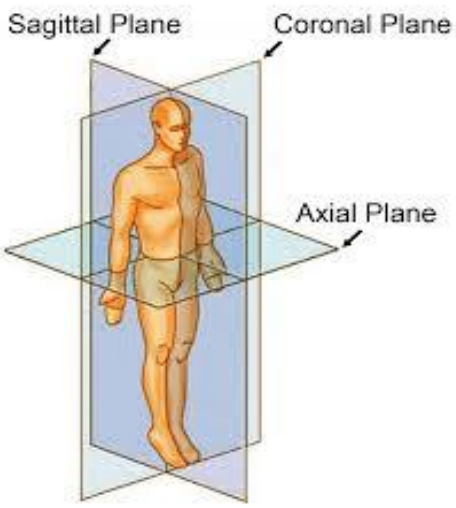
INTRODUCTION

Digital Image processing has applications in fields ranging from engineers to doctors and many more [1]. Many diseases and abnormalities are diagnosed with the help of image modalities varying from X-ray, Ultra Sonography (USG) to fMRI. Recent advances in imaging techniques have made it possible for the medical practitioners to view the details of abnormalities present in human body. Since last few years many techniques have been devised and implemented which can be used in conjunction with the imaging devices so as to diagnose automatically the medical problem existing a human body. Images allow us to peek inside the human body providing with views of anatomy and physiology, due to which in present scenario there is rarely any diagnosis done without the involvement of imaging. Improved medical image techniques has led diagnoses increasingly accurate and render precise which has helped in providing significantly improved medical care to patients. After the discovery of X-Rays by Wilhelm Conrad Rontgen in 1895 [2] there was a worldwide veritable boom especially in medicine field. Later on other modalities such as USG, CT Scan, MRI, fMRI etc. were discovered for better and detailed view of the lesion present. This paper focuses on how the medical images of various modalities have been used in the diagnosis of abnormalities present in human body [3]. The main focus is on the computed tomography (CT) images.

MEDICAL IMAGING MODALITIES

Computed tomography (CT)

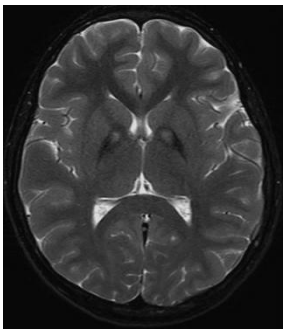
Development of computed tomography (CT) took place in 1972 as a result of ability of computer to perform complex mathematics to reconstruct and process images [4], [3]. This mathematics is based on radon transformation [5]. CT is also known as image reconstruction from projection, CAT (Computerized Axial Tomography) which is a natural progression from x-rays and principle of 3-D object reconstruction from its 2-D projection. CT is mainly used in the diagnosis of tumor, calcifications, acute and chronic changes in the lung parenchyma, pulmonary embolism, and abdominal diseases. [3]. Figure shows the three types of views from which a CT-Scan image can be obtained.



Three types of views from which a CT-Scan image

Magnetic Resonance Imaging

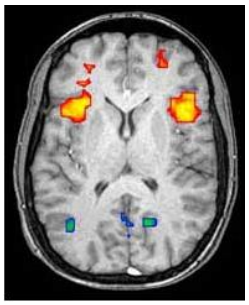
MRI was invented by Paul C. Lauterbur in 1971, which used magnetic field and radio waves to create detailed images of organs and tissues within a body. MRI images are used to determine the severity of injuries, blood vessels, breasts, bones, abnormal tissues etc. can also be examined. MRI has shown excellent results in contrast of soft-tissues but in some cases MRI is not capable of discriminating benign from malignant lesions [4] [6] [3]. MRI segmentation is mainly focused in [7].



Brain MRI with much lower connectivity in basal ganglia

Functional MRI

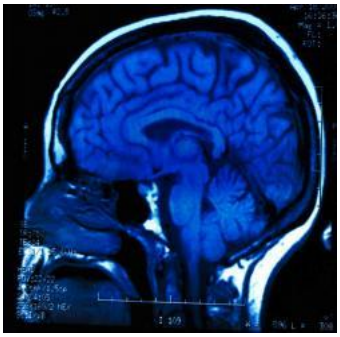
fMRI is an imaging technique that measures the brain activity by detecting the changes in blood flow, which came into existence in 1990s as a result of efforts of Seiji Ogawa and Ken Kwong. It is a neural-imaging procedure which focuses on changes in cerebral blood. fMRI produces activation maps by capturing the physiological changes and representing the parts of brain involved in a particular mental process. In this paper we are considering medical images using CT scan using only. There are many others also [4] [8] can be referred.



Axial MRI slice at the level of the basal ganglia, showing fMRI BOLD signal changes overlaid in red (increase) and blue (decrease) tones.

Positron Emission Tomography (PET)

Positron Emission Tomography (PET) is a nuclear imaging technique that provides physicians with information about how tissues and organs are functioning. PET, often used in combination with CT imaging, uses a scanner and a small amount of radiopharmaceuticals which is injected into a patient's vein to assist in making detailed, computerized pictures of areas inside the body. PET is often used to evaluate: Neurological diseases such as Alzheimer's and Multiple Sclerosis, Cancer, Effectiveness of treatments, Heart conditions.



PET for Brain Cancer

THE PROBLEM OF AUTOMATIC DIAGNOSIS

Automatic Diagnosis has become the necessity in today's world in each and every aspect of life [9]. But for this paper our focus is over the medical needs. Capacity to timely consideration of relevant options and consequences of a particular task will differ from individual to individual; judgments are made informally by concerning physicians or other health experts or family members many a times. These judgments or assessments are based on common sense and past experiences which sometimes can exclude a minor but an important detail and may lead to some severe problem in future. With the aim of health care software systems to operate efficiently in

runtime environment, so as to meet patient's needs, practitioners also require these systems for timely and error-free information. Thus leading to automatic diagnosis [8] as a necessity, advances in the development of automatic system help in timely detection, reporting and treating diseases.
Major issued with automatic diagnosis is dependence over hardware and high complexity which can conflict at runtime known as model based diagnosis which help in building distributed health care software systems. However, all such systems are complex and augmenting hardware with software so as to control the functioning of the system is much more complex. This complexity is addressed by probabilistic hierarchical constraint-based automat (PHCA) [9].

IMAGE SEGMENTATION METHODS

For most of the applications like image recognition or compression, whole image cannot be used directly. Therefore, image segmentation is a fundamental step used in data extraction and analyses of an image, which serves the basic purpose of division of images into non-overlapping regions, that is into useful structures. Image segmentation is middle and a crucial step which directly influence the overall understanding from an image.
There is a broad categorization of image segmentation techniques [10] [8] [3] some are mentioned below:

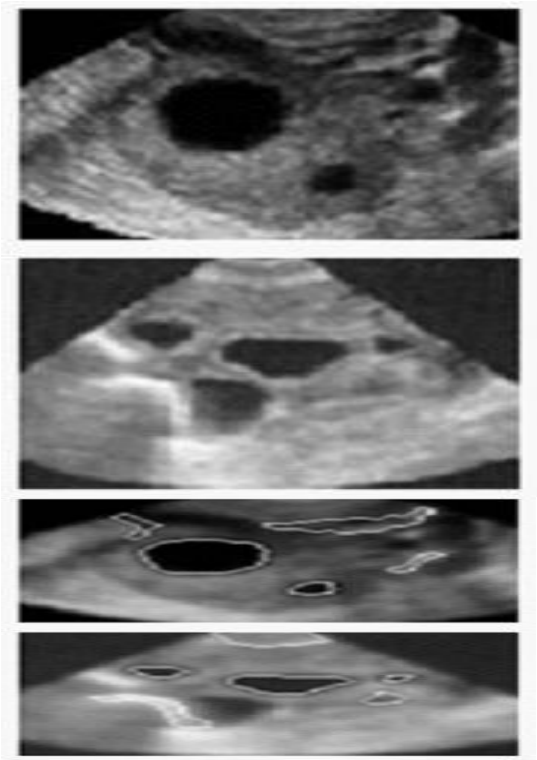
Threshold based segmentation
Thresholding is one of the simplest and way of segmentation which is probably most frequently used [10]. In thresholding process multilevel image is converted into a binary image. It can be done automatically or manually, depending on the user requirement. Thresholding can be further categorized as global and local. Consider a threshold value't', 'v' representing grey value of an image and a operation 'g' is defined by [10]:

$g(v) =$

There are some of the notable drawbacks of thresholding, its inability to segment complex images and selection of appropriate threshold value. For more work on threshold based image segmentation [11].

Input image (left) and output image (right) after thresholding based segmentation [12]

Edge Based Segmentation
Edge based segmentation is based on detection of edges i.e. boundaries which separate distinct regions. With the help of edges detected different discontinuities in the images are identified, after image identification as per the requirement obtained result can be classified using any classifier like SVM (Support Vector Machine), KNN (K Nearest Neighbor) [10]. There are various edge detecting inbuilt operators are present in MTALAB which allow us to perform edge based segmentation over an image like Prewitt, Sobel, Roberts (1^{st} derivative type) and Laplacian (2^{nd} derivative type), Canny [13] [3].



Input image (left) and output image (right) after edge based segmentation.

Region Based Segmentation

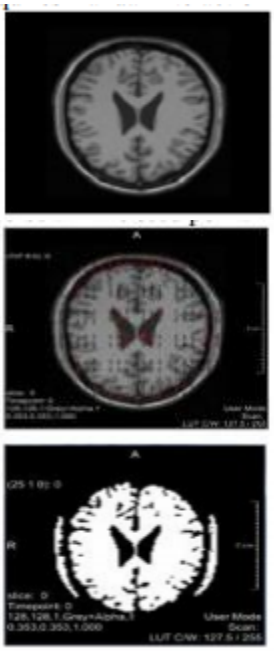
Region based segmentation is based over the homogeneity of pixels and is related to pixels form cluster and thus a segmented region is obtained. Region based segmentation can also be termed as 'Similarity Based Segmentation'. Two basic operations involved are splitting and merging [10].

Algorithm for segmentation using merging:

(1) Initial segmented image is considered
(2) Similar adjacent segments are merged, similarity criteria is defined.
(3) Step 2 is repeated until no segments are left to be merged

Algorithm for segmentation using splitting:

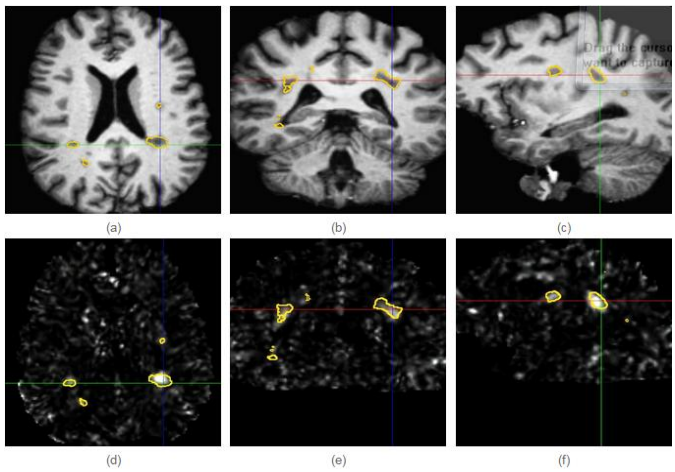
(1) Initial segmented image is considered
(2) Split inhomogeneous segments, inhomogeneous criteria is defined.
(3) Step 2 is repeated until all segments are homogeneous.



Input image (left), image with seed points (middle) and output image (right) after region based segmentation [12].

Atlas Based Segmentation

Atlas based segmentation is a technique of extracting contour from medical images, in this data is stored in database names as atlas. Each atlas is first registered with target image to obtain set of deformed labels and transformations are applied to gain final result [1] [3].



Voxel-wise z-scores for a given ms patient. Illustration of the z-score maps obtained for a patient (images (d), (e), (f)) compared to the corresponding anatomy (axial (a), (d), coronal (b), (e) and sagittal slices (c), (f)). The contours correspond to the manual delineations of the MS lesions.

Peter Karasev, Ivan Kolesov, Karl Fritscher, Patricio Vela, Phillip Mitchell, and Allen Tannenbaum [14] have thrown light over mistrust of doctors and patient on fully automated medical systems. Segmentation is core step of diagnosis, algorithms available for segmentation uses iterative methods with respect of time but the results are not accurate enough, so as to overcome its drawback. Partial differential equation is used to model the space-time relationship between image data and segmentation boundaries. As a result author noticed that at nominal level set PDE is assumed to give correct result but do not agree with human expert's decision [3]. For achieving trustworthy results author has tried to develop a system which requires constant interaction with the user, so synthesis problem can be controlled. Technique's effectiveness was tested over shattered femur CT images and parallel tendon MRI. In the end author was able to conclude that with less effort and time desired segmentation results are obtained.

Bjoern H. Menze_y, Andras Jakaby, Stefan Bauery, Jayashree Kalpathy-Cramery, Keyvan Farahaniy, Justin Kirbyy, Yuliya Burreny, Nicole Porzy, Johannes Slotboomy, Roland Wiesty, Levente Lanczi, Elizabeth Gerstnery, Marc-Andr´e Webery, Tal Arbel, Brian B. Avants, Nicholas Ayache, Patricia Buendia, D. Louis Collins, Nicolas Cordier, Jason J. Corso, Antonio Criminisi, Tilak Das, Herv´e Delingette, C¸ a˘gatay Demiralp, Christopher R. Durst, Michel Dojat, Senan Doyle, Joana Festa, Florence Forbes, Ezequiel Geremia, Ben Glocker, Polina Golland, Xiaotao Guo, Andac Hamamci, Khan M. Iftekharuddin, Raj Jena, Nigel M. John, Ender

Konukoglu, Danial Lashkari, Jos´e Ant´onio Mariz, Raphael Meier, S´ergio Pereira, Doina Precup, Stephen J. Price, Tammy Riklin Raviv, Syed M. S. Reza, Michael Ryan, Duygu Sarikaya, Lawrence Schwartz, Hoo-Chang Shin, Jamie Shotton, Carlos A. Silva, Nuno Sousa, Nagesh K. Subbanna, Gabor Szekely, Thomas J. Taylor, Owen M. Thomas, Nicholas J. Tustison, Gozde Unal, Flor Vasseur, Max Wintermark, Dong Hye Ye, Liang Zhao, Binsheng Zhao, Darko Zikic, Marcel Prastaway, Mauricio Reyesyz, Koen Van Leemputyz [15] authors have tried to automate brain tumor segmentation and performance of algorithms is evaluated by applying a Multimodal Brain Tumor Image Segmentation Benchmarks (BRATS) challenge in conjunction with the international conference on Medical Image Computing and Computer Assisted Interventions (MICCAI). The results of segmentation algorithms were compared. A higher quality automatic segmentation algorithm in combination with hierarchical fusion algorithm is applied to automate image segmentation. The quality of segmentation algorithm is decided on the basis of Dice scores.

Dice (P, T) = ——————

Where ∧ is the logical AND operator, is the size of the set (i.e., the number of voxels belonging to it), and P_1 and T_1 represent the set of voxels where P =1 and T=1, respectively [15] [16].

Due to different variations observed, it has been concluded by the author that there is no perfect algorithm for segmentation but pooling of algorithms often leads to concrete results.

YuanBeen Chen and OscalTC Chen1 have presented the importance of segmentation in image analysis [11]. An image segmentation method based on different threshold values selected at run time for different areas. In addition on the basis of histogram of gradients a contour threshold is determined which enabled to obtain appropriate segmented region with least computational time. Sometimes in a medical image there is more than one region of interest which is needed to be extracted and this can be done with being sequentially involved in the system. For doing so author has divided an image in blocks and algorithm is applied on each block separately and then result is combined. Contour threshold generated by blocks will give better results saving much of computation time. The above stated method is capable of segmenting those objects which were performed by E-GVF snake even [17]. With the help of method proposed by author problems faced while using watershed method is also resolved to an extent and noise interference is also reduced which directly effects edge based segmentation[13].

Xu Gongwen, Zhang Zhijun, Yuan Weihua, Xu Li'na [18] have thrown light over image segmentation using wavelet transform, a mathematical tool and proved improved result over traditional ones. As in a medical image mostly there is more than one region of interest so multi-threshold segmentation is used. But due to multiple threshold values image histogram will suffer with some impurities in image in noise form. Wavelet transform possess good features in both time and frequency domain. Quality of the signal produced is dependent on SNR (signal to noise ratio) as SNR is inversely proportional to signal quality.

Andrea Valsecchi, Pablo Mesejoyx, Linda Marrakchi-Kacemz, Stefano Cagnoniy and Sergio Damas [19] have proposed hybrid approach over image segmentation, combining edge and region based segmentation [3], and parameter optimizing technique which is from evolutionary computing. In this paper Genetic Algorithm is considered and overall performance is analyzed ranging from image registration to parameter learning but all these techniques are very mostly application specific [20]. For accurate results multiple features are required to be detected which can be done only with some prior knowledge of segmentation. Author has used atlas based segmentation in first phase as it requires image registration to be done at first and will be effective in terms of both speed and accuracy and then genetic algorithm is applied [20]. For performance estimation mean, median and standard deviation is computed and 20 repetitions is done per image. In finally it's observed that the whole set up showed best result for bio-medical images. Wilcoxon test proved with highest confidence HLS-GA (Hybrid –Level set and Genetic Algorithm) has edge over other methods.

Ricard Delgado-Gonzalo, Virginie Uhlmann, Daniel Schmitter, and Michael Unser [21] have told about the importance of need of microscopy and how it is effected by technological achievements. Author has worked over SNAKE (active contour) for image segmentation [17]. SNAKE is a technique which faces challenges many challenges like Robustness, stability, multi target interaction, computational efficiency etc. and it's a human interaction technique [3]. In fact in case of SNAKE being human interactive, its framework is not easy to implement as parameters are controlled by the control points and generator basis function. But due to its easy working it attracts researcher's especially biological imaging and due to its versatile nature which makes it suitable for problems which need the combination of segmentation and reconstruction of cell lineages.

Farzad Khalvati, Cristina Gallego-Ortiz, Sharmila Balasingham, and Anne L. Martel [16] have presented a robust atlas based segmentation algorithm for segmentation of MRI images of breast. Authors have used atlas in combination with of phase congruency maps instead of intensity variations proceeding further to more robust results. Efficiency of the algorithm was measured on the basis of Dice similarity coefficient and for both cases high accuracy is obtained [15], [16]. A new approach is proposed by the authors which combines atlas selection method and probabilistic atlas generated. Two configurations are presented namely: intra sequence and inter sequence. In Intra Sequence Setting, goal is to get accurate results so construction is done in two phases clustering function and probabilistic atlas building. It was observed with the increase in atlas classes there in failure cases. In Inter Sequence setting atlas and target images from different imaging sequence is taken so as to bring details of image structure in an image in notice. Thus improving the practical use of the algorithm and increase the usability of an atlas. Here with the help of proposed algorithm it was found that less number of cases are needed to create probabilistic atlas.

Wireless Sensor Networks have emerged as an important new area in wireless technology. In the near future, the wireless sensor networks are expected to consist of thousands of inexpensive nodes, each having sensing capability with limited computational and communication power which enable us to deploy a large-scale sensor network.

References

[1]. Fitzpatrick, J. M., & Sonka, M. (2000). *Medical Image Processing and Analysis*. SPIE Press.

[2] . Linton, O. W. (1995). Medical applications of X-rays. *Beam Line*, *25*(2), 25-34.

[3]. Angenent, S., Pichon, E., & Tannenbaum, A. (2006). Mathematical methods in medical image processing. *Bulletin of the American Mathematical Society*, *43*(3), 365-396.

[4]. Ammari, H. (2008) *An Introduction to Mathematics of Emerging Biomedical Imaging*. Springer.

[5]. Høilund, C. (2007). The radon transform. *Aalborg University, Vision, Graphics and Interactive Systems (VGIS), November*, *12*.

[6]. Zhu, H. (2003). Medical Image Processing Overview. *University of Calgary, Summer School Program-Introduction to Mathematical Medicine, held at the University of Waterloo. MIDDLE EAST JOURNAL OF INTERNAL MEDICINE*, *2*(3), 21.

[7]. Pham, D. L., Xu, C., & Prince, J. L. (2000). Current methods in medical image segmentation 1. *Annual review of biomedical engineering*, *2*(1), 315-337.

[8]. Sharma, N., & Aggarwal, L. M. (2010). Automated medical image segmentation techniques. *Journal of medical physics/Association of Medical Physicists of India*, *35*(1), 3.

[9]. Mikaelian, T., Williams, B. C., & Sachenbacher, M. (2005, September). Autonomous diagnosis based on software-extended behavior models. In*Proceedings of the 8th International Symposium on Artificial Intelligence, Robotics and Automation in Space-iSAIRAS*.

[10]. Ashburner, J., & Friston, K. J. (2003). Image segmentation. *Human Brain Function*.

[11]. Yuan Been, C., & Oscal T-C, C. (2009). Image segmentation method using thresholds automatically determined from picture contents. *EURASIP Journal on Image and Video Processing*, *2009*.

[12]. Vkumar, M., & MG, S. (2012). Performance comparison on medical image segmentation algorithm. *IJIPVS. (ISSN. 2278-1110), vol-1, iss-3, 4*.

[13]. Yogamangalam, B. K. R., & Karthikeyan, B. (2013). Segmentation Techniques Comparison in Image Processing. *IJET (ISSN: 0975-4024)*, *5*(1), 307-313.

[14]. Karasev, P., Kolesov, I., Fritscher, K., Vela, P., Mitchell, P., & Tannenbaum, A. (2013). Interactive medical image segmentation using PDE control of active contours. *Medical Imaging, IEEE Transactions on*, *32*(11), 2127-2139.

[15]. Menze, B., Jakab, A., Bauer, S., Kalpathy-Cramer, J., Farahani, K., Kirby, J. ... & Shotton, J. The multimodal brain tumor image segmentation benchmark (BRATS) (2014). *URL http://hal. Inria. fr/ hal-00935640*.

[16]. Khalvati, F., Gallego Ortiz, C., Balasingham, S., & Martel, A. (2015). Automated Segmentation of Breast in 3D MR Images Using a Robust Atlas.

[17]. Kass, M., Witkin, A., & Terzopoulos, D. (1988). Snakes: Active contour models. *International journal of computer vision*, *1*(4), 321-331.

[18]. Gongwen, X., Zhijun, Z., Weihua, Y., & Li'Na, X. (2014, June). On Medical Image Segmentation Based on Wavelet Transform.

In *Intelligent Systems Design and Engineering Applications (ISDEA), 2014 Fifth International Conference on* (pp. 671-674). IEEE.

[19]. Valsecchi, A., Mesejo, P., Marrakchi-Kacem, L., Cagnoni, S., & Damas, S. (2014, July). Automatic evolutionary medical image segmentation using deformable models. In *Evolutionary Computation (CEC), 2014 IEEE Congress on* (pp. 97-104). IEEE.

[20]. Maulik, U. (2009). Medical image segmentation using genetic algorithms.*Information Technology in Biomedicine, IEEE Transactions on*, *13*(2), 166-173.

[21]. Delgado-Gonzalo, R., Uhlmann, V., Schmitter, D., & Unser, M. (2015). Snakes on a Plane: A perfect snap for bioimage analysis. *Signal Processing Magazine, IEEE*, *32*(1), 41-48.

Android-Security Enhanced Linux

Nitish Kr Gupta
Ajay Kumar Garg Engineering College
Nitish-Gupta@outlook.com

Khushboo Singh
Ajay Kumar Garg Engineering College
khushboosingh@outlook.com

Prof J K Seth
Ajay Kumar Garg Engineering College
mrjkseth@gmail.com

***Abstract* -Users are now able to shop online, share information with the applications that they install on their smart devices. According to the information that Google provided in September 2012, 500 million Android devices have been activated [1].The increasing popularity of smart devices have led users to complete all of their daily work with these devices. Installed applications gain access to various sensitive information, such as the user's contact list, phone number, location. However, there is no control mechanism in place that can check whether these applications are safe to install. Therefore, applications are installed according to the users‘ decisions, without any limitations or warnings. As a result, users become the target of malicious applications, and the personal security and privacy are compromised. In this study, we investigate the security solutions that aim to protect the privacy and security of Android users. We reveal the shortcomings of mobile security solutions and shed light on increasing Android security using SELinux.**

INTRODUCTION

According to the information that Google provided in September 2012, 500 million Android devices have been activated [1].There is a large number of operating systems that are used for mobile devices. Through use of these operating systems, Android continuously increases its popularity and market share. In addition, the open-source nature of the Android platform, the ease of application development and the submission process with the application Anyone who wants to develop Android-based mobile applications is able to submit his/her application to Google's application store without any problems. The applications that are developed can compromise personal security, privacy and user experience by misusing sensitive information, such as photos, the contact list, e-mails, documents, SMS, calling services, the battery and the camera. store have made this platform more attractive. However, security risks and threats have increased and continue to increase more so than for other mobile platforms, such as Apple's iOS. This misuse of sensitive information is the most important and indispensable problem that affects these users and mobile devices.

ANDROID OPERATING SYSTEM

Android is an open-source, Linux-based operating system that was developed under the leadership of the Open Handset Alliance (OHA) and Google. The platform was previously developed by Android Inc., which was a Silicon Valley-based company. In 2005, Google acquired this company, and the Android operating system became a growing, developing platform. After 3 years of development, the first Android-based mobile device was available for sale in November 2008. Table 1 shows the milestones of the Android platform.

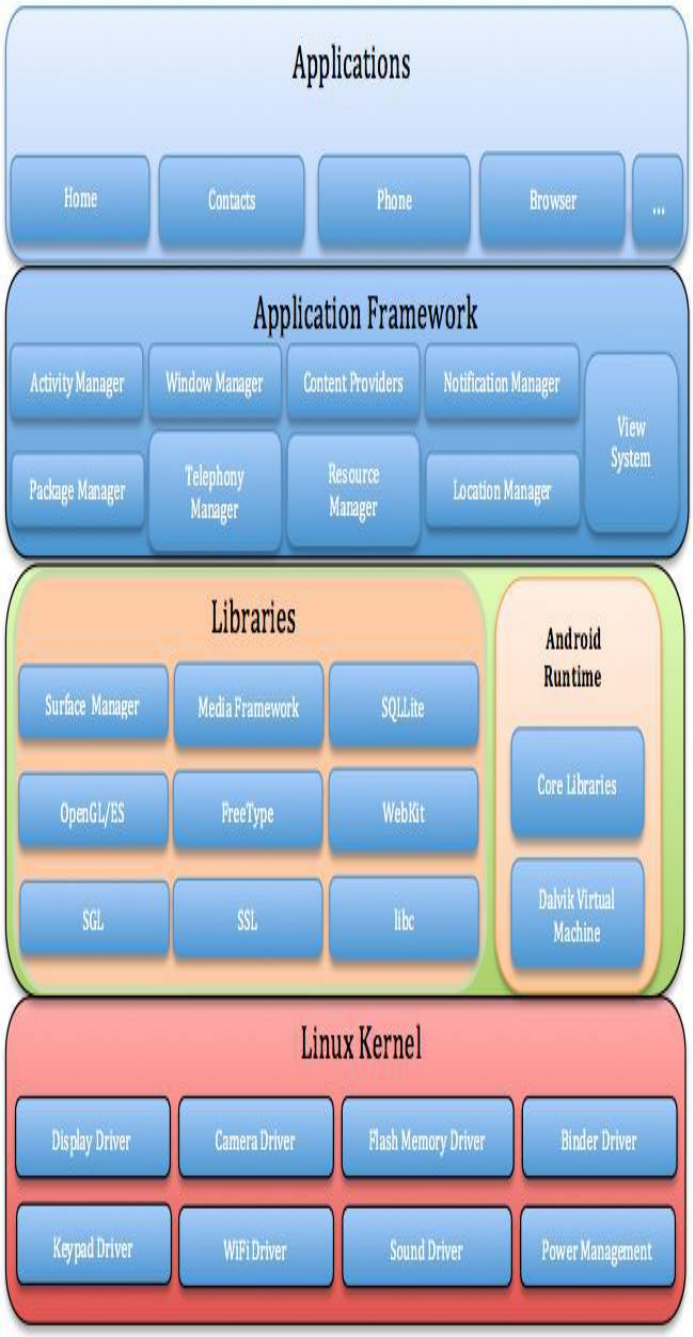
Table 1. Milestones of Android Platform [2]

Date	Event
1 July 2005	Google acquired Android Inc.
12 November 2007	Android was released.
28 August 2008	Android Market was announced.
23 September 2008	Android 1.0 platform was released.
21 November 2008	Android was released as open-source.
13 February 2009	Paid applications were accepted in the USA Android Market.
2009-2013	Android platform was updated to new versions and It continues to be updated. Latest version is Android 4..5.1 Lollipop

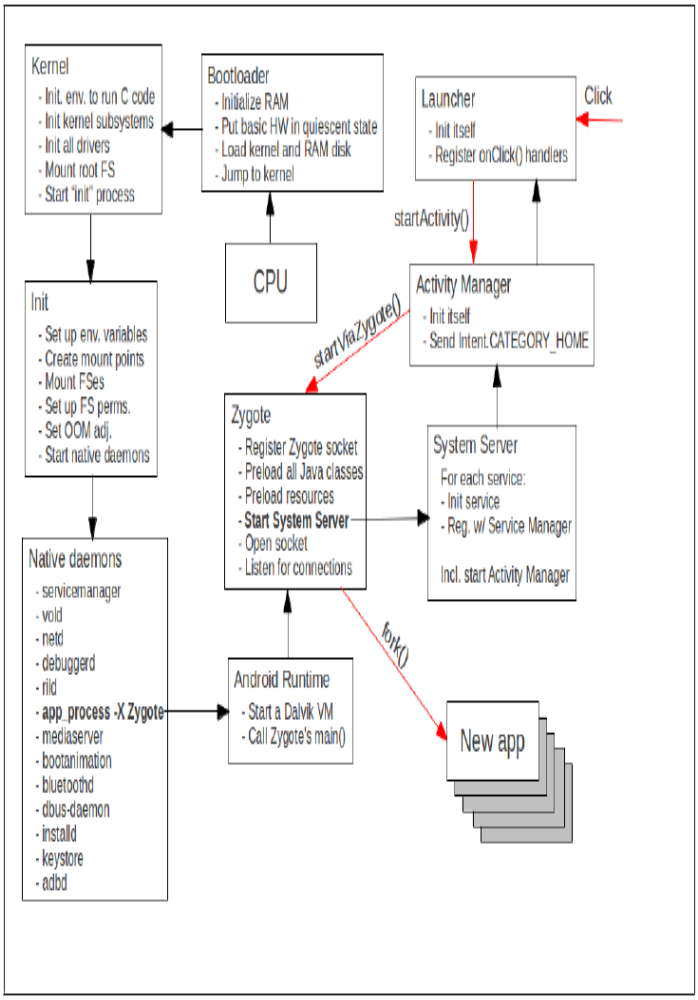
ANDROID ARCHITECTURE

Android architecture [5] is comprised of 5 basic layers, and each layer has different program groups. The following list provides these layers [2]:

- Application Layer
- Application Framework Layer
- Library Layer
- Runtime Layer
- Linux Layer



Dalvik Virtual Machine Process [6]



1) Linux Layer: This layer resides at the bottom of the architecture. Although developers and users do not have a direct communication with this layer, it is the heart of the whole system. It provides following functions in Android system:

- Abstraction for hardware
- Memory Management
- Security
- Power management
- Hardware drivers
- Support for shared libraries
- Network connection
- A Binder framework for inter-process communication

2) Library Layer: This layer resides on top of the Linux kernel layer and includes several libraries. These libraries provide functionalities that can handle various data. For instance, the Media Framework is responsible for the management of how different types of videos or audio will be played. The following list provides other open-source libraries that are included in this layer:

- **Surface Manager:** Responsible for the management of windows on the screen.
- **SGL:** Graphic library that provides 2D functionality.
- **OpenGL/ES:** Graphic library that provides 3D functionality.
- **Media Framework**: Responsible for audio, vide playback, recording, photo display, etc.
- **Freetype:** Library that manages fonts.
- **Webkit:** Browser engine.
- **Libc:** System C library.
- **SqlLite:** Serverless SQL database.
- **Open SSL:** Security library.

3) Runtime Layer: This layer is located in the same level as the Library layer. It contains a Dalvik Virtual Machine (DVM) and Java libraries for users that are used in the development of applications. The virtual machine requires the applications to run on Android devices. It is register-based and optimized for low memory requirements. It runs on the application codes that are converted from Java class files to DVM compatible DEX files.

4) Application Framework Layer: This layer is where the developed applications directly communicate. The applications manage the basic functionalities, such as phone resource management, sound management and call management. The management applications include the following:

- **Activity Manager:** Responsible for the activity life cycle of applications.
- **Content Provider:** Responsible for data exchange between applications.
- **Telephony Manager:** Responsible for all of the voice calls.
- **Location Manager:** Responsible for location management by using GPS coordinates and cell towers.
- **Resource Manager:** Responsible for the management of resources that are used by applications.

5) Application Layer: This is the top level layer in Android architecture in which the standard applications reside and where users have the most interaction by making calls, receiving calls, surfing online, etc. The layers where the developers and programmers have the most interaction are the layers that are between the Linux Kernel layer and this layer.

Security Threats-Current Scenario

Attack Vectors

In this section we evaluate the security concept of the Android platform against common attack vectors, known from desktop systems, and against new vectors, which are specific to mobile systems [1].Attack vectors are paths through a security concept that can be used in order to elevate permission levels, gain access to the system or data, which are stored on the system. Attacks on Android devices are motivated by different attack goals. Android devices have significant value to serve as bot in a botnet due to the fact that these devices are always on and most of the time connected to the internet. This is one of the most important threats for today's computer systems and has also been found on Android [7]. Another goal could be to steal credentials for online services or private data like emails, contacts and pictures. Compared to desktop systems it is easier to gather and find such information due to the fact that the platform provides functionalities to access them and that in most cases it is well known where these information are stored. Furthermore, it is very likely that these information are up to date and therefore more valuable, because these devices are designed and mainly used to communicate which e.g. needs up to date contact information. Another new attack goal, that comes with smartphones, is to capture mTans, which are send via the short messages service (SMS). These mTans are used by online banking systems, when the user initiate a new bank transaction. Then an SMS with a mTan is send in order to have a two-way authentication. So an attacker is interested in capturing this mTans.

Drive-by Exploitation

Drive-by Exploitation is an attack method that uses bugs within software, running on the device and processing external data. In most cases this attack vector is done using bugs within the web browser. While a user is surfing the web, the web browser gets data from server, processes this data, and displays it, so that the user can see the website. In case of a bug within the processing of this data, the attacker is able to execute code, also called payload, on the device. These bugs could be e.g. buffer or heap overflows. This kind of attacks have a big impact on the security of a system, because the attacker can execute malicious code without users knowledge. They have been seen a lot on desktop systems and therefore especially browser software have been hardened by further security mechanisms like sandboxing and memory protection mechanisms. But still, there are many bugs within browser and also contests are organized where the attendees have to find bugs and exploit them [8]. On the Android platform the situation is a little bit different, due to the fact that on desktop systems most of the software is implemented as native executable, which are prone to such bugs. On Android most of the software is implemented in Java and therefore executed within the Dalvik Virtual Machine (DVM). So, the combination of the Java language, which protects data structures by boundary checks, and the DVM protects against the exploitation of such bugs. So, these parts of an application are still vulnerable for such attacks. This e.g. apply to the Android default browser, which is distributed within every Android device. A proof of concept attack has been shown at the RSA conference [9]. On the one hand, the attack space for Drive-by Exploitation has been reduced, by using Java and DVM as a base for the major part of Android applications. On the other hand, some parts are implemented as native libraries and so they become vulnerable for such memory management bugs. Furthermore, a huge amount of Android devices are still running under older versions [10] and wound get updates in order to eliminate well-known bugs.

Phishing

A Phishing attack is used in order to gather information, especially credentials from a user by masquerading itself as an official instance. This can be done by sending faked emails or serving similar looking website e.g. for an online banking system. On the Android platform this also holds. But the situation here is different, because for most online services, which are used on mobile devices, there are also applications available to have a better user experience while using the service. Therefore, most users do not use the website directly, but use an application for this service. So in this case the attack vector can not be applied that easy because the application can not be tricked as easy as the user. Finally, for other use cases this attack vector is still applicable.

WebView

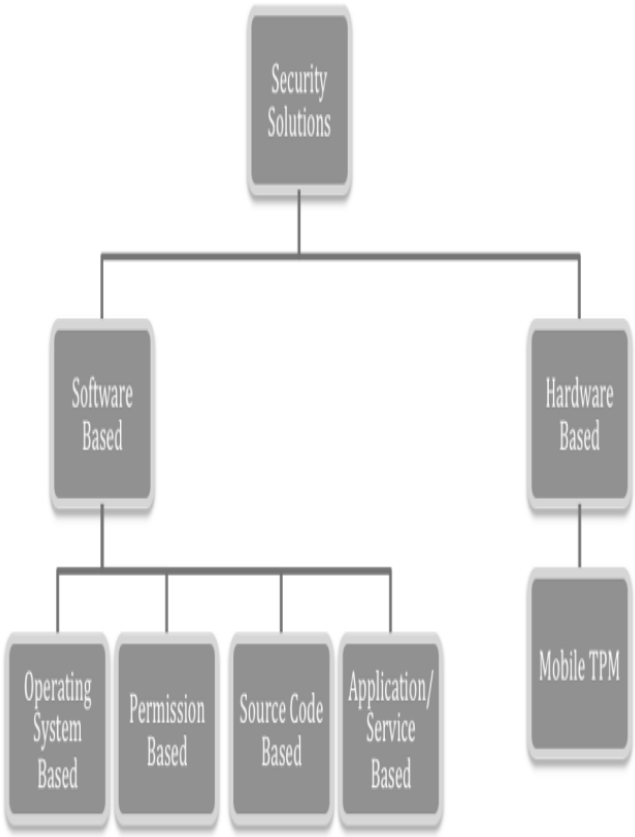
WebView is a new technique, specific to mobile devices, that enables applications to integrate a browser component and to have a well defined communication interface between the displayed website and the application. The

WebView feature comes with the WebKit framework and has been integrated into Android, because many applications want to integrate and display the content of a particular website, like e.g. social networks. Furthermore, these applications want to enrich the displayed content with locally available content like contacts. In this case, WebView can be used, which provides an interface so that a JavaScript component, integrated into the website, and a handler function within the application can communicate and exchange such data. Finally, this website can access data stored on the Android devices, if the application uses WebView. The same holds for other mobile platforms like iOS, where this technique is called UIWebView [11]. The attack vector can be described as the following. The user of an Android device is using an application, which integrates a WebView, in order to use an online service like a instant messenger which uses phone numbers to identify the communication partner. So, this service must have access to the locally stored contacts, which can be done using the WebView feature. So this service, which is implemented as a website, can access the contacts using JavaScript. In the case of an attacker can modify the website and integrate further JavaScript into it, which e.g. can be done using cross site scripting (XSS), he is able to use these functionalities of WebView to get access to contacts. This attack vector is specific to mobile platforms and is not possible on desktop system.

ANDROID SECURITY

Figure 2 shows the levels of Android security. The proposed solutions for Android security under two main titles: ―Software-Based Solutions‖ and ―Hardware-Based Solutions‖. Our emphasis is on permission based security.

Each API call in the Android operating system corresponds to a permission in the manifest file (AndroidManifest.xml) that contains the list of permissions. When a user installs an application, the list of permissions is presented to the user. When the permission is granted, API calls become active. However, users can only allow or reject all of the permissions and do not have the power to select certain permissions. Allowing many unnecessary permissions causes security and privacy problems. Once the permissions are granted at the installation time, there is no way of changing these permissions. Furthermore, the model does not support dynamic permission assignment. After an application is granted permissions, the users have no idea about how



the application will use the data on their devices and what effects it will have on privacy and security. Permission-based security solutions provide experimental analysis and practical solutions.

Kernel challenges

The first set of challenges to using SELinux in Android was in the Linux kernel. Even though SELinux is part of the standard Linux kernel, enabling the use of SELinux in Android requires more than merely enabling SELinux in the kernel build configuration. In order to provide per-file protection and to support automatic security context transitions on executables, SELinux requires that the filesystem provide support for security labeling. In Linux, the underlying storage for file security labels is typically provided through the use of extended attributes on files. However, the original preferred filesystem type for

Android devices was the yaffs2 filesystem, which is not part of the mainline Linux kernel and did not originally support extended attributes at all. More recently, yaffs2 has gained support for extended attributes, but still lacked the necessary support for automatic security labeling of newly created files.

Sandbox

Every application on the Android platform runs within its own sandbox by default. By this, the application is isolated from other applications except well-defined and system supervised interfaces like the IPC. In order to achieve this, the multiuser paradigm of the kernel is used by assigning individual user accounts to the installed applications. As a result, every application is executed as a different user and therefore its resources are protected and only accessible by the owning application itself. Data and files, which are stored by an application are also protected by default file system permissions in a way, that an application must explicitly grant permissions in order to allow other applications to get access to this data. This approach is well-known and used within unix server installations for years

To overcome this problem Google started a project to identify and address critical gaps in the security of Android. Initially, the project is enabling the use of SELinux (**Security-Enhanced Linux**) in Android in order to limit the damage that can be done by flawed or malicious apps and in order to enforce separation guarantees between apps. SELinux is LSM i.e. Linux Security Module SELinux is a set of kernel modifications and user-space tools that have been added to various Linux distributions. Its architecture strives to separate enforcement of security decisions from the security policy itself and streamlines the volume of software charged with security policy enforcement. Since Android's debut, apps have run inside a "sandbox" that restricts the data they can access and isolates code they can execute from other apps and the operating system as a whole. Built on a traditional Unix scheme known as discretionary access control, Android sandboxing prevents the pilfering of sensitive passwords by a rogue app a user has been tricked into installing or by a legitimate app that has been commandeered by a hacker.

Originally developed by programmers from the National Security Agency, SELinux enforces a much finer-grained series of mandatory access control policies. Among other things, SELinux allows varying levels of trust to each app and dictates what kind of data an app can access inside its confined domain.

Key facts about SELinux:-

- Security-Enhanced Linux* (SELinux) is an implementation of mandatory access control using Linux Security Modules (LSM) in the Linux kernel, based on the principle of least privilege. It is not a Linux distribution but instead a set of modifications that can be applied to UNIX*-like operating systems, such as Linux and BSD.
- Discretionary Access Control (DAC) is the standard security model for Linux. In this model, access privileges are based on the user identity and object ownership.
- Mandatory Access Control (MAC) limits privileges for subjects (processes) and objects (file, socket, device, etc.).

SELinux does not change any existing security in the Linux environment; instead, SELinux extends the security model to include Mandatory Access Control (e.g., both MAC and DAC are enforced in the SELinux environment).

SEAndroid enhances the Android system by adding SELinux support to the kernel and user space to:

- Confine privileged daemons to protect them from misuse and limit the damage that can be done via privileged daemons
- Sandbox and isolate apps from each other and from the system
- Prevent privilege escalation by apps
- Allow application privileges to be controlled at installation and runtime using MMAC
- Provide a centralized, analyzable policy.

The SEAndroid Policy

SEAndroid policy[4] is one of the cores of the entire SEAndroid security mechanism. In addition, the security architecture must also have a strict security policy to ensure that the access subject has only minimal access permissions to the object, so that the program can execute the basic functions but will be prevented from executing malicious operations.

As mentioned above, SEAndroid's implementation is in enforcing mode, instead of the non-functional disabled mode or the notification-only permissive mode, to act as a reference and facilitate testing and development.

The security context of SEAndroid is basically consistent with SELinux. The four parts, user, role, type, sensitivity, i.e., **u: object_r: system_data_file: s0** are described below:

- User: The security context of the first column is the **user** in SEAndroid and the only one that is **u**.
- Role: The second column indicates the **role** in the SEAndroid, **r** and **object_r**, respectively.
- Type: For the third column type, SEAndroid defines the 139 different policy types, such as **device type**, **process type**, **file system type**, **network type**, **IPC type**, and so on.
- Security level: The fourth column is designed for Multiple Level Security (extension MLS), which is the access mechanism to add security context and format sensitivity **[: category list] [- sensitivity [: category list]]**, for example **s0 - s15: c0 - c1023**, whereas the category may not be required in the current Android version. The combination of sensitivity and category together declares the current security level, and numbers are identified around the lowest and highest level of security. The parameters of this column are used in the MLS constraint checking, with "15" and "1023" representing the maximum sensitivity and category. This parameter range can be defined in the **Android.mk**.

The security context is the most important part of the third column type, and the process type is called**domain**. **Type** is the most important of SEAndroid parameters and the policy parameters are greatly expanded, so the system for each file marked with the appropriate type becomes extremely important.

The SEAndroid policy sources are located under **external/sepolicy**.

The policy consists of source files used to generate the SELinux kernel policy file, a **file_contexts**configuration, a **property_contexts** configuration, a **seapp_contexts** configuration, and a**mac_permissions.xml** configuration.

- The **file_contexts** configuration is used to label files at build time (e.g., the system partition) and at run time (e.g., device nodes, service socket files, /data directories created by init.rc, etc.).
- The **property_contexts** configuration is used to specify the security context of Android properties for permission checking purposes.
- The **seapp_contexts** configuration is used to label app processes and app package directories.
- The **mac_permissions.xml** configuration is the middleware MAC policy.

The device-specific policy sources are located under **device/<vendor>/<device>**.

- The device-specific policy can be specified by defining **BOARD_SEPOLICY_DIRS**,**BOARD_SEPOLICY_UNION** and/or **BOARD_SEPOLICY_REPLACE** variables in a**BoardConfig.mk file** under the **device/<vendor>/<device>** or **vendor/<vendor>/<device> directories**, i.e., the configuration file for Intel® Atom™ processor-based tablet (codenamed Bay Trail) FFRD8 is **"/device/intel/baytrail/BoardConfig.mk"**.
- An example can be found in **device/intel/baytrail/BoardConfig.mk**, which defines these variables to reference device-specific policy files under **device/intel/baytrail/sepolicy**.

- Documentation for per-device policies can be found in the **external/sepolicy/README**.

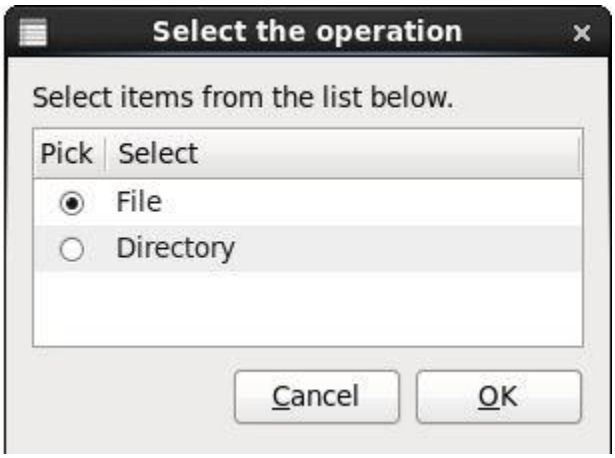
Proposed Systems

Android Application Sandbox Application sandboxing, also called application containerization, is an approach to software development and mobile application management (MAM) that limits the environments in which certain code can execute. The goal of sandboxing is to improve security by isolating an application to prevent outside malware, intruders, system resources or other applications from interacting with the protected app. The term sandboxing comes from the idea of a child's sandbox, in which the sand and toys are kept inside a small container or walled area. Android uses the concept of a sandbox [3] to enforce inter-application separation and permissions to allow or deny an application access to the device's resources such as _les and directories, the network, the sensors, and APIs in general. For this, Android uses Linux facilities such as process-level security, user and group IDs that are associated with the application, and permissions to enforce what operations an application is allowed to perform. Sandboxes are often located within kernel space since access to critical parts of the OS can be realized. The kernel is a very essential part of a system because it acts as bridge between hardware and software. One approach of sandbox systems is to monitor system and library calls including their arguments. This is often done trough system call redirecting, also known as system call hijacking. System calls, short system calls, are function invocations made from user space into the kernel in order to request some services or resources from the operating system.
Android uses a modi_ed Linux basis to host a Java-based middleware running the user applications. This implies that calls should not be monitored on Java level since other calls being made by native Linux application might get lost.

Our proposed system works on dynamic access permissions . SELinux used in enforcing mode allows to change permission as per user and application requirement i.e. allowing only operational level permissions. User can select the application to which the application data is accessible. Although the application is running in separate sandbox ,any application can access only limited resource of other application. We developed a prototype in which even the root user cannot modify the application data.
This achievement help in resisting the rootkit attack.

Experiment Model

Our system works on basic structure of linux on which android runs. We use access controlled commands in our module to control access to privileged data by other and root user. Following are the glimpse of our proposed system:



Choose the resource to be protected

Enter the application group who can access the resources

Priviliged user with full access

After the above three step operation access operation are executed . In our proposed policy root user can only read and append data but cannot delete it.

References

[1] Rheinische Friedrich-Wilhelms-Universitat Bonn, ¨ Germany 2015

[2] A Comprehensive Analysis of Android Security and Proposed Solutions
I.J. Computer Network and Information Security, 2014, 12, 9-20

[3] Introduction to Android 5 Security Lukas Aron and Petr Hanacek

[4] Security Enhanced (SE) Android: Bringing Flexible MAC to Android Stephen Smalley and Robert Craig,Trusted Systems Research

[5] Securing Android-Powered Mobile Devices Using SELinux Asaf Shabtai, Yuval Fledel, and Yuval Elovici Ben-Gurion University 2014

[6] Android Architecture Leon Romanovsky leon@leon.nu www.leon.nu

[7] X. Jiang. New rootsmart android malware utilizes the gingerbreak root exploit. Visited: Jun, 2012. [Online]. Available: http://www.cs.ncsu.edu/faculty/jiang/ RootSmart

[8] D. Alperovitch and G. Kurtz. Rsac us 2012 – hacking exposed: Mobile rat edition. Visited: May, 2012. [Online]. Available: http://365.rsaconference.com/community/archive/usa/blog/2012/03/15/ video-rsac-us-2012-hacking-exposed-mobile-rat-edition--dmitri-alperovitch-george-kurtz

[9] Google Inc. Current distribution. Visited: May, 2012. [Online]. Available: http://developer.android.com/about/dashboards/index.html

[10] T. Luo, H. Hao, W. Du, Y. Wang, and H. Yin, “Attacks on webview in the android system,” 2011.

CYANOGENMOD : A NEW ERA OF MOBILE OS

Shweta Yadav
Ajay Kumar Garg Engineering College Ghaziabad, India
Shwetayadav.jan@gmail.com

Yash Garg
Ajay Kumar Garg Engineering College, Ghaziabad, India
yashakgec@gmail.com

Ruchin Gupta
Ajay Kumar Garg Engineering College
Ghaziabad, India
skg11in@yahoo.co.in

***Abstract*—Mobile devices implementing Android operating systems provides many new and exciting features for users to enhance functionality and improve working environment provided by Google but there are set of restrictions that Google has made on the development of Android Operating System. A CyanogenMod community distribution of the Android operating system provides solutions that prevents data extractions, blocked the installation of unwanted tools, enhance security and provide easy environment for development of applications in the Android Market.**

About 1-2 years, the vanilla Android operating system (known as AOSP, Android Open Source Project) is internally developed then released to public by Google. CyanogenMod Community takes this newly developed code and modifies it and ports it into dozens of old and new devices, simultaneously, added new features, fixes bugs and provide improvements which Google didn't include in its code. Later, the CyanogenMod have appeared in never version of "official" Android and takes advantage of "code dump" by Google [1].

Our Main focus is to emphasize the features, modifications, customizations and enhanced security provided by the CyanogenMod and its current development in Android world which has taken the Android to new horizon and makes its development easier but such improvements are restricted by Google to maintain its stand in market place. Such Modifications are provided by CyanogenMod and further updates to the Android devices with easy installation at any required schedule.

INTRODUCTION

The word 'CyanogenMod' is formed from two words – 'Cyanogen', after its creator "Steve Kondik" who is also known as "Cyanogen" and 'Mod', which means "to modify". Hence the word 'CyanogenMod' means the modified firmware (of Android) developed by the Cyanogen (Steve Kondik).

CyanogenMod (pronounced /saɪ.'æn.oʊ.dʒɛn.mɒd/) is an enhanced open source firmware distribution for Smartphone and tablet computers based on the Android mobile operating system. It offers features and options not found in the official firmware distributed by vendors of these devices.

Features supported by CyanogenMod include native theming support, FLAC audio codec support, a large Access Point Name list, an Open VPN client, an enhanced reboot menu, support for Wi-Fi, Bluetooth, and USB tethering, CPU over clocking and other performance enhancements, soft buttons and other "tablet tweaks", toggles in the notification pull-down (such as Wi-Fi, Bluetooth and GPS), app permissions management, as well as other interface enhancements. CyanogenMod does not contain spyware or bloat ware. In many cases, CyanogenMod may increase performance and reliability compared with official firmware releases[8].

WHAT IS CYNOGENMOD ?

CyanogenMod is free and open source software. Open source software(OSS) is computer software that is available in source

code from which the source code and certain other rights normally reserved for copyright holders are provided under a software license that permits users to study, change, and improve the software. This means its source code is freely available to any person, and this offers you the freedom to personalize it according to your own needs – it's not about just changing the design or the theme, but anyone can take this software and modify it entirely. This also provides you the power to view the source code and catch any bugs or loopholes or backdoors in the software, being open source software, it's developed.

Steve Kondik started 'Cyanogen Inc.' in 2013 with a goal to commercialize his operating system. The objective behind his company is "to grow the open source project and to work with partners to share the freedom of user choice with the world", as stated by its website .CyanogenMod is the most popular custom ROM for Android devices, available for 350+ devices combining both of its official and unofficial ports. It is one of the oldest firmware for Android, still in active development.

CyanogenMod is a customized version of Google's Android operating system, and updates come directly from CyanogenMod itself, which makes the process significantly faster than it is for most other devices.

CURRENT ISSUE WITH CYANOGENMOD IN MARKET[2]

i. Microsoft is investing in a hot start up that's trying to weaken Google's hold over Android in the Android World.

ii. Microsoft is providing investment money to Cyanogen, which has the motive to developing a new version on Android mobile Operating System outside Google.

iii. Microsoft become a minor investor by financing about $70 million which provide benefits of about a high hundreds of millions to Cyanogen. The finance increases as it involves several other strategic investors that expressed their interest in Cyanogen but more importantly, they're also eager to diminish Google's control over Android.

iv. Since Microsoft has its own Windows Phone Operating System, so its investment would be unusual. Moreover, Windows phone has only about 3% of market Share which enforces Microsoft to proceed with such steps.

v. As we all know that Android is an "open source" operating system that enables hardware makers to deploy in their devices for free. Yet Google has frustrated manufacturers in recent years by requiring them to feature Google apps and set Google search as the default for users, in exchange for access to the search engine, YouTube, or the millions of apps in its Play Store.

vi. These restrictions have created difficulties for others to compete with Google, so as to win distribution on Android devices. But for Microsoft, this means less exposure for its Bing search engine, which stands up against Google search which could limit growth of other Microsoft software products.

vii. Cyanogen offers an alternate version of the Android mobile operating system free of such restrictions. The 80-person company claims to have a volunteer army of 9,000 software developers working on its own version of Android.

viii. "We're going to take Android away from Google," said Kirt McMaster, Cyanogen's chief executive, in a brief interview on Jan 29, 2015 12:47 pm. The next day, at an industry event sponsored by tech news service The Information, McMaster said Cyanogen had raised $100 million to date. Previously the company had disclosed that it raised $30 million of funding. The company spokeswoman declined to make McMaster available for this story.

ix. McMaster said more than 50 million people use a version of the Cyanogen Android operating system, most of whom have installed it in place of their phone's initial operating system.

x. Cyanogen started deals with hardware makers to install the software on their devices. Recently, a deal is signed between Indian Smart Phone maker Micromax and Cyanogen to ship handsets with Cyanogen's software to spread adoption among the people more quickly and is also announcing more such deals related to it.

xi. For Microsoft to distribute its apps and services on smartphones, a third mobile ecosystem that rivals Google and Apple could help Microsoft.

xii. "Cyanogen may have a greater chance than Microsoft to build a third ecosystem for mobile," says Rajeev Chand, managing director at Rutberg & Co., an investment bank focused on the mobile industry.

xiii. Independent versions of the Android operating system are already popular, particularly in China where Google has struggled to enter the market. In total, these other versions represented 37% of Android shipments world-wide in the third quarter, according to Strategy Analytics.

xiv. Smartphone makers and wireless carriers are looking for a standard bearer to offset Google's growing market power, Chand says.

xv. Prior investors in Cyanogen included Benchmark Capital, Redpoint Ventures, Andreessen Horowitz and Chinese social-networking giant Tencent. New venture capital investors are expected to join the strategic corporate investors in this latest round of funding.

RELATIONSHIP BETWEEN CYANOGENMOD AND ANDROID

CyanogenMod is built over Android. CyanogenMod is simply a different version or flavor of Google's Smartphone Operating System. It is very similar to reaching a same destination point but choosing different paths- this is the same situation with CyanogenMod, vanilla Android (AOSP) and various other ROMs.

This is the result of Android being an open source operating system. The open source Apache license lets anyone release his/her own flavor or version. This is the case with CyanogenMod – it's essentially android but wrapped up in a whole new package with simple looks and better features. People like to make choices, and that's why CyanogenMod was developed to provide Android users with a new, better and community-driven choice. The CyanogenMod community (Consisting of unpaid Volunteers and enthusiasts around the world) takes this source code and developed it into new and old legacy devices. At the same time, other CyanogenMod developers start adding features, fixes, and improvements that Google didn't include to the CyanogenMod code, which benefits all the devices. The CyanogenMod community has a whole infrastructure for people to build and test experimental versions, report bugs, and contribute back to the source code.

Sometimes features that started in CyanogenMod have appeared in newer version of "official" Android Every Time Android does a new "code dump" of their latest version, CyanogenMod benefits from Google's changes [1].

WHY SHOULD I MODIFY MY DEVICE?

While making the decision whether we need to modify the device or not, some points come into picture. It is very similar to modifying the computer or Laptop system after the installation from the stock.

There are Some Pros and Cons that we need to focus to have better understanding to decide this key point [7].

v. It provides better performance.

Pros:

i. It helps in removing unwanted software and programs from the system.

ii. It receives security updates more easily and conveniently.

iii. Taking control of our operating system, we can update the android of our device anytime we want without the interference of manufacturers.

iv. It does not require any re-rooting as device is already rooting enabled.

Cons:

i. Some manufacturers or mobile providers may provide a limited or voided warranty after modifying.

ii. It is possible that by installing a rooted operating system, we may introduce new security risks. For instance, we need to be smart about the permissions we grant to applications.

iii. Non-stock firmware could contain malicious code - which is a good argument for making sure we download custom ROMs from trusted sources, or even better, learn to build it yourself!

iv. Stability issues may arise when using an experimental operating system.

However, for many people, CyanogenMod has proven to be more stable than many official ROMs [7].

INCREASED APPLICATION USE

The table1 below represents the various applications provided by cyanogenMod operating system in one column corresponding to its description in second column. The table 1 demonstrates the special features of the cyanogenMod [7].

Table 1[4] [7]

S.NO.	Application Of Use	Description
1.	CM Updater	Update your device at your required Schedule with latest releases
2.	Privacy Guard	Control what your applications can learn about you and your contacts. Protect yourself with a simple click, or long press an app to delve deep.
3.	Global Blacklist	Enables the users to blacklist telemarketers, robo-callers and annoying people.
4.	Quick Setting Ribbon	Embed quick toggles (and even your camera) right in your notification drawer, just one swipe away.
5.	Quick Settings Config.	Whether use Ribbon View or large grid view, customize layout and order of quick settings.
6.	Theme	With integrated theme engine, we can change the look and feel of the entire OS.
7.	Trebuchet	With Trebuchet which is built from ground up theme engine, by custom themes we can alter window styles, icons, fonts, wallpaper, the lock screen, boot animations, and sounds!
8.	Status Bar Behavior	Customize your status bar and unlock some additional behavior.
9.	CM Account	With Secure, encrypted and optional account, if we ever lose our device, we still have some control over the device.
10	CM File Manager	Organize, edit, and manage your files with simple Powerful File Manager.
11	Display and Lights	Control brightness, rotation, wallpapers, remote displays, notification lights, and battery lights.
12	Profiles	With profiles we can control application, sounds and even connectivity to quickly adapt to the environment in which we are using our phone. Go one step further and set up a profile to be location aware, or use NFC to trigger a profile change.
13	Button Configuration	Enable additional functionality from your hardware keys, or even remap them altogether.
14	Navigation Bar	Customize the Navigation bar as needed without affecting other h/w buttons.
15	Lockscreen	a) Add quick unlock targets to access our favorite apps directly from the lockscreen. b) Use our custom lockscreen widget to increase your productivity. c) Show the weather and your calendar events without unlocking the device. d) Optionally display battery status or even your name and ICE information.
16	DSP Manager	Unlock the potential of our headphones by tuning music with built in equalizer.
17	Tethering	With built in tethering Share data over USB, Wi-Fi and Bluetooth.
18	Developer Tools	Customize your device hostname; go wireless and use ADB over your network.
19	Root Access	Useful to developers and users alike, control your exposure to root applications and debugging tools.
20	Super User	Manage root access to only the applications we trust, check access logs, and revoke their access when we are done.
21	Performance Tools	Push it up to eleven and access power tools to overclock, manage device governors and more.
22	Advanced Device Tools	These options vary by device, but allow for even more control over the hardware on your phones.
23	Battery Consumption	Since apps consume comparatively less space of RAM, so it provides long battery life.

Currently, the recent device that runs CyanogenMod 11 on the Android mobile device is “Micromax YU Yureka” and it is provided with all the specifications and all the features mentioned [5].

Based on the Android Open Source Project, CyanogenMod is designed to increase performance and reliability over Android-based ROMs released by vendors and carriers such as Google, T-Mobile, HTC, etc. CyanogenMod also offers a variety of features & enhancements that are not currently found in these versions of Android.

CyanogenMod offers the most barebone Android experience coupled with some very powerful tweaks. This whole package by now is not wholly developed by CyanogenMod developers alone, but is a collaborative effort between them and independent developers around the world.

CURRENT DEVELOPMENT IN CYANOGENMOD

CyanogenMod Theme Engine[3]

CyanogenMod makes it easy to quickly customize & change the look of your UI.As someone that loves to tinker; this explains how things actually work and how themes are developed in CyanogenMod.

At the most basic level, themes are simply a mechanism to allow resources to be replaced at runtime (as opposed to compilation time – the time when the build is created on the buildbots).Whenever an application is started, Android loads up the resources associated with that app and the application makes requests for these resources(see Fig-1).

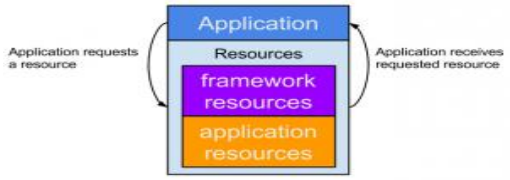


Fig- 1

That's the normal flow of retrieving resources, but what happens when a theme is applied? When the system loads the resources for the application, it checks if there is a theme applied and if there is, it adds the themed resources to the original resources. This is the point at which the magic happens. When the app requests a resource, the system will check if there is a themed version of it and if so, returns the themed resource, and if not it simply returns the original.

The key point here is the original resources are never modified/moved/altered, the system simply returns a resource from the theme instead of the original.

As below, fig 2 represents that there is no difference as far as the application is concerned.

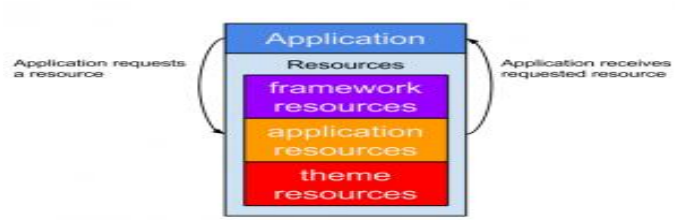


Fig- 2

Now the question arises that how does the system know which themed resource to replace an application resource with?

This is done by leveraging a framework known as Runtime Resource Overlays, which was contributed to AOSP by Sony in 2014. Part of the RRO framework is a tool called IDMAP. IDMAP inspects the resources in an application and compares the resource types and names to those in the themed resources. For those resources that match it stores a mapping of the original resource to the matching resource in the theme. Completion of this process results in an efficient way to determine if a resource is themed and where that resource resides.

Resources can range from images such as JPEGs or PNGs, XML that defines how things should be laid out on the screen, XML that define various color values that can be used to color text or highlight buttons, and even more XML that describe animations. The list goes on but there are a couple of resources that warrant a bit more explaining. One of those is the nine patch image [3].

A nine patch is a PNG image that has special markers around the borders that tell Android how it can stretch and place content within the image. Because analyzing those borders at runtime would take a bit of unnecessary processing, the image is processed and the border is removed and encoded into the image at build time. Android can then quickly read that information and know exactly how to handle the image. Android also likes to have all the plain text XML that the application developer has written converted it into a more efficient binary format that can be read a lot faster at runtime. The final step that needs to be done to the resources is to create a special file that indexes all of the applications resources so that they can be quickly retrieved by the android framework. Fortunately this is not a manual process, as there is a tool called the Android Asset Packaging Tool, AAPT for short.

Now what makes the Theme Engine so unique. With the original implementation of the RRO (from Sony), for every application that one wanted to theme one needed to create a theme just for that app. Sony's method also doesn't account for items like changing fonts, or some of the XML elements – it is primarily just overlays. The theme designers should be able to theme multiple applications for many more elements, just like they were able to do in the legacy theme engine from T-Mobile.

Every application has a unique name, known as the package name that identifies it. Fortunately, Android has one place an asset folder that allows us to put all sorts of files and even create directories that can be accessed later by the application and by using directory names that match the unique package name of an application a theme designer can include resources for many applications, all within one theme. This was great but there was one problem. Anything you place in these locations does not get processed like all the other resources do when an application is be built. This meant we either needed to require the theme designer use special tools or go through a painstaking process just to get the resources created in the format Android likes, or we could let them easily drag and drop their themed resources into these folders and let the device do a bit of the heavy lifting at install time. This is a very simple and convenient way for someone to create a theme without jumping through a lot of hoops, but that doesn't mean a nice tool to create an efficient theme out of the box is out of the question. Letting the resources remain in their original format means we had to come up with a way to keep Android happy and not lose any of the efficiency that RRO provides. To accomplish this we actually have a version of AAPT that runs on the device, and is part of every

CyanogenMod build. When the theme is installed a special service goes through and creates the indexed resource file as well as processes the nine patch images and the XML. We store this file on the device and that is what provides the themed resources that can be attached to an application at runtime.

DIFFERENT VERSIONS OF CYANOGENMOD

Fig-3[8]

CyanogenMod main version	Android version	Last or major release	Recommended Build release date	Notable changes[79] [collapse]
3	Android 1.5 (Cupcake)	3.6.8.1	1 July 2009[80]	3.6.8 onwards based on Android 1.5r3
		3.9.3	22 July 2009[81]	3.9.3 onwards has FLAC support
4	Android 1.5/1.6 (Cupcake/Donut)	4.1.4	30 August 2009[82]	4.1.4 onwards based on Android 1.6 (Donut); QuickOffice removed from 4.1.4 onwards; Google proprietary software separated due to cease and desist from 4.1.99 onwards
		4.2.15.1	24 October 2009[83]	4.2.3 onwards has USB tethering support; 4.2.6 onwards based on Android 1.6r2; 4.2.11 onwards added pinch zoom for Browser, pinch zoom and swipe for Gallery.
5	Android 2.0/2.1 (Eclair)	5.0.8	19 July 2010[20]	Introduced ADW.Launcher as the default launcher.
6	Android 2.2.x (Froyo)	6.0.0	28 August 2010[84]	Introduced dual camera and ad hoc Wi-Fi support, Just-in-time (JIT) compiler for more performance
		6.1.3	6 December 2010[85]	6.1.0 onwards based on Android 2.2.1.
7	Android 2.3.x (Gingerbread)	7.0.3	10 April 2011[27]	7.0.0 onwards based on Android 2.3.3
		7.1.0	10 October 2011[86]	Based on Android 2.3.7[30]
		7.2.0	16 June 2012[87]	New devices, updated translations, predictive phone dialer, ability to control haptic feedback in quiet hours, lockscreen updates, ICS animation backports, ability to configure the battery status bar icon, many bug fixes[30]
8	Android 3.x (Honeycomb)	N/A	N/A	Skipped due to Google not releasing Android 3.0 Honeycomb source code.
9	Android 4.0.x (Ice Cream Sandwich)	9.1	29 August 2012[34]	Advanced security: deactivated root usage by default.[88] Added support for SimplyTapp.
10	Android 4.1.x (Jelly Bean)	10.0.0	13 November 2012[89]	Expandable desktop mode. Built-in, root-enabled file manager.
	Android 4.2.x (Jelly Bean)	10.1.3	24 June 2013[90]	
	Android 4.3.x (Jelly Bean)	10.2.1	31 January 2014[90]	Phone: *Blacklist*-Feature added.
11	Android 4.4.x (KitKat)	**11.0 M12**	13 November 2014[2]	*WhisperPush*: Integration of TextSecure's secure messaging protocol as an opt-in feature. Enables sending encrypted SMS messages to other users of CM or TextSecure.[91][92]
12	Android 5.0.x (Lollipop)	Nightly	5 January 2015	
Legend: Old version	Older version, still supported	**Latest version**	Latest preview version	Future release				

Conclusion

The Android Operating System developed by Google is to provide easy accessibility of applications to make the work easier. Android was intended as an "open source" operating system that hardware makers can deploy in their devices for free. Yet Google has frustrated manufacturers in recent years by requiring them to feature Google apps and set Google search as the default for users, in exchange for access to the search engine, YouTube, or the millions of apps in its Play Store. Such restrictions make it harder for apps that compete with Google's to win distribution on Android devices.

So, CyanogenMod provides a rebuilt version of the Android Operating System so that the user, manufacturer and

developers have all the privileges to access and the source code of the apps and according to the requirement, user can now modify its device which include rooting, privacy guard, randomized screen locks pattern, scheduling updates of the phone on the Go, Customizing Navigation tabs, start screens, applying personalized and customized themes (which includes changes icon, fonts etc.) and Folder locks and many other features etc. Moreover, Installing CyanogenMod on an Android device is very simple and easy

So, CyanogenMod should have better future development in the field of Android which provides more User Interactivity, Experience and Satisfaction towards use of technology and development in these smart and changing trends of technology in mobile devices.

References

[1] http://wiki.cyanogenmod.org/w/About About CyanogenMod

[2] http://blogs.wsj.com/digits/2015/01/29/microsoft-to-invest-in-rogue-android-startup-cyanogen/50 ,The Wall Street Journal.

[3] http://www.cyanogenmod.org/blog/developer-blog-the-theme-engine CyaogenMod Developer Blog

[4] http://www.howtogeek.com/192602/8-reasons-to-install-cyanogenmod-on-your-android-device

[5] https://www.youtube.com/watch?v=8c4Y3JKcL5s ,Youtube Video on Micromax Yu Yureka Mobile With running CyanogenMod11.

[6] http://forum.xda-developers.com/wiki/Rooting ,Rooting in Android

[7] http://wiki.cyanogenmod.org/w/Why_Mod%3F.

[8] http://en.wikipedia.org/wiki/CyanogenMod

Comparative study of routing protocols for wireless sensor network

Anupriya Shahi
GCET,Greater Noida (U.P.), India.
anupriyashahi01@gmail.com

Komal Soni
GCET,Greater Noida (U.P.), India.
komal.ks.soni@gmail.com

Divyansh Dixit
GCET,Greater Noida (U.P.), India.
dixvyansh@gmail.com

Manish Singh
GCET,Greater Noida (U.P.), India.
manish.sipu@gmail.com

Abstract - **Recent developments in the area of micro-sensor devices have accelerated advances in the sensor networks field leading to many new protocols for Wireless sensor networks (WSNs) .Wireless Sensor Networks (WSNs) has foreseen big changes in data gathering, processing and disseminating for monitoring specific applications such as emergency services, disaster management, and military applications etc. Wireless sensor network consists of a group of spatially distributed sensor nodes which are interconnected without wires. Wireless sensor network can be classified into Static Sensor Network (SSN) & Wireless Sensor Network (WSN). In Static Sensor Network, the sensor nodes localize only first time during deployment. In case of Wireless Sensor Network, nodes collect the data by moving from one place to another place, hence localization is needed. Wireless sensor networks are more energy efficient, better targeting and provide more data fidelity than Static Sensor Network (SSN). Wireless Sensor networks have gained great attention in recent years due to their ability to offer economical and effective solutions in a variety of fields. In this paper we discuss about LEACH (Low Energy Adaptive Clustering Hierarchy)and TEEN (Threshold Sensitive Energy Efficient sensor Network) routing protocols for wireless sensor networks. Further, we propose anEfficient Tree Based Routing Protocol (ETBRP) which handles the mobility for the sensor node. Finally, we provide a comparative study on LEACH, TEEN and ETBRP which shows how ETBRP outperforms LEACH and TEEN in terms of mobility, energy efficiency & network life time.**

Keywords: Wireless Sensor Networks (WSN), Routing Protocols, Hierarchical Routing, LEACH, TEEN, TBRP.

INTRODUCTION

Wireless sensor network consists of a large number of such sensor nodes that are able to collect and disseminate data in areas where ordinary networks are unsuitable for environmental and/or strategic

reasons. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on. Nodes in WSN vary from a few to several hundreds or even thousands, where each node is connected to one or sometimes several sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding.

1.1 Limitations and Challenges in Wireless Sensor Network

. The sensor nodes have the various limitations such as low battery power, minimum computation capability and energy. Some of the commonly applied sensors used are for measuring now, temperature, humidity, vibrations, pressure, brightness, mechanical stress, and proximity.

It requires the interaction of elements or members that perform different tasks. The common participants in this WSN are:

i. **Sources** that are in charge of generating the data of the task,
ii. **Intermediate nodes** that make additional processing or forwarding data, and
iii. **Sinks** where the information is received. In some applications, these sinks are part of the networks, whereas in others they are external elements that enquire information from the network.

Managing a wide range of application types in a WSN is hardly possible with a single conception and design of the wireless network. However, certain attribute identified are related to the characteristic requirements and the mechanisms of such systems. The realization of these characteristics with newer mechanisms is the major challenge foreseen to WSNs.

1.2 Mobile Sensor Network

In WSNs, the participants are the sensor nodes, i.e. sinks, sources and intermediate sensor nodes. The sinks are identified as external elements that interact with the network. Examples of sinks in the WSN are PDAs, Laptops or getaways to other networks. Mobile sensor networks are sensor networks in which nodes can move under their own control or under the control of the environment. Mobile networked systems combine the most advanced concepts in perception, communication, and control to create computational systems interacting in meaningful ways with the physical environment. A key difference between a mobile sensor network and a static sensor network is how information is distributed over the network. Under static nodes, a new task or data can be flooded across the network in a very predictable way. Under mobility this kind of flooding is more complex. Under natural mobility this depends on the mobility model of the nodes in the system.

The Static Sensor Networks (SSNs) have various disadvantages such as first, less energy efficient, most of the gateway nodes loss their energy first means these nodes are die thus the whole network goes to die. Second, Static Sensor Networks (SSNs), the sensor nodes are static so it cannot move to other places but in Mobile Sensor Networks (MSNs) the sensor node can move and reach the places where event is fired. Mostly the sensors are deployed randomly, as opposed to precisely, therefore there is often a requirement to move the sensor node for better sight or for close proximity. Also mobility helps in better quality of communication between sensor nodes.

Thus, in case of Static Sensor Networks (SSNs), we have faced various problems. These problems can be overcome by using the Mobile Sensor Networks (MSNs).

1.3 Mobility in WSNs

Considering the capabilities that wireless communication offers, the sensor nodes and the objects of interest can have mobility identified as:

a) Event mobility: Typical in applications with events, tracking is required for detection of objects.

b) Node mobility: Sensor nodes have the capability to adjust their position, offer better results for the task, or when the network is used to monitor a moving object. This kind of network requires a more flexible and self-configurable behaviour due to variables like the speed of the node, energy consumption for connectivity, requirements to maintain a good level of functionality and QoS of the WSN.

c) Sink mobility: The sink is an external element like a PDA or Laptop, whose function is to consult the information provided by the WSN

LITERATURE SURVEY

2.1 Routing in Wireless Sensor Networks (WSNs)

Wireless Sensor Networks (WSN) design has been influenced by many factors, which include fault tolerance, scalability, production costs, operating environment, sensor network topology, hardware constraints, transmission media, and power consumption [1]. The basic blocks are in the areas of routing, time synchronization, and localization. The routing protocol allows different types of traffics to be delivered and fused during delivery to lower the amount of information exchange. The time synchronization protocol enables the sensor nodes to maintain a similar time while the localization technique provides a way to find the sensor nodes in the sensor field. The routing, time synchronization and localization schemes may be used to provide Quality-of-Service when data is gathered from the sensor networks.

2.2 Routing Protocols for Wireless Sensor Networks (WSNs)

Routing protocols for Wireless Sensor Networks (WSNs) are mainly classified into three categories: *Data centric or flat routing protocols, Hierarchical routing protocols.*

2.2.1 Data Centric or Flat Routing Protocols

Data centric protocols are the first categories of protocol; every node in the network has been assigned the same role. Whenever source node requires the data, it fires a query in the whole network. It is not an appropriate to use global identifiers for this huge number of randomly deployed nodes. However this introduces complexity to query data from a specific set of nodes. Therefore the data is collected from the deployed region. Since the collected data is correlated and mostly redundant; collected data is aggregated in some nodes resulting decrease in the amount of transmitted data so in transmission power. The following routing algorithms main consideration is data and its properties.

a) ***Flooding:*** This is a classical and old routing mechanism [24]. The data gathered is broadcasted unless the specified maximum number of hops per packet is reached, or the packet delivered to the destination. This protocol brings implosion, overlap, and resource blindness problems.

b) ***Gossiping:*** This is also a classical and old method, resembling flooding [23]. The gathered data is not broadcasted but sent to randomly chosen neighbor node until the specified maximum number of hops per packet is reached or the packet delivered to the destination. The delivery takes much time.

c) ***SPIN (Sensor Protocol for Information via Negotiation):*** The basic idea is using a metadata or high level descriptors [5]. There are three types of messages, ADV, REQ, and DATA. As shown in Figure 2.2, the source node broadcast an ADV message to its neighbors, ADV message indeed is meta-data. The interested nodes send REQ, and then the source node sends the DATA to interested nodes. Data aggregation is employed.

d) ***Directed Diffusion [6]:*** The sink broadcasts the "interest" message, namely the task descriptor to all nodes, as shown in Figure 2.2. The interest is stored

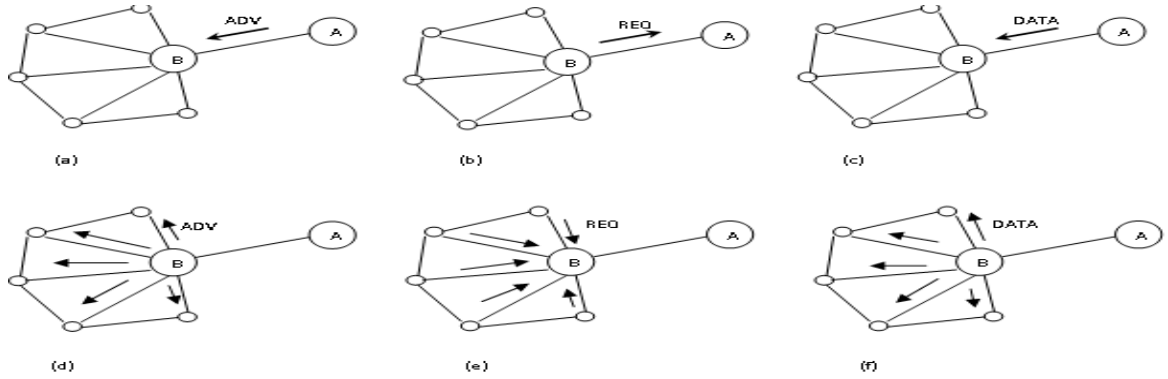


Figure 2.2 SPIN Protocol (a) Node A starts by advertising its data to node B. (b)Node B responds by sending a request to node A. (c After receiving the requested data, (d) node B then sends out advertisements to its neighbours,(e-f) who in turn send requests back to B.

to cache of every node, until timestamp of time specified messages expires. The message contains several gradient fields. The gradient to the sink is set up as the interest propagated through network. When the source node gets the interest it sends the data through the gradient path of the interest. The directed diffusion algorithm solves problems of node addressing or maintaining a global network topology, data caching also reduces energy consumption.

e) ***Energy-aware Routing [7]:*** In order to increase network life time a set of sub-optimal routes are proposed to use. The paths are chosen according to energy consumption of the path. Using the path that is consuming minimum energy frequently deplete energy source of specific nodes. Since one of the certain paths are chosen with equal probability, the network life time increases.

f) ***Rumour Routing [8]:*** Rumour routing can be considered as a derivation of "directed diffusion". If the number of queries is large, but number of events is small, directed diffusion becomes inefficient. Considering this shortcoming of the directed diffusion, flooding the events not the queries is proposed. Rumour Routing is another solution to this problem. The main idea is to route the queries to specific nodes that have observed specific events. When a node detects an event, it adds it to its event table and generates an agent in order to flood through network and propagate the detected information to the distant nodes. The sink queries then the query transmitted to the related node easily and efficiently.

g) ***Gradient Based Routing [9]:*** This algorithm is to some extent different than "Directed Diffusion". The interest packet is diffused through network in order to query the data. During the query process, the distance to the sink in terms of number of hops is recorded in the interest packet. Each node can discover the minimum distance from itself to the sink. The gradient is calculated as the difference between the node's gradient and its neighbor's gradient. The node decides to forward the packet to the sink with the largest gradient. Three different spreading techniques have been proposed: Stochastic Scheme (when two or more next nodes have the same gradient the node selects one randomly), Energy-Based Scheme (when a node has scarce energy, it increases its gradient), and Stream-Based Scheme (to divert streams away from nodes relaying traffic).

h) ***CADR (Constrained Anisotropic Diffusion Routing) [10]:*** The objective of the algorithm is to maximize information gain; however this causes a reduction in latency and bandwidth. There are two techniques; CADR and IDSQ (Information-Driven Sensor Querying). In CADR, each node calculates information, cost objective. According to this and end user requirements, the node specifies a route. In IDSQ, querying node determine the node that can provide the most useful information also considering energy cost.

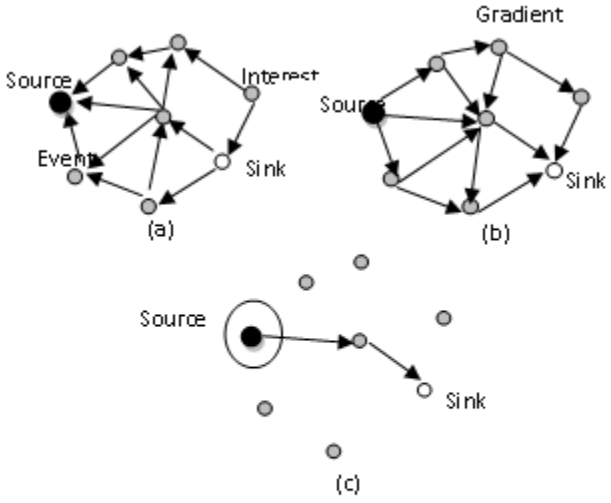


Figure 2.2 Directed Diffusion protocol phases. (a)Interest Propagation, (b) Initial Gradient setup and,(c) Data delivery along reinforcement.

2.2.2 Hierarchical or Cluster-Based Routing Protocols

Hierarchical routing or cluster based routing protocols have been proposed in order to meet the energy efficiency and scalability requirement of the WSNs. The main issue is forming sub network

clusters, encouraging multi hop transmission and enabling data fusion.

a)*LEACH, (Low Energy Adaptive Clustering Hierarchy) [13]:* The algorithm is based on clustering. Clusters of sensor nodes are formed according to the received signal rate of the nodes. Local cluster heads act as a router to the sink. The number of the cluster heads is limited, approximately 5% of the all nodes. The cluster head selection is performed randomly, in order to balance the energy of the network. Every node picks a number between 0 and 1 randomly if the number is greater than the calculated value for following equation, where p is the desired percentage of the cluster heads, r is the current round, and G is the set of nodes that have not been cluster heads in the last 1/p rounds.

$$T(n) = \begin{cases} \dfrac{p}{1 - p * (r \bmod \frac{1}{p})} & if \ \ n \in G, \\ 0 & \text{otherwise} \end{cases}$$

LEACH is completely distributed; no global knowledge is applied.

b)*TEEN (Threshold Sensitive Energy Efficient sensor Network Protocol) [16]:* In TEEN, the Closer nodes form clusters, with a cluster heads to transmit the collected data to one upper layer. Forming the clusters, cluster heads broadcast two threshold values. First one is hard threshold; it is minimum possible value of an attribute to trigger a sensor node. Hard threshold allows nodes transmit the event, if the event occurs in the range of interest. Therefore a significant reduction of the transmission delay occurs. Unless a change of minimum soft threshold occurs, the nodes don't send a new data packet. Employing soft threshold prevents from the redundant data transmission. Since the protocol is to be responsive to the sudden changes in the sensed attribute, it is suitable for time-critical applications. In the LEACH protocol, every cluster-head directly communicate with sink, however in TEEN there are three kinds of nodes and a base station (sink) as shown in Figure 2.5. Simple nodes gather the data from environment and forward it to the "*1st* Level Cluster Head's. Each 1st Level Cluster Head aggregates the data gathered from the simple nodes connected to its cluster, and then forward it to "*2nd*Level Cluster Heads. *2nd* Level Cluster Head can directly forward the data gathered from its cluster to base station. Some of simple nodes may be belong to cluster of *2nd* Level Cluster Heads when they are close to these nodes.

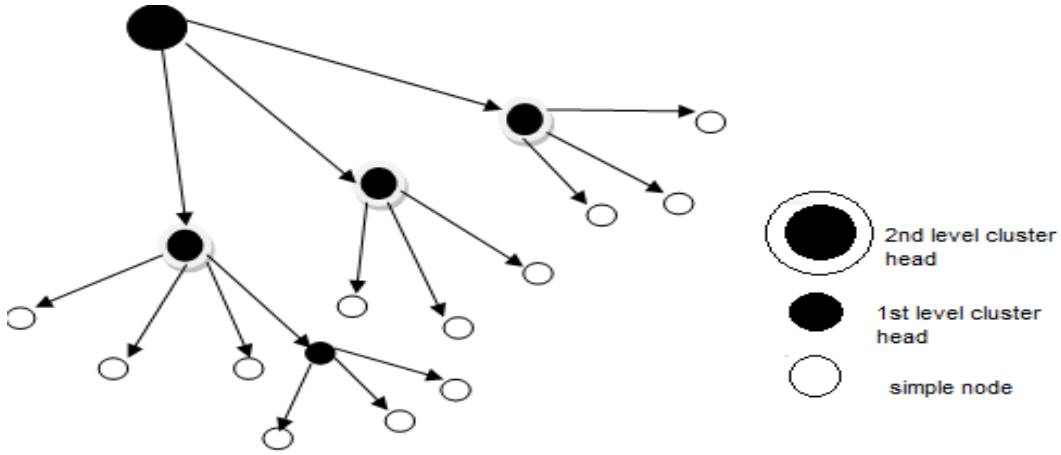


Figure 2.5 Hierarchical Clustering in TEEN[29]

LOCALIZATION ALGORITHM FOR WIRELESS SENSOR NETWORK

Recent technological improvements have made the deployment of small, inexpensive, low power, distributed devices capable of local processing and wireless communication, such nodes are called as sensor nodes. Each sensor node is capable of only limited amount of processing. Sensor networks consisted of small number of sensor nodes wired to a central processing station. However, nowadays, the focus is more on wireless, distributed, sensing nodes. In most of the cases, sensor nodes are deployed in an ad hoc manner. It is up to the nodes to identify themselves in some spatial co-ordinate system, referred as localization. In sensor networks, nodes are deployed into an unplanned infrastructure where there is no a priori knowledge of location. The problem of estimating spatial coordinates of the node is referred to as localization. Localization [19, 20] in wireless sensor networks is the problem of individual

sensor's awareness of their position relative to a coordinate system common to the entire sensor network. In routing applications, it is sufficient for the nodes to know the positions of their neighbors relative to a local coordinate system. Thus, sensor nodes would need to have other means of establishing their positions and organizing themselves into a coordinate system without relying on an existing infrastructure. To support mobility applications, a node must move in a specific direction in a manner that is related to its neighbors. In this paper we discuss the various localization algorithms for the mobile sensor network.

3.1 Localization algorithm

We can divide our location algorithm into two parts based on the measuring system used: *GPS based* and *GPS free localization algorithm:*

3.1.1 GPS based localization Algorithms

In GPS based localization algorithm we require a GPS system because GPS system to find the position of the node. In this technique, few nodes commonly known as *anchors,*useGPS to determine their location using GPS system and, broadcast its position information in the network, i.e. cached by the other node in the network and with the help of this information other nodes (neighbor nodes) calculate their own position without using GPS. Further, GPS based localization algorithm is divided into two parts, based on the range of the anchor nodes: *Range-free* and *Range-Based.* Monte Carlo localization algorithm [19], [20] and color-theory-based dynamic localization algorithm [21] etc. are the example of range free algorithm. *Range-free algorithms* do not need absolute range information; the accuracy is less than the range-based but satisfies many applications requirements and range free algorithms are cost effective than range based algorithms. Range-based localization algorithms use techniques such as radio signal strength indicator (RSSI) [22, 23] or radio and ultrasound with angle of arrival [24, 25] (AOA) or time-difference-of arrival [26, 27] (TDOA), to measure the distance that separates an un-localized node from an anchor. These distances, also called ranges, are sensitive to range errors, i.e., inaccuracies in the range measurements and often rely on additional hardware.

a) Sequential Monte Carlo localization Algorithm

The Monte Carlo localization algorithm is mainly used for the robot localization [23] which is based on its motion, perception, and possible pre-leaned map of its environment. L. Hu and D. Evans [19] used this algorithm for mobile sensor node. This is the first range free localization algorithm for mobile sensor network. The localization of sensor nodes is more difficult than the localization of robot.

The authors assume sensor has little control

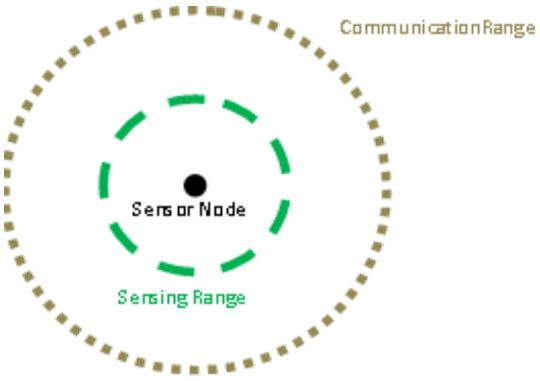


Figure 3.1 Various range of the sensor node

and knowledge over its movement, in contrast to a robot. They target an environment where there is no hardware for obtaining ranging information, the topology of the network is unknown and most likely irregular, the density of anchors is low and both anchors and sensor nodes can move in an uncontrollable manner. The Sequential Monte Carlo localization algorithm has three steps: *Initialization step, Prediction step, and filtering step.* Prediction step and filtering step are combined called *location estimation* step.

In the first step (*initialization step*), initially the node has no knowledge about its location. So the authors consider that sensor nodes take a random set of N samples say L_0. And the time is divided into discrete time intervals.In the second step, after each time interval a new sample has been calculated. In the

Prediction steps, the authors assume that every node aware about its speed and direction. The speed of the sensor node is ranging between 0 to v_{max}. In this step, the author predict a new sample $L_t$which is based on the previous sample L_{t-1} andspeed of the nodes, and chosen from the disk radius $v_{max}$and l_{t-1}(previous location) with centre. The probability distribution for the new sample based on the previous sample is given by the following equation:

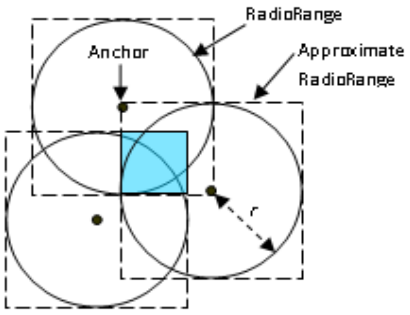


Figure-3.3 Building Anchor Box

$$p(l_t|l_{t-1}) = \begin{cases} \frac{1}{\pi v_{max}^2} & \text{if } d(l_t, l_{t-1}) < v_{max} \\ 0 & \text{if } d(l_t, l_{t-1}) \geq v_{max} \end{cases}$$

Inthe*filtering step,* all the impossible locations are removed from the sample by using the direct and indirect anchor information as shown in figure 3.2.

After filtering step the predicted sample contains only the desired location. The prediction and filtering steps are repeated in each time interval until the desired sample has been obtained. This algorithm gives the satisfactory result for the localization of sensor node but requires the high density of anchor nodes.

b) Monte Carlo localization

The Sequential Monte Carlo Localization algorithm presented by Hu and Evans [19] is less accurate even when memory limits are severe, the seed density is low, and network transmissions are

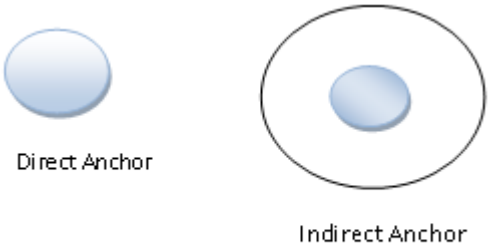


Figure 3.2Direct and Indirect Anchor node

highly irregular. AlineBaggio and KoenLangendoen [20] improve the way of Anchor to be used so that the accuracy and efficiency of the algorithm can be improved. Aline*et. al.* in [21] making better use of the information, a node gathers from one-hop and two-hop anchors and by restricting the area a node has to draw samples box (Monte Carlo localization Box with co-ordinates $\{(x_{min}, x_{max}), (y_{min}, y_{max})\}$ and improve the whole process of localizing. As shown in figure-3.3 example of an anchor box (shaded area) in the case a node hear three one-hop or two hop anchors and draw a box where the radio range of these three anchors are overlaps. This box is termed as *anchor box*. This region is called deployment area where the nodes have to be localized. For each one-hop anchor heard, a node builds a square of size *2r*centred at the anchor position, *r* being the radio range. Since the dimensions of the anchor box is approximately equal to the radio range of the anchor node so it is easy to filter the predicted sample within this region. The prediction and filtering steps are repeated until the required sample is no found. Thus by using the anchor information for the anchor box Alineet. al. improve the efficiency of the localization, and gives the better accuracy, the coverage of the localization also improve.

c) Colour theory based Dynamic Localization algorithm

$$H_t, S_t, V_t = RGBtoHSV(R_t, G_t, B_t)$$

$$H_{it} = H_t,\ S_{it} = S_t,\ V_{it} = V_t \cdot (1 - D_{it} / Range)$$

$$R_{it}, G_{it}, B_{it} = HSVtoRGB(H_{it}, S_{it}, V_{it})$$

$$R_i, G_i, B_i = (1/n) * \sum_{t=1}^{n} (R_{it}, G_{it}, B_{it})$$

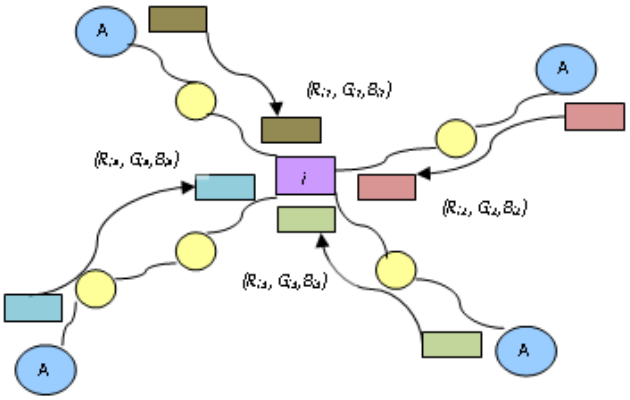


Figure 3.4 Node*i* obtain the RGB value from different

The colour theory based localization algorithm is proposed by the Shen-HaiSheeet. al. [21], it comes under the category of Range-free localization algorithm. In this algorithm, a sensor node is represented by the set of RGB value. With the help of RGB value we can find the most possible location of the sensor node. This centralized localization algorithm is based on the colour theory to perform positioning in mobile wireless sensor networks. For localization of the sensor node the RGB value of the sensor node is frequently updated. It builds a location database in the server, which maps a set of RGB values to a geographic position and measure the distance between sensor nodes that are based on the DV-Hop [35]. The colour theory based algorithm uses the two algorithms: RGB to HSV and HSV to RGB. The RGB to HSV algorithm converts the RGB values to HSV values, which is received by a sensor node from its anchor node. Here HSV stands for Hue, Saturation, and Value. Based on colour theory, only the lightness of colour fades out with the increasing of propagating distances. That is, the V of HSV of an anchor, which is corresponding to the lightness, is decreased in proportion to the distance from the node to the anchor. And by using HSV to RGB algorithm the new HSV value is converted back to RGB value. The node then calculates its own RGB values by

averaging these adjusted RGB values, corresponding to the anchors. The node then sends its RGB values to the server so that the server can find its most probable location by looking up the location database. The RGB value first randomly assign to the anchor node from 0 to 1. After a sensor node *i* obtain the each anchor RGB value and the hop count and convert it into HSV value by using the RBG to HSV algorithm. With the help of hop count and hop distance from the anchor node the HSV value is updated and this HSV value is converted back to RGB value. The RGB value of the node *i*is the mean of the RGB value obtain from the *n* anchor nodes as shown in figure 3.4. The following equations are used in the whole process.

A location database is established when the server obtains the RGB values and locations of all anchors. The mechanism is based on the theorem of the mixture of different colours. With the RGB values of all anchors, the RGB values of all locations can be computed by exploiting the ideas of colour propagation and the mixture of different colours. The location for each sensor node can be constructed in the location database by maintaining the coordinate (x_i,y_i) and the RGB values (R_i,G_i,B_i) at each location *i*. Then, the location of a sensor node can be acquired by looking up the location database based on the derived RGB values.

3.1.2 GPS free localization Algorithms

GPS Based localization algorithm requires some GPS system which only suitable for outdoor environment and has several disadvantages: *first*, the availability of GPS signals, *second*, the availability of global positioning systems (GPS) which requires additional hardware at additional costs, *third*, size of the sensor nodes, *fourth*, power of the sensor nodes and *last*, the availability of a number of fixed-point reference nodes, or anchors, with globally known locations. Due to these reason we require an algorithm which is GPS free. The directional or GPS-free localization algorithm is the first localization algorithm given by Akcan*et. al.* [12].

a) Directional Localization Algorithm

The directional localization algorithm is a GPS-free localization algorithm [12], which has the following assumptions: *first*, each node has a compass pointing to north, *second*, Node can measure distance to their neighbors using a well know measurement method (i.e. TOA Time of Arrival [13] or signal strength [14]), *third*, Motion actuators allow each node to move in a specific direction (with respect to North), *fourth*, Actuator, compass and distance measurements are subjected to errors caused by various real world disturbances and *fifth*, Other than the above, we do not need any additional equipment or infrastructure.

This algorithm works on two sub-algorithms: *Core localization algorithm and Verification algorithm*. In Core localization algorithm two neighbors suppose n_1 and n_2 generate two possible relative positions, whereas the Verification algorithm uses third neighbor to know to correct position. Here we discuss both algorithms.

Core Localization algorithm: This algorithm works on some well-defined rounds and each round consist of three steps: *first*, Measurement of distance between the neighbours, *second,* Individual movement of the

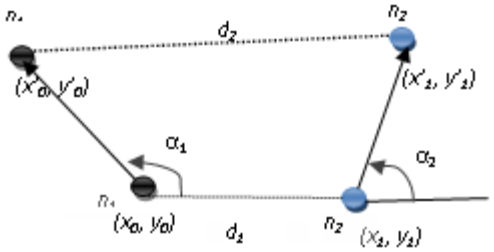


Figure 3.5 Movement of two nodes

neighbour and *finally,* An exchange between neighbours of direction and distance values for that round. Whenever any nodes need localization, they initiate the rounds. There is no pattern or continuity between the rounds. The authors do not assume anything about the temporal duration of the rounds. And also assume that the direction of the node does not change within a round. Figure 3.5 shows the movement of the two nodes n_1 and n_2. According to core localization algorithm, the distance between the n_1 and n_2 has been calculated by using the Euclidian distance formula. Then consider the movement of the nodes, supposes at any time $t_0$the nodes n_1 and $n_2$has their co-ordinates (x_0, y_0) and (x_1, y_1) respectively. After some time suppose at t_1, the now nodes gets new co-ordinates (x'_0, y'_0) and (x'_1, y'_1) respectively. Each node $\{n_i \mid i=1, 2\}$ move in direction α_i and distance r_i. When the nodes gets its new position then the distance between the $n_1$and n_2 is re-calculated, after that the value of $r_i$and α_i has been calculated for $i=1$ and 2. After calculating the value of $r_i$and α_i the co-ordinate of n_1 has been easily calculated by using the equations (4), (5) and (6) with respect to n_2.

$$x'_0 = r_1 \cos \alpha_1, \qquad y'_0 = r_1 \sin \alpha_1 \qquad (1)$$

$$x'_1 = x_1 + r_2 \cos \alpha_2, \; y'_1 = y1 + r_2 \sin \alpha_2 \qquad (2)$$

$(x'_0 - x'_1)^2 + (y'_0 - y'_1)^2 = d_2^2$, $x_1^2 + y_1^2 = d_1^2$ (3)

By solving equations (1), (2), and (3) we get the following equations (4), (5) and (6).

$x'_0 A + y'_0 B = C$, (4)

$x'_0 D - 2x'_0 E + F = 0$, $y'_0 D - 2y'_0 G + H = 0$ (5)

$$x_1 = \frac{-E \pm \sqrt{E^2 - DF}}{D}, \quad y_1 = \frac{-G \pm \sqrt{G^2 - DH}}{D} \quad (6)$$

*Verification Algorithm:*In the *Core-Localization algorithm*, by solving equation (4) , (5) and (6) we get the two possible co-ordinate of node $n_1\{n_j^{1,2} \mid j=2, 3\}$ for each neighbour$n_2$and n_3. So in verification algorithm we verify the neighbor position using the third node. To find the exact position, $n_1$gets calculate the Inter-distance $d_{2,3}$between n_2 and n_3 from either one of the node and simply find the correct position pair $\{n_j^{1,2} \mid j=2, 3\}$.

Exceptional configuration: Due to rigid geometry and configuration, the above algorithms have some exceptional configuration: *equal parallel movement* and *excessive error*. Equal parallel movement occur, for $D=0$ in equation (6), this implies $A=0$ and $B=0$ since $D = A^2 + B^2$. In equal parallel movement the nodes move parallel with same speed and equal distance. While excessive error occur due to inaccurate measurement of distance, actuator, and compass. When highly erroneous d, v and α values create a non-rigid geometry, such that $E^2 - DF < 0$ or $G^2 - DH < 0$ in equation (6), our core algorithm cannot localize n_1 and n_2.

b) GPS less, outdoor, self-positioning algorithm

Hung-Chi Chu et. al. [20] Has been proposing a GPS less localization algorithm. In this algorithm some sets of nodes are known as reference points (RP's). These RP's are deployed in a region, called deployment area and broadcast some packets, these packets contain the localization data. The other nodes in the networks receive these packets, process these packets and can easily localize it. The characteristics of self-positioning algorithm are given as; it is a distributed self-positioning algorithm, and the energy consumption is low because sensor nodes simply use the connectivity information. In this algorithm, a set of RP's are placed in known location and they form a hexagonal or mess structure as shown in figure 3. 6. The radio range of a RP is shown as the circle and sensor nodes receive the localization packets if they are in the radio range of the RP. In figure 3.6, P_i and S_j are representing the reference point and sensor nodes respectively. Figure 3.6 shows that there are 3 types of regions, *first*, region covered by the radio range of only one RP point, *second*, region covered by the overlapping radio range of two RP points, and *third*, region covered by the radio range of three RP points. Centroid of each localization region has been calculated. When any sensor nodes want to localize they use these centroid points and calculate their position by using self-localization algorithm.

In the *Self Localization Algorithm*, the authors assume the centroid of localization region has known to each *reference points*. The RP broadcast beacon packets, these beacon packets contains type of RP

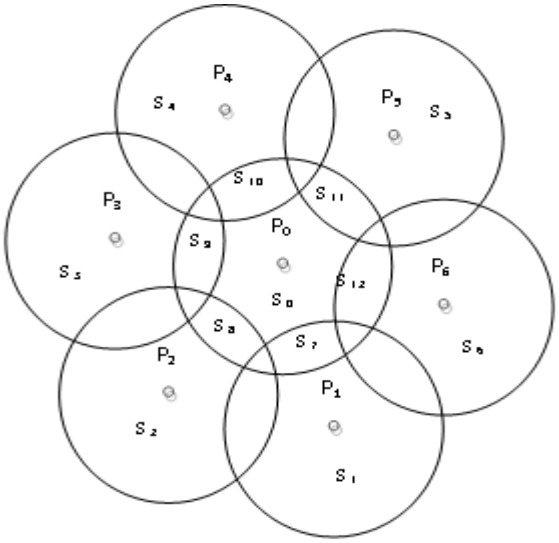


Figure 3.6 Hexagonal structure formby thereference points

structure (hexagonal or mess), type of localization region, and centroid of the region etc. when any sensor node receive these beacon packets, they determine the number of RP's that it has listen, extract the centroid set from the beacon packets and calculates it location by intersecting all the centroid sets. From the above discussion, we see that sensor node only collect the localization data from the RP's and localize them. This localization algorithm no needs any additional GPS system and little computational cost is required by the sensor nodes. So this type of localization algorithms is more suitable for sensor network.

Efficient Tree Based Routing Protocol (ETBRP)

4.1 System Architecture

The system model Efficient Tree Based Routing Protocol (ETRBP) properties:

- The entire nodes in the network form a tree with different level; the node of the tree has

some degree constrain which depends on the level of the node.

- The distance between two levels is equal to the radio range of the sensor nodes (which is approximately equal to the maximum distance cover by the node in 1 second).

4.2 Efficient Tree Based Routing Algorithm

Efficient Tree-Based routing algorithm with Degree Constraint for mobile sensor network has been proposed. This algorithm work in three phases: Tree formation phase, Data collection and Transmission phase, and finally Purification phase.

Phases of Algorithm

Our algorithm work in three phases: Tree formation phase, Data collection and Transmission phase, and Purification phase.

4.2.1 Tree formation phase

The tree formation phase has the following steps:

Step 1: In tree formation phase, first base station broadcast an initialmessage which contains the information about the position of the each base station and level distance, when any node gets this message it first calculates the Euclidian distance from the base station. And according to that distance assign a level to itself.

Step 2: After assigning level, each node broadcast the join request packet which contains the node id and level of the node.

Step 3: When any node listen a join request, it first checks its parent and the level of the joining request. If the parent of the node is null or level is higher than or equal to the node itself then node discard this join request packet, otherwise the node check its node degree if the node degree is greater than or equal to the degree constrain and also discard the request, otherwise response with a positive acknowledgement .

Step 4: The requested node join the node from which it get the first acknowledgement and add as a child node to itself, then the parent node add this node to its child list and increase the node degree count by 1.

Step 5: Step2-4 are repeated until whole tree has been form. The flow chart for tree formation phase.

4.2.2 Data collection and Data transmission phase

Step 6: After Tree formation phase, each node send its child list to its father node. According to the child list, the father node sends a TDMA schedule to its child node. In its schedule the child node can send its data to the father node.

Step 7: If the child node have the data, then it forward its data to its parent node in its time slot (TDMA slot) otherwise it send a negative acknowledgement to its parent node. CSMA/CA approach is used by the node to send the data.

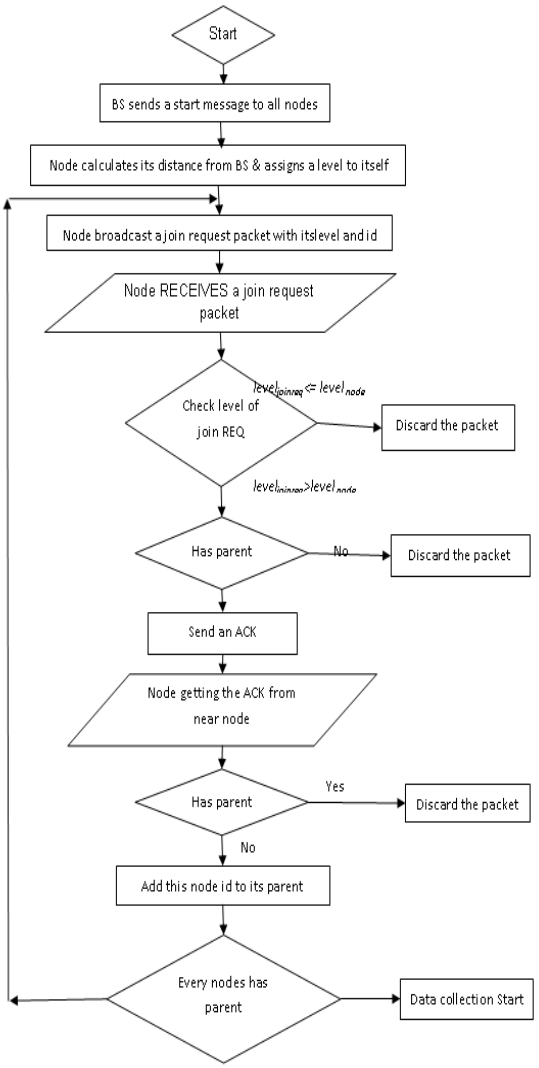


Figure 4.3 Flow chart for tree formation

Step 8: The parent node aggregate its data with children data and send it to its parent node. Finally the node near to the base

station sends the collected data to the base station. The flow chart for data transmission phase

4.2.3 **Pu**Error! Reference source not found.**rification phase**

This phase handle the several situations such as failure or movement of the parent or child node and energy level of the nodes.

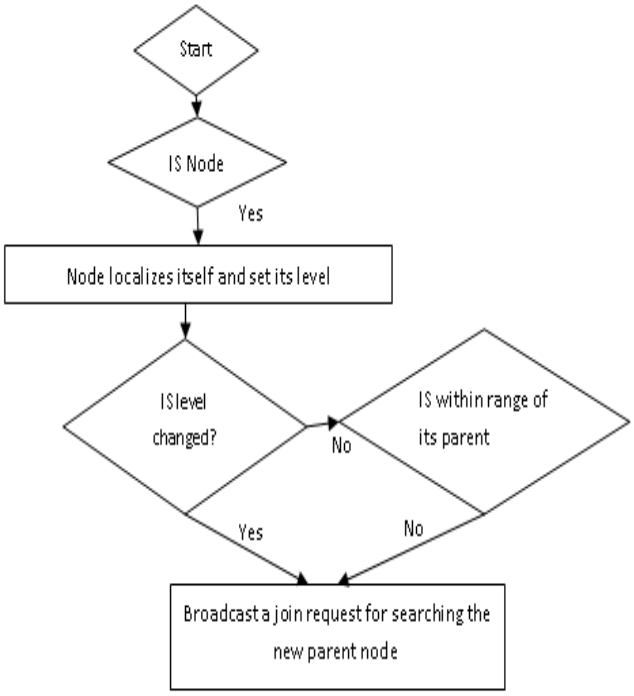


Figure 4.10Flow chart for Purification phase

Step 9: When a node moves from one location to another location. There are two possibilities regarding the movement of the node as shown in figure 4.5.
The node either moves within the same level or
One level above or below
When the position of the node will get change it localizes itself by localization algorithm. After calculating its position, node calculates its distance from the base station and re-calculates its level

Step 10: If the level of the node does not change, then node checks that it is in the range of its father or not, if it is within the range of its parent node then no need to re-join the tree, otherwise, node change its level according to the distance from the base station and

Broadcast a join request and add the new node in its father node list and remove the old. The flow chart for

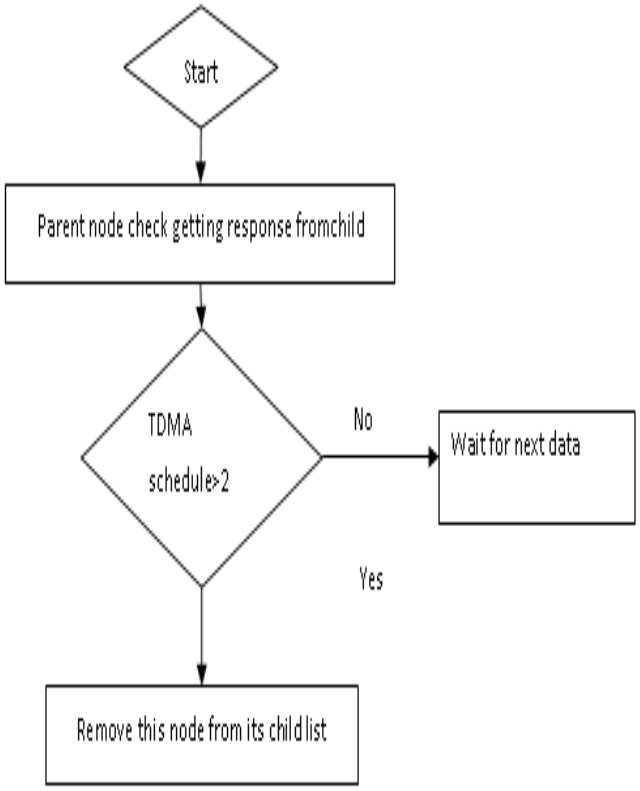


Figure 4.12Flow chart for Child nod invalidation

purification
phase is shown in figure 4.10.

Step 11: Handling the node Invalidation
(a). Child node invalidation: when the data transmission take place if the parent node does not get any response from any of its child it add this node in the invalid list and wait for the next time slot. In the next time slot, the node not getting any response this node will infer as an invalid child and remove this node from its child list.
The flow chart for handling child invalidation is shown in figure 4.12.

(b). Parent node invalidation: Each node transmits the data after receiving the data request packet to from its parent node. If any node does not receive the data request from the long time (approximately 2 time slot), it delete the father node from its list. And send the join request packet. And Re-join the tree.

The flow chart for handling parent node invalidation is shown in figure 4.13.

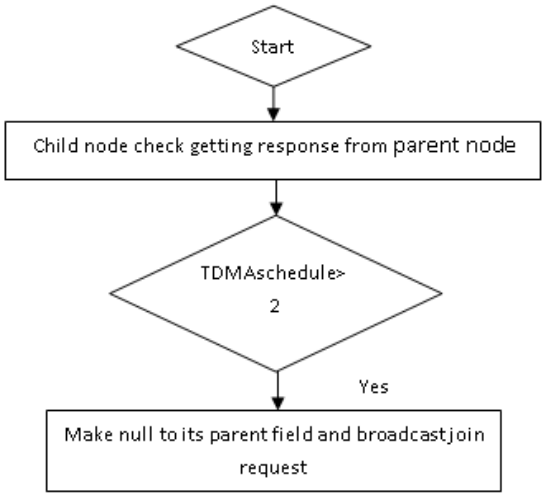


Figure 4.13 Flow chart for parent nod invalidation

Step 12: Handling the energy constrains: There are two possible value of the energy level of the node.

- A node with an energy level lower than half of the original battery capacity but higher than the average energy level.
- A node with an energy level higher than half of original battery.

(a) A node with an energy level higher than half of the original battery capacity If the node energy level is lower than half of the original battery capacity but higher than the average energy level (Threshold value) then move the node one level lower and increase the level count by 1. Otherwise, if the node energy level is lower than the threshold value then move this node to the lowest level.

(b) If the leaf node has the energy higher than the battery capacity then move this node one level above and decrease the level count by 1.

COMPARISON

5.1 Average Time for First Node to die vs. Number of nodes

in case of TBRP protocol average time take time taken to first node die is more as compared to LEACH & .TEEN that the first node of TBRP protocol dies first when 20 nodes were taken for simulation. But as the number of nodes increases the performance of the TBRP protocol improves. This is because when less nodes are deployed, nodes were scattered very far from each other, so in order to form a tree structure more control messages were required and node had to move in order to be a part of a tree. Because of the mobility and more control messages transmitted by node, more energy was consumed hence the first node in the network with less number of nodes die early in case of TBRP. But as the number of nodes are increases then in tree formation phase the control message energy is consume and energy in mobilty is less hence the performance of TBRP protocol improve.

5.2 Network Life Time vs. Number of nodes

The network lifetime vs. Numbers of nodes. The performance of TBRP protocol is better when the number of nodes increase because of the fact that as the number of the nodes increases, less mobility of nodes is required to form the tree structure and the number of control messages also decreases hence the performance of TBRP Protocol increases.

5.3 Average Energy Consumed Vs. Time

The average energy consumed by the nodes vs. time. Initially, the energy consume in the TBRP protocol is little high than the LEACH & TEEN protocols because of the mobility of the nodes and numbers of control messages required are more. Each node broadcasts the join request and receives several join request from other nodes to form a tree structure, so initial energy consumption of the node is little high due to number of control messages but once the tree is form the energy consumption decreases. Thus the performance of the TBRP protocol increases as the time increases than LEACH & TEEN. Thus the TBRP protocol is energy efficient protocol for the Mobile Sensor Networks (MSNs).

5.4 Average delay vs. Number of nodes for TBRP

The average delays vs. number of nodes for different levels for TBRP protocol. When we simulate TBRP Protocols, the average delay is high for the level 2 nodes and less for the level 0 nodes (Nodes near to the Base Station). The figure 6.4 shows that as average delay at the various levels is not increasing proportionally to the increase in the

numbers of nodes. As the numbers of nodes have increased, there is a very small change in the delay. This shows that delay will not be much for large number of nodes hence this protocol can be used for more number of nodes and is scalable.

5.5 Average Data Rate vs. Number of node for TBRP Protocol

The average data rate vs. number of nodes for TBRP Protocol. TRBP protocol is a tree based routing protocol and each node in the tree has some level. The average data rate of node at different level .Data rate for TBRP protocol in the nodes near to the base station is high. As the level of nodes increases the average data rate decreases. The number of nodes increases the data rate also increases. The energy consumption at level 0 is more than in case of level 2, because of more data rate. Since in TBRP protocol when the nodes reach a critical energy level, they move to the next higher level where energy consumption is less; hence the life time of the nodes as well as network increases.

5.6 Average Energy Consumed vs. Number of node for TBRP

The number of nodes vs. average energy consumed in TBRP protocol. In the TRBP protocol, each node in the tree has a level. The average energy consumed by nodes at different level is shown in figure 6.6. The energy consumption of nodes near to the base station i.e. level 0 is higher than the nodes at level 1 & level 2 because the receiving energy of these nodes is higher than the other nodes at level 1 or level 2. So the nodes that are at level 0 will consume more energy. In case of TBRP as the nodes reach a threshold value of energy, they move from level 0 to level 1 and so on to next level, where the energy consumption is less. TBRP thus reduces the failure of nodes and increases the network lifetime.

CONCLUSION

Mobile Sensor Networks (MNSs) have enhanced performance over static wireless sensor networks because of the mobility of the nodes. In static WSNs, the nodes closer to the sink always lose their energy first, thus causing the overall network to "die". In this work TBRP has been proposed to build an optimum mobility pattern for maximum energy efficiency. The other advantage of TBRP is that it is better targeting because sensor nodes are deployed randomly, therefore there is often a requirement to move the sensor nodes for better sight or for close proximity to the physical activity. Mobility in TBRP helps in better quality of communication between sensor nodes. TBRP is a Mobile Wireless Sensor Network Protocol. TBRP protocol improves nodes and network life time by moving the node to the next higher level. Simulation results show that the nodes in level 0 consume more energy than at higher level. When these nodes at lower level reach a critical level of energy, they move to next higher level, where energy consumption is less thus improving the life time of the nodes and network. Simulation results show that because of mobility in TBRP energy dissipation is more efficient. Simulation results also show that the TBRP protocol for Mobile Sensor Networks (MSNs) performs better than the Static Networks (SSNs) Protocols such as LEACH and TEEN. The TBRP protocol is energy efficient than LEACH and TEEN.

References

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Communications Magazine, Volume: 40 Issue: 8, pp.102-114, August 2002.

[2] C. Intanagonwiwat, R. Govindan and D. Estrin, "Directed diffusion: A scalable and robust communication paradigm for sensor networks", in the Proceedings of the 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'00), Boston, MA, August 2000.

[3] R. Shah and J. Rabaey, "Energy Aware Routing for Low Energy Ad Hoc Sensor Networks", in the Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC), Orlando, FL, March 2002.

[4] D. Braginsky and D. Estrin, "Rumor Routing Algorithm for Sensor Networks," in the Proceedings of the First Workshop on Sensor Networks and Applications (WSNA), Atlanta, GA, October 2002.

[5] C. Schurgers and M.B. Srivastava, "Energy efficient routing in wireless sensor networks," in the MILCOM Proceedings on Communications for Network-Centric Operations: Creating the Information Force, McLean, VA, 2001.

[6] M. Chu, H. Haussecker, and F. Zhao, "Scalable Information-Driven Sensor Querying and Routing for ad hoc Heterogeneous Sensor Networks," The International Journal of High Performance Computing Applications, Vol. 16, No. 3, August 2002.

[7] Y. Yao and J. Gehrke, “The cougar approach to in-network query processing in sensor networks,” in SIGMOD Record, September 2002.

[8] N. Sadagopan et al., “The ACQUIRE mechanism for efficient querying in sensor networks,” in the Proceedings of the First International Workshop on Sensor Network Protocol and Applications, Anchorage, Alaska, May 2003.

[9] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless sensor networks," in the Proceeding of the Hawaii International Conference System Sciences, Hawaii, January 2000.

[10] S. Lindsey and C. S. Raghavendra, "PEGASIS: Power Efficient Gathering in Sensor Information Systems," in the Proceedings of the IEEE Aerospace Conference, Big Sky, Montana, March 2002.

[11] L. Hu, and D. Evans, “Localization for mobile sensor networks”, in: Tenth International Conference on Mobile Computing and Networking (MobiCom’04), Philadelphia, Pennsylvania, USA, September 2004, pp. 45–57.

[12] AlineBaggio, and KoenLangendoen “Monte Carlo localization for mobile wireless sensor networks”, Ad Hoc Networks 6 (2008) 718–733.

[13] Shen-HaiShee, Kuochen Wang, I.L. Hsieh, “Color-theory-based dynamic localization in mobile wireless sensor networks”, in: Proceedings of Workshop on Wireless, Ad Hoc, Sensor Networks, August 2005.

[14] J. Hightower, R. Want, and G.Borriello “SpotON: An indoor 3D location sensing technology based on RF signal strength”, Technical Report UW-CSE 00-02-02, Springer, Seattle, February 2000.

[15] R. Peng and M.L. Sichitiu, “Robust probabilistic constraint based localization for wireless sensor networks”, in: Second Annual IEEE Communications Society conference on Sensor and Ad Hoc Communications and Networks (SECON’05), Santa Clara, CA, USA, September 2005.

[16] D. Niculescu, and B. Nath “Ad hoc positioning system (APS) using AoA”, in: IEEE INFOCOM 2003, San Francisco, CA, USA, 2003 (March–April).

[17] D. Niculescu, and B. Nath, “Error characteristics of ad-hoc positioning systems (APS)”, in: ACM Mobihoc’2004, Tokyo, Japan, May 2004

A Survey on Testing Services in Cloud Computing

Surbhi Kapoor
Jaypee Institute of Information and Technology Noida, India
surbhikapoor0509@gmail.com

Shilpi Sharma
Jaypee Institute of Information and Technology Noida, India
shilpi.sharma.er@gmail.com

Jitendra Kumar Seth
Ajay Kumar Garg Engineering College, **Gzb**
mrjkseth@gmail.com

***Abstract* - Cloud computing has seen a rapid growth as an emerging technology in the past few years. The use of different services provided by the cloud has gained a lot of popularity. Many IT companies, business organizations well as end users use different services provided by the cloud such as infrastructure, software, platform, security, storage, computing etc. Since last 5-6 years, Testing is a new name added to the list of services provided by the cloud. Earlier testing approaches used by companies for testing their software incurred a lot of cost and were time consuming. Cloud testing has solved all these drawbacks of traditionally testing a software. Testing as a service (TaaS) in cloud is used by many companies to test their software or web applications by simulating real traffic with the help of cloud. In this paper we have surveyed the Testing as a Service model of the cloud with its advantages over the traditional methods and its future objectives and scope. Finally, we conclude our work with the challenges and issues that come with testing in cloud computing.**

Keywords—cloud computing; software testing; testing as a service (TaaS)

INTRODUCTION

Cloud computing has been the fastest growing technology that has supplied the users all around the world with almost all types of services. From business organizations to IT companies to end users, cloud services have brought immense benefits and cost savings. Testing has been a recent service that has shifted to the cloud with all its developments from 2009 and after. According to a research from Fujitsu [1], testing and development is the second most popular workload being put on the cloud (57%) after websites (61%).

Software testing is a procedure in which an application or a program is executed with the intention of detecting the software bugs. It is used by software developers to test whether their software is validated and verified to perform as per the requirements.

Traditional approaches of testing a software has a few drawbacks. It incurs a lot of cost because servers, network and storage devices are required for testing purpose for a limited amount of time. Companies have to set up labs for testing their products and these labs stay useless for a long period of time. Underutilization of these resources adds to the cost.

In some of the applications, extensive resources are required for testing. For example testing a bank website or an online shopping website for scalability and performance requires loading it with millions of users for a small interval of time. Also mobile application developers require testing their applications on different types of platforms. Also we know that more and more services are migrating towards cloud, so testing of these services over cloud is necessary for their verification. All these requirements have shifted the testing services to the cloud. A voice over IP telephony network

management system was tested in Amazon's cloud costing for less than US$130[2].

The rest of the paper is divided as follows. In section II, we will discuss the various service models provided by the cloud computing. In section III, we will review the related work on testing as a service in cloud. In section IV, discussion and evaluation of related work has been done. Finally in section V, we conclude our work with the improvements that can be done in the field.

SERVICE MODELS IN CLOUD COMPUTING

Cloud computing offers many types of services which are benefited by IT companies, business organizations and end users as well. All these services are provided by cloud vendors to the customers on a pay-per-use basis. The basic service models provided by the cloud are as follows:

Infrastructure as a Service: This service model delivers hardware, storage, servers and other network components to the customers as per their requirements. These components delivered are hosted by the cloud vendor only. The customer just rents them in the quantity as per his demand, uses them, pays on hourly, weekly or monthly basis and then releases them. The infrastructure provided by the cloud vendors is highly scalable which can be adjusted as per the demand of customer.

Platform as a service: Platforms that include different types of operating systems and related services are also delivered by various cloud vendors over the internet. The customers do not have to purchase licenses for required software but instead they can use the hardware and software tools provided by the vendors required for their application development. This eliminates the need for downloading and installing tools. The hardware and software tools are hosted by the service providers themselves.

Software as a service: This includes delivery of various types of applications to the customers over the cloud. The customers can use the software given on the cloud without getting concerned about the latest updates or so. The software are managed by the vendors only and are accessed by customers through web browsers.

Apart from these three basic service models, other models are also there in the list of cloud services.

Desktop as a service (DaaS) means a virtual desktop is provided to the customer access to which is independent of the device, network and location. During logon and logoff, the customer's personal data is copied to and from the virtual desktop. The responsibilities of backup, security, data storage and up gradation of data is on the shoulders of service provide

Another service provided is Backend as a service (BaaS) which delivers mobile and app developer's backend storage for linking their applications. Other features provided by BaaS include integration with social networking services, push notifications and user management. This service is a new development in cloud area with its major developments starting from 2011.

Communications as a Service (CaaS) is a very fast growing communication service that cloud vendors provide which include videoconferencing, instant messaging, VoIP (Voice over IP). Its evolution is along the same path as SaaS.

Monitoring as a Service (MaaS) is still an evolving technology in the cloud environment which is likely to grow and gain more popularity in future. The customer can log onto their applications from any location and can manage it accordingly. This service like others reduces the cost load of the companies as against fully managing the service on their own.

Finally there is a service that provides either one or combination of Platforms as a Service (PaaS), Infrastructure as a Service (IaaS), Software as a Service (SaaS), Monitoring as a Service (MaaS) or Communication as a Service (CaaS). It is termed as XaaS or Everything as a Service in the cloud. XaaS is a term that is evolving for recognized services that were previously separated on public or private clouds.

Apart from all these services, Testing as a Service (TaaS) is also there in the list of service models of the cloud. We are surveying this service in our paper with its possible directions. We have observed the advantages of this service over traditional approach of testing software.

RELATED WORK

In this section, we will be going through some of the work that has been done in the area of testing in the cloud.

The author in the paper [3] has introduced and clarified testing services in cloud including its objectives, scope, features, benefits and distinct requirements. A detailed comparison between conventional software testing and testing in cloud has been given by the author. The unique features of cloud based software testing are detailed by the author that include cloud-based testing environment, utility billing and pricing, on demand testing, large scale test simulation and SLA based software testing. According to author, there are three different types of testing as a service in the cloud which are TaaS for web-based software on clouds, TaaS on clouds and TaaS over clouds. Also the issues and challenges in building TaaS based clouds and also the technical problems have been detailed by the author.

In [4], the author has given the benefits of performing software testing on cloud. The author initially explains the advantages of cloud computing which includes providing large computing power, security, reliability, scalability and many more. Author then describes the process of software testing which includes drawing up the test plan, constructing the test environment and executing the test cases and finally analyzing the results and optimizing. The flaws in this traditional software testing approach are mentioned which include difficulty in configuring test environments and test cases, difficulty in obtaining large scale computing power,

high cost incurred in purchasing required hardware and software and so on. After that, advantages of performing testing in cloud are detailed. These advantages are less cost, rapid response, easier expansion and improved efficiency. Thus author has given the positives and developing trends in software testing field in cloud computing.

In [5], the author has proposed a model driven method for testing the cloud environments on the basis of security. Author mentions that this has been the first approach till date that performs security testing of cloud which is based on risk analysis. As design flaws are the risk prone areas in a software system, so risk analysis has been performed on design level to give securer software. This analysis will give negative requirements which will be used to generate test cases. In the proposed approach, test related information has been separated from the system model of cloud to allow system model's independent development. The system model is defined manually by either the cloud provider or consumer whereas the sub-models of test model i.e. the Risk Model (RM), the Negative Requirements model (NRM) and Misuse case model (MCM) are automatically generated via Model-to-Model transformations. RM is generated out of system model with the vulnerability repository as the input. RM gives the identified risks depicted in a domain specific language. An M-to-M transformation is applied on RM to get NRM. NRM has negative requirements. Finally the third sub-model i.e. MCM will contain the malicious activities which will define possible attacks against CUT which will give the test cases. The model will cover 80% of the manually discovered risks.

In the paper [6], the author proposes an approach to manage the testing tasks submitted by the customers to the cloud. The testing tasks have some uncertainties. The deadlines and conflicts associated with testing tasks and also their runtime environments are analyzed so as to determine the relationships between them. On the basis of this analysis, clustering algorithms are made to divide the similar tasks into groups. Two of the clustering algorithms have been given in the paper that are quick clustering and constrained clustering. After that dynamical scheduling of these clusters are done so as to assign them to the suitable VMs to finally accomplish the SLA requirements and balance the load efficiently. Also a fault tolerant mechanism is proposed to deal with testing errors so as to get a high level of agreements for service level. Author has performed a set of experiments to compare his proposed algorithms with the other existing algorithms. On the basis of faults or errors detected from fault tolerance mechanisms, clustering and scheduling algorithms can be improved.

In the paper [7], the author has offered a static testing platform in cloud to the customers. This platform can be accessed via famous browsers such as firefox and IE. This architecture is named as Static testing Cloud System (STCS). The architecture is built on Hadoop with the component Hadoop distributed file system for cloud storage and mapreduce components for choosing working servers. Authors have also developed a static testing tool called DTS. A distributed column oriented database has been chosen for static data storage testing so as to decrease storage occupation of results of testing. The characteristics of the STCS include website cluster model, centre request end assistant model and cloud storage system over the cluster. All the valid customers register their accounts on STCS. It is a pay-per-use model. The software to be tested must be first compressed and then the package must be uploaded and tested by executing it stepwise. The test results can further be downloaded from a remote server. Author has given the future direction on static testing by considering the scheduling methods used for allocating testing tasks to the nodes. Author suggests that waiting time of the tasks should not be too long.

In [8], a testing model has been developed to test the mobile applications of cloud on different platforms and environments. This way testing of mobile apps is cost-effective. The challenges in testing mobile devices have been discussed which include diversity of devices ranging from mobile phones to tablets, diversity in Operating systems of devices on which applications will run ranging from Android phones to Windows phones to iOS. Also the networks of the devices and their runtime environments are different which is a challenge for testing the mobile applications. The model developed for testing mobile applications focuses on overcoming these challenges. It has features like emulator through which any mobile device with any OS or network can be emulated in no time. Another feature is customers don't actually have to buy the devices for performing testing. Also automated testing tools can be installed in the model as per the requirements. Such a testing model will be cost effective and time saving.

DISCUSSION AND EVALUATION

Testing in cloud can be either viewed as a service provided to the customers to test their services over the cloud or it can be viewed in a second way as testing the services provided by the cloud. In one of the papers reviewed in above section, risk based security testing of cloud services has been done. In another paper, managing testing tasks submitted to the cloud has been done. In another paper discussed, application and development of providing software testing in cloud along with its advantages over traditional method has been given. Yet another paper discusses the scope and objectives of TaaS (Testing as a Service) over the cloud. This testing service has been a newer service in cloud with all its development starting from 2009 and after. Till then, many of the work have been done in this area. We have tried to discuss and evaluate this testing service model to our best in the paper.

CONCLUSION AND FUTURE WORK

Testing services provided by the cloud vendors are very beneficial for IT companies and many business organizations for verifying and validating their application or product in the cloud environment. These services have their advantages in terms of scalability, lesser cost and availability of large computing power resources and so on. The developers can test their applications over a variety of platforms with the help of cloud. However testing in cloud comes with its own challenges that include lack of automation testing tools, problems in defining cost models and some security issues, unauthorized access and more. Due to security problem and other drawbacks, some business organizations still prefer to follow traditional testing approach. There is a need to address these challenges so that more and more focus goes on using the testing service model of cloud instead of depending on the traditional testing approaches. Also further work must be done so as to reduce the waiting time of testing tasks to be submitted to the cloud. For this, proper scheduling algorithms must be applied on the tasks submitted to the cloud for testing.

References

[1] Confidence In Cloud Grows, Paving Way For New Levels Of Business Efficiency," Fujitsu, 2010.

[2] Z. Ganon and I.E. Zilberstein, "Cloud-Based Performance Testing of Network Management Systems," Proc. IEEE 14th Int'l Workshop Computer Aided Modeling and Design of Communications Links and Networks (CAMAD 09), IEEE CS, 2009, pp. 1–6.

[3] Lian Yu; Wei-Tek Tsai; Xiangji Chen; Linqing Liu; Yan Zhao; Liangjie Tang; Wei Zhao, "Testing as a Service over Cloud," *Service Oriented System Engineering (SOSE), 2010 Fifth IEEE International Symposium on* , vol., no., pp.181,188, 4-5 June 2010 doi: 10.1109/SOSE.2010.36

[4] Peng Zhenlong; Ou Yang Zhonghui; Huang Youlan, "The Application and Development of Software Testing in Cloud Computing Environment," *Computer Science & Service System (CSSS), 2012 International Conference on* , vol., no., pp.450,454, 11-13 Aug. 2012

[5] Zech, P., "Risk-Based Security Testing in Cloud Computing Environments," *Software Testing, Verification and Validation (ICST), 2011 IEEE Fourth International Conference on* , vol., no., pp.411,414, 21-25 March 2011 doi: 10.1109/ICST.2011.23

[6] Lian Yu; Xiaohu Li; Zhongjie Li, "Testing Tasks Management in Testing Cloud Environment," *Computer Software and Applications Conference (COMPSAC), 2011 IEEE 35th Annual* , vol., no., pp.76,85, 18-22 July 2011 doi: 10.1109/COMPSAC.2011.18

[7] Siqin Chen; Junfei Huang; Yunzhan Gong, "Static Testing as a Service on Cloud," *Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on* , vol., no., pp.638,642, 25-28 March 2013 doi: 10.1109/WAINA.2013.257

[8] Murugesan, L.; Balasubramanian, P., "Cloud based mobile application testing," *Computer and Information Science (ICIS), 2014 IEEE/ACIS 13th International Conference on* , vol., no., pp.287,289, 4-6 June 2014 doi: 10.1109/ICIS.2014.6912148

A SURVEY ON MOBILE SENSING SYSTEM

Sunil Kumar
Jawaharlal Nehru University, New Delhi, India
sunilkumarmeenajnu@gmail.com

Karan Singh
Jawaharlal Nehru University, New Delhi, India
karancs12@gmail.com

***Abstract* - Now a day Smart-phone is known as a hand keeping computer which has full of multiple properties to run the applications. The important fact is that sensor gave a platform to Smart-phone's or mobile sensing device, which are attracting for the next revolution in social networks, green technologies, local and global environmental monitoring, sensing enabled games, transportation systems etc., government, private and as well as social health care. The mobile sensing system infrastructure is as a part of a new sensing prototype leveraging humans that study on the security issues that develop in the timeserving people-centric sensing. The security of Smart-phone is being ensuring most important for these reasons that Smart-phone have unique quality that make security most challenging and it can provide best solution for security issues desired in the many areas. In this paper we describe how Smart-phones are useful in different areas for connecting peoples for better facilities with security for human at globally.**

Keywords:- Smart-phone, mobile sensing system, data aggregation, security, Smart-phone application, sensor, scope and classification, human environment.

INTRODUCTION

Mobile devices have become an integral part of human life. There are a wide range of mobile devices available in market. Due to the advancement in mobile sensing technology, one can get a well-furnished smart phone with required sensing features to capture the human activity and its surrounding.These mobile devices have a large set of sensing functions like as global positioning system (GPS), camera, microphone, etc [1].

Mobile devices have wireless sensors. These wireless sensors are playing an important role in finding the answers of many challenging problems related to regulation and monitoring of real world activities [7]. Mobile sensing devices generate a big amount of data which are important to gain insight into human activities such as health location, social activities and his surrounding like pollution, noise, weather etc [1]. This information is very helpful in developing various mobile sensing applications such as weather forecasting. The information related to these events and applications are stored in data form which forms the basis for the analysis and forecasting [5] . One of the major issues related to these data is security and integrity of data[2]. For an accurate and correct result, these data should be free from noise and replica. Thus for security point of view, these data are kept in encrypted form, which uses various encryption algorithms [7].

Users data are privacy sensitive data and it is required that no third party can see the data value. Thus, user data privacy is an important issue related to mobile sensing system. Aggregation statistics are used to study time series data, which provides mobile data security at the time of untrusted aggregator [2].

This paper consists of **10 sections**. After a brief introduction in Section 1, mobile sensing system and its Components are discussed in Section 2. Architecture of mobile sensing system is discussed in Section 3. Classification of mobile computing system and its scope are given in Section 4 and Section 5, respectively. Application of mobile sensing system is given in Section 6. Research Issues in Mobile Sensing, Research domain, work related to research domain and various research groups are discussed in Section 7, Work Related to Research Domain in Section 8, conclusion in Section 9 , respectively.

MOBILE SENSING SYSTEM COMPONENTS

Mobile devices like laptop, tablet, smart phones, Bluetooth and wireless devices uses general purpose

sensing and computing platform and interact with each other via available communication infrastructures.

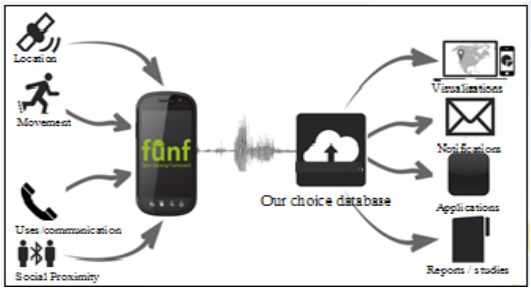


Fig. 1: Overview of Mobile Sensing System [3]

Thus, mobile sensing system can be defined as a collection of mobile devices with sensing, computing and communication capabilities for performing various real time applications. A mobile sensing system has many components like mobile sensor, microphone, camera, GPS, ambient light sensor, gyroscope, headphone and screen sensor, etc. [6].

ARCHITECTURE OF MOBILE SENSING

Architecture of mobile sensing system is illustrated in Figure 2. It has a multilayer architecture [5]. Environmental sensors and other wearable sensors exists at the first/top layer of the architecture whereas database exists at the root. In between root at top layer various other layers exists like mobile aggregation layer, mobile devices, middleware sensors etc. Middleware software that provides services to software application beyond those available from OS, makes efficient for software developers to perform communication. Data aggregation is process to gather information for statistical analysis [2]. Wearable sensors enables to large term continuous physiological monitoring for treatment and management of chronic, mental health and neurological disorders e.g. autism spectrum disorder (ASD), diabetes, depression drug addiction [5].

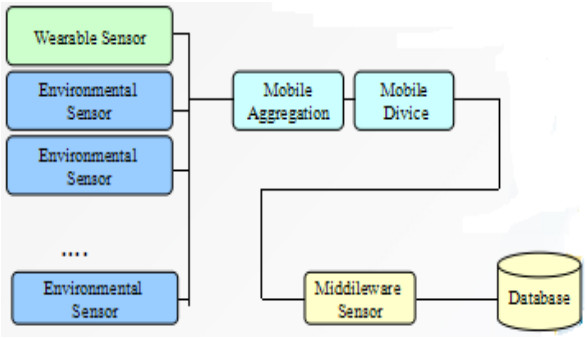


Fig. 2: Architecture of Mobile Sensing

CLASSIFICATION OF MOBILE SENSING SYSTEM

Mobile sensing system increases the facilities to human in many ways.

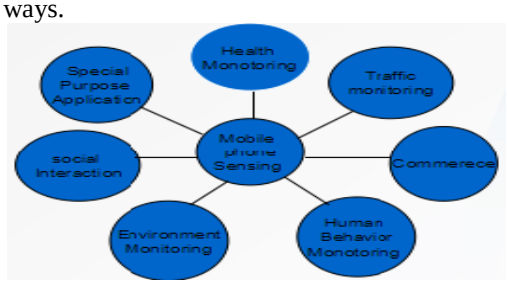


Fig. 3: Classification of Mobile Sensing Systems

On the basis of uses for the real world problem, a mobile sensing system can be classification as health monitoring, traffic monitoring, commerce, human behavior monitoring, environment monitoring, social interface, special purpose application [6]. Figure 3 is representing a classification of mobile sensing system.

SCOPE

Statista has done a survey for smart phone users in India from 2010 to 2017. This report reflects that mobile users and smart mobile phone system are rapidly increasing [9].

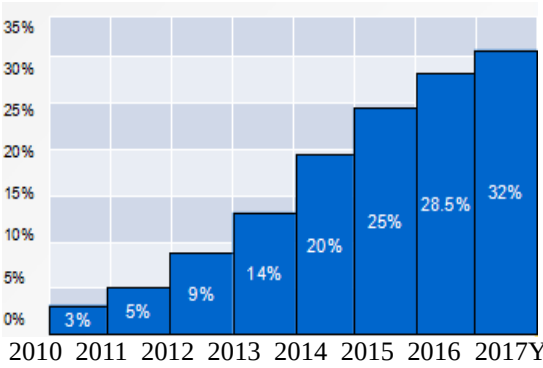


Figure 4: Scope Mobile Phone Sensing Systems

APPLICATIONS

Mobile sensing system has a wide range of application. Some major areas of application of mobile sensing system are environmental monitoring, traffic monitoring, health care, social networks, safety [2].

RESEARCH ISSUES IN MOBILE SENSING

The applications are integrated by a set of technical challenges allied with mobile sensing systems. There are some research issues in the mobile sensing as a joining the sensors, applications integration, sensing the people and their environment, develop a useful systems for real time data collection and its analysis, energy efficient and green sensing systems, interaction with users, provide

information and feedback to users, to perform data fusion across multiple domains and develop smart inferences, security in mobile sensing system, interpretation and mining of mobile sensor data.

WORK RELATED TO RESEARCH DOMAIN

We have explore the survey paper released to our research domain. Some researchers such as

Wazir Zada Khan et.al. "Mobile Phone Sensing Systems: A Survey", propose described thoroughly about all those systems which are related and acting with smart phones and mobile phone sensors for the social optimal and the better communication between the peoples.which are attracting for the next revolution in social networks, green technologies, local and as well as global environmental monitoring, private and as well as social health-care, sensing enabled games, transportation systems and as well as many areas [11] .

Delphine Christin et.al. "Security and Privacy Objectives for Sensing Applications
in Wireless Community Networks", identified important research topics and gave a light in their challenges by applying many different security and privacy from the networking and as well as cryptography to form sensing applications in WCNs[12].

Martin Azizyan et.al "Surround Sense: Mobile Phone Localization via Ambience Fingerprinting", explained that as the mobile's phone sensors are increases it create a chance for logical recognizance. And accepted that the many type of sound which are our all around, different wavelength based light and the beautiful pictures could be sensed by the camera and microphone of phone. There are also accelerometer based phone which can be useful for user motion as different matte [14].

Xuan Bao et.al. "MoVi: Mobile Phone based Video Highlights via Collaborative Sensing", try to explain to carry forward of social context with use of mobile phones as a change with the small things. Authors imagined a social application where mobile phones concurs sense their atmosphere or environment and grasp interesting information of society. The phone with a good application which can take a video recording and after that video-clips from others phones are moved into a video events of the occasion [15].

Qinghua Li et.al, "Efficient and Privacy-Aware Data Aggregation in Mobile Sensing", provide a scheme that uses the redundancy in the security to subjugate the communication cost for every join and leave. Protocols of author show evaluations is orders of magnitude batter than existing the solutions, it has lower communication overhead.

Steffen Hallsteinsen "Using the mobile phone as a security token for unified authentication",describes a hallmark strategy based on a One-Time Password (OTP) MIDlet running a smart phone for merge hallmark towards different service on the internet[16].

Sohail Khan et.al. "How Secure is your Smartphone: An Analysis of Smartphone Security Mechanisms", the basic Android security model and explained its advantages and limitations. Authors studied firstly about the android architecture like the lowest layer in the Android's architecture is the Linux Kernel that contains hardware drivers and performs low-level functionalities like memory management, threading and power management[17].

Do van Thanh et.al., "Strong authentication with mobile phone as security token", explained with an evaluation of the different way and a debate of the most probable attacks. A classification of the way is also provided, according to defined criteria [18].

A. Dardanelli et.al., "A Security Layer for Smartphone-to-Vehicle Communication Over Bluetooth", a smartphone integrates by a hierarchically distributed control system architecture with classical embedded systems is conferred, ad-hoc, and end-to –end security layer is configured to present that a smartphone can interconnected securely modern vehicle without needing changing to the existing in vehicle network, how it is possible. The result of observational present the effectuate of the set about [19].

Alexios Mylonas et.al. "Smartphone Security Evaluation The Malware Attack Case",the workable of malware progress in smartphone platforms by programmers that have turn to the official tools and smartphone platforms are provided by programming libraries. Authors studied in this paper on the security models and development environments of the surveyed **smartphone platforms:** (a). Android OS, (b). BlackBerry OS, (c). Symbian OS, (d). Apple iOS, and (e). Windows Mobile 6 OS [8].

KunalGupta, "Smartphone Security and Contact Synchronization", Authors goal is to develop an application which give solution the problem of smartphone about its security and contact synchronization by getting one's lost contacts and tracked one's lost mobile handset[9].

Yong Wang et.al. "Security Threats and Analysis of Security Challenges in Smartphones", author summarize threats and attacks on smart phone that expose the unique quality of smart phone and appraise their affect on smart phone security and search the countermeasures to surmount these challenges. There are many enterprises have already started to front into security problem in the smartphone. Hence the smartphone have the unique qualities with these solutions most equate. The smartphone can provide best solution security issues are must desired in the new business.

Mubarak AI-Hadadi et.al. "Smartphone Security Awareness: Time to Act",The result of this paper focus on a smartphone security cognizance analyze. This paper provide shameful finding and delineate effectual recommendations to smartphone extenuate security treats

and hazard. The targeting of recommendations is soul end-users as well as government or private organizations that have an integrated character in smartphone security cognizance [10]. Provide the solution related securing in mobile sensing system but still they have not provide a better solution.

Apu Kapadiay et.al., "Opportunistic Sensing: Security Challenges for the New Paradigm", Author target to inspire discussion of the decisive challenge , because opportunistic people centric sensing will never come through without tolerable victuals for security and privacy. In last author schema some important issue and suggest worldwide solutions that moderate promise in this new sensing prototype.

1. Conclusion

This paper describes the role of Smart-phones or mobile sensing systems for human environment platform that is necessary for research and development. Because sensors of mobile sensing system generate a big amount of data of human environment from different fields that can increase standard of living of human to the highest in lowest time at lowest cost globally. The most important issue in mobile sensing system is data aggregation, security and privacy when it is used to connect to each others, socially or globally interactions for communicating the information or facilities. In mobile sensing system there are many issues and challenges are required to be solved in future research work.

References

[1]. Qinghua Li, Guohong Cao, "PROVIDING PRIVACY-AWARE INCENTIVES FOR MOBILE SENSING", Department of Computer Science and Computer Engineering, University of Arkansas, Department of Computer Science and Engineering, Pennsylvania State University.

[2]. Qinghua Li and Thomas F. La Porta, Guohong Cao, "EFFICIENT AND PRIVACY-AWARE DATA AGGREGATION IN MOBILE SENSING", IEEE transactions on dependable and secure computing, vol.

[3] Akio Sashima, Takeshi Ikeda and Koichi Kurumatani, "TOWARD MOBILE SENSOR FUSION PLATFORM FOR CONTEXT-AWARE SERVICES", National Institute of Advanced Industrial Science and Technology / crest, JST, Jjapan

[4]. D.Sheela, Naveen kumar. C,Dr. G.Mahadevan,"A NON CRYPTOGRAPHIC METHOD OF SINK HOLE ATTACK DETECTION IN WIRELESS SENSOR NETWORKS", IEEE International Conference on Recent Trends in Information Technology, ICRTIT 2011.

[5]. Robert Scoble & Shel Israel, "AGE OF CONTEXT: MOBILE, SENSORS, DATA AND THE FUTURE OF PRIVACY" 1st Addition, DBA of on Demand Publishing LLC.

[6]. N.D. Lane, M. Mohammod, M. Lin, X. Yang, H. Lu, S. Ali, A.Doryab, E. Berke, T. Choudhury, and A. Campbell, "BEWELL: A SMARTPHONE APPLICATION TO MONITOR, MODEL AND PROMOTE WELLBEING," Proc. Fifth Int'l ICST Conf. Pervasive Computing Technologies for Healthcare, 2011.

[7] V. Rastogi and S. Nath, "Differentially Private Aggregation of Distributed Time-Series with Transformation and Encryption," Proc. ACM SIGMOD Int'l Conf. Management of Data, 2010.

[8]. Alexios Mylonas, Stelios Dritsas, Bill Tsoumas and Dimitris Gritzalis, et.al."SMARTPHONE SECURITY EVALUATION The Malware Attack Case", Proceedings of the International Conference on Security and Cryptography (SECRYPT), IEEE, 18-21 July 2011, Page(s): 25 - 36.

[9]. Kunal Gupta, RaviKumar, SachinLoothra et.al."SMARTPHONE SECURITY AND CONTACT SYNCHRONIZATION", Fourth International Conference on Communication Systems and Network Technologies , IEEE, 2014, India.

[10]. Mubarak AI-Hadadi, Ali AI Shidhani et.al."Smartphone Security Awareness: Time to Act ", International Conference on Current Trends in Information Technology (CTIT), IEEE ,Page(s),166 - 171, 2013 Dubai.

[11]. Wazir Zada Khan,Yang Xiang, Mohammed Y Aalsalem, and Quratulain Arshad,, "Mobile Phone Sensing Systems: A Survey", IEEE Communications Surveys & TutorialS, VOL. 15, NO. 1, First Quarter 2013.

[12]. Delphine Christin, Matthias Hollick and Mark Manulis, "Security and Privacy Objectives for Sensing Applications in Wireless Community Networks", Computer Communications and Networks (ICCCN), 2010 Proceedings of 19th International Conference on, IEEE, Page(s): 1 - 6, 2-5 Aug. 2010, Zurich.

[13]. J. Hicks, N. Ramanathan, D. Kim, M. Monibi, J. Selsky, M. Hansen, and D. Estrin, "AndWellness: An Open Mobile System for Activity and Experience Sampling," Proc. Wireless Health, pp. 34-43, 2010.

[14] .Martin Azizyan ,Romit Roy Choudhury, Ionut Constandache, "SurroundSense: Mobile Phone Localization via Ambience

Fingerprinting",September 20–25, 2009, Beijing, China.

[15]. Xuan Bao, Romit Roy Choudhury, . "MoVi: Mobile Phone based Video Highlights via Collaborative Sensing ",June 15–18, 2010, San Francisco, California, USA.

[16]. Steffen Hallsteinsen, Ivar Jørstad, "Using the mobile phone as a security token for unified authentication",Second International Conference on Systems and Networks Communications, IEEE,Pp 78-98, No:68,Pp 78-98,2007,Cap Esterel

[17]. Sohail Khan, Mohammad Nauman, Abu Talib Othman, Shahrulniza Musa, "How Secure is your Smartphone: An Analysis of Smartphone Security Mechanisms", Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conferencein in IEEE,No:76 - 81,Kuala Lumpur.

[18]. Do van Thanh, Tore Jenvik, "Strong authentication with mobile phone as security token", Mobile Adhoc and Sensor Systems, 2009. MASS '09. IEEE 6th International Conference, No: 777 - 782, 12-15 Oct. 2009, Macau.

[19]. A. Dardanelli, F. Maggi, M. Tanelli, S. Zanero, S. M. Savaresi, R. Kochanek, and T. Holz.,"A Security Layer for Smartphone-to-Vehicle Communication Over Bluetooth",IEEE Embedded Systems Letters, VOL. 5, NO. 3, September 2013

[20] .Yong Wang, Kevin Streff, and Sonell Raman, "Security Threats and Analysis of Security Challenges in Smartphones", IEEE Computer Society,2012.

[21]. Kapadia, A. ; MIT Lincoln Lab., Lexington, MA ; Kotz, D. ; Triandopoulos, N. "Opportunistic Sensing:Security Challenges for the New Paradigm",Communication Systems and Networks and Workshops, 2009. COMSNETS 2009. First International ,IEEE, 5-10 Jan. 2009, Page(s): 1 -10, Bangalore.

Survey on Cloud Computing Security Models

Shilpi Sharma
Jaypee Institute Of Information Technology Noida, India
shilpi.sharma.er@gmail.com

Surbhi Kapoor
Jaypee Institute Of Information Technology Noida, India
surbhikapoor0509@gmail.com

Jitendra Kumar Seth
Ajay Kumar Garg Engineering College, Gzb
mrjkseth@gmail.com

***Abstract*-Cloud computing is considered as the next generation of information technology system. It includes various types of resources and services which are provided to the users on demand. As more number of users are using the services of the cloud. This rapid increase in the cloud computing demands makes it more vulnerable and increases serious security issues. Absence of security is the only problem in the wide acceptance of cloud computing. Cloud computing encompasses many security and privacy issues like securing the data, analyzing the use of cloud by the cloud vendors, identification of the cloud users/vendors, authentication of data. In this paper we analyze security and privacy concerned issues related to cloud and survey some cloud security models. These cloud security and privacy models aims in achieving higher security. In this paper we analyze the security issues concerned with cloud computing models and study various kinds of solutions provided to solve these issues**

Keywords—Cloud Computing, Security

INTRODUCTION

Cloud computing is a paradigm that stores data and various applications by using internet and remote servers. Resources are accessed from the cloud from anywhere at any time using the internet . The users of cloud only pay for those resources which are allocated to them. Cloud has left all the available distributed computing technologies far behind in terms of competition popularity and success. The main reason behind this is that any kind of resources can be scaled up or down as and when needed based on the customer's requirement. Cloud computing provides organizations with an efficient, flexible and cost effective alternative to hosting their own computing resources [1]. However, hackers, attackers and security researchers have shown that this model can be compromised and is not 100% secure [2]. There are many security problems which appear inside or outside of the cloud vendor's/user's environment.

The Cloud Computing has three service delivery models which are as follows:

1. Software as a Service (SaaS): It is a model in which applications are organized by a vendor or cloud service provider and made available to the customers over a network.
2. Platform as a Service (PaaS): It is a model in which cloud vendor deliver applications over the Internet and holds users' hardware and software on their infrastructure.
3. Infrastructure as a Service (IaaS): It is a model in which third-party cloud provider hosts virtualized cloud computing resources over the Internet.

The Cloud Computing has four deployment models which are as follows:

1. Private Cloud: It is a cloud computing architecture that is implemented within the firewall of the organisation under the direct control of the

Information Technology department. It includes a well defined and secure cloud environment in which only the allowed used can operate.
2.Public Cloud: Public cloud is based on cloud computing model in which a cloud service provider makes the resources available to the general public over the network. Public clouds are established much faster and with more flexibility. Public clouds provides services to multiple users using the same shared infrastructure.
3. Community cloud.: It is a multi-tenant infrastructure that is shared between various organizations with common computing concerns.
4.Hybrid Cloud: It is an integrated cloud model including both the private and public clouds to perform various functions within the same corporate. It is a cloud computing environment in which a corporation delivers and controls some resources inside the organization and also externally provides to others.

Due to the ever growing interest in cloud computing, there is an explicit and constant effort to evaluate the current trends in security for such technology, considering both problems already identified and possible solutions[3]. In cloud we have identified the main security problems in the different areas and group them into seven categories which are as follows:

1. Network security: This includes problems related to network communications and configurations concerning cloud computing infrastructures. It consists of the provisions and approach approved by a network administrator to avert and monitor unwanted access, exploit, alteration, or denial of resources. Network security includes the permissions to access data in the network, which the network administrator manages.
2. Data security: It includes protection of data regarding confidentiality, availability and integrity of data. When organizations move applications/data to the cloud , problems arises from data storage, industry compliance needs, privacy and third party responsibility regarding the management of sensitive data.
3. Virtualization: It includes separation between VMs, hypervisor vulnerabilities and other problems which are associated with the use of virtualization technologies. Virtualization changes the relation between the Operating System and hardware. This challenges conventional security aspects. There are many vital security related problems we need to take care while using virtualization for cloud computing. One possible new risk has to do with the potential to balance a virtual machine hypervisor. If the hypervisor is unprotected, it will become a primary prey. In the cloud, such kinds of risks will have a wide impact if not otherwise reduced.
4.Interfaces: It concentrates on all the issues related to the user and administrative for using and controlling the clouds.
5. Governance: It includes issues related to administrative and security controls in cloud computing environment. Governance in the organization is the set of processes, procedures, strategies, laws, affecting the way an enterprise works, managed or controlled. Corporate governance includes the relationship between the stakeholders and the plans of the company involved.
6. Compliance: It includes requirements that are related to the service availability and audit capabilities. Almost every regulation needs organizations to appropriately protect their physical and informational resources. For doing this, there is a presumed potential to control and prove:

- Which type of information is stored on the system?
- Where is the data stored?
- Who can access the data in the system?
- What can they access?
- Is the access suitable?

All the above questions states a level of ownership of the above stated questions, and that is where cloud compliance issues appears.
7. Legal issues: It includes aspects that are related to judicial demands and law. Now days it is essential that organizations should know where their data is placed at all times. In the cloud environment, location of the data matters, particularly from a legal point of view. Cloud computing legal issues arises from where the cloud vendor keeps the data, including the applications of foreign data security laws and espionage.

LITERATURE SURVEY

In the paper[4] the author has introduced some cloud computing systems, current security and privacy problems in the cloud and examines the approaches to tackle these issues. In the paper four types of cloud computing systems are described that are Amazon, Google, IBM and Windows. These cloud computing systems are used to store and manage the data resourcefully. Moreover the systems also reduce the complexity of programming in the cloud, performs the scheduling of tasks, provides the cloud platform for the developers. As all these cloud systems are running in the internet, it is very obvious that they will definitely face the security and privacy issues. The main security problems in cloud are data privacy and availability of service. In the paper many security vulnerabilities are described like virus attacks and intrusion by various hackers and malicious users, fast recovery of resources,

data control, data integrity. In cloud The users are unaware of the location of the data and the servers handling the data. So that the cloud computing services must be improved and protected. In the paper the author has described the three traditional techniques to protect and secure the user data that are encryption mechanisms, security authentication techniques and access control approaches. The encryption methods are of two types symmetric key encryption and asymmetric key encryption. Security authentication approach includes PKI technology and X.509 certificate standard .The access control mechanism ensures that network resources are not illegal to use. It contains network access control and directory level security control. At last the author provides some more security measurements which can be included in the cloud environment. The movement of worms and viruses in cloud must be controlled. Harmful programs should be isolated. On damage, the system must be repaired instantly. The data traffic must be monitored in real time. The uncommon action of network and system should be detected and fixed on time. Defence system must be established in the cloud network. Approaches of disaster recovery in cloud computing must be installed that includes system backup and data recovery.

In the paper[5] the author has researched on the data security model based on multi dimension.The model uses a multi-dimension hierarchical architecture of three layers of defence. .All the three layers have their own responsibilities and are combined with each other for providing more data security in the cloud environment. The first layer is responsible providing authentication, digital certificates and permissions to the user. In this layer user is authenticated to ensure that user data is not altered. The authenticated users can then perform various operations on the data such as modification, addition and deletion. Moreover for the purpose of privacy each authenticated user is granted a digital certificate. The second layer is responsible for providing encryption. In this layer if the unwanted user uses unlawful means to defraud the authentication system the file automatically gets encrypted. The third layer is responsible for providing fast recovery of the user data. In this layer the user data gets regenerated several times even if it damaged. In this model users do not need to concern about the lost of data..

In this paper[6] the author has introduced a new cloud computing security management structure which is based on arranging the FISMA standard to apt the cloud computing model, which will enabling both the providers and consumers of the cloud to get to get certified. The main aim of the approach is to improve and support the partnership between various cloud stake holders to develop a standard cloud security specification covering all of their requirements. The proposed framework architecture consists of three layers which are management layer, enforcement layer, and feedback layer. The *Management layer is responsible for representing* security specifications like security services, risk assessment services, security control manager and multi-tenant security service. *The Enforcement layer* is responsible for providing security planning and security controls selection which are based on the identified risks. *The Feedback layer* has two key services, monitoring service and analysis service. This layer is responsible for collecting the various measures to make sure that the system is operating within the specified boundaries of each metric.The proposed framework is also implemented on a testbed cloud platform. On evaluating it was found that the approach is comprehensive that supports all the perspectives of the stakeholder and satisfying their demands.

In this paper[7] the author presents a new strategy that provides more security to cloud environment using reconfigurable computing. The proposed strategy depends on the reconfigurable hardware that creates co-processing hardware which the user can directly use. In the strategy FPGA devices that are physical devices are used and located at the client side to provide non reproducible identity from the third party client/user. Using FPGA four different types of solution are proposed to provide security and user authentication that are trusted cloud computing platform, user enabled security groups for data collaboration, data security, verifiable attestation. These four solutions are believed to identify various kinds of attacks scenario like SPAM attacks in Cloud service user, DDOS attacks and worms in Cloud service user. The main aim of these solutions is that the responsibility of the security and privacy should be kept with the user itself. All the proposed four solution are implemented together that provides a trusted computing and allows cooperation while keeping the user data secure within the cloud environment.

In this paper[8] the author has presented a new and enhanced data security model for cloud computing. The proposed security model is based on three layer architecture. The first layer is responsible for providing user authentication. The second layer is responsible for providing data encryption, secure the privacy of users by using any of the symmetric encryption technique. The third layer is responsible for fast recovery of user data that depends on the speed of decryption algorithm. The proposed model solves many security problems. It implements API access control by making use of two way authentications. By using the top most security

algorithms, it encrypts and protects the data. Moreover this software fast retrieval of data while using encryption/decryption. The proposed application is implemented in Amazon EC2.On implementing it has been found that this model provides more security and privacy of data and faster retrieval of data.

CONCLUSION AND FUTURE WORK

In this paper we first discussed the security issues of the cloud. These issues include Network security, Data security, Virtualization, Interfaces, Governance, Compliance and Legal issues. The main aim of these issues is to protect and manage the data in the cloud. Cloud Computing is not fully established and still needs lots of improvements. Security is the most significant risk to both the cloud providers and the users. Later we discussed different approaches and models that have been proposed to overcome the problem of security. Finally as cloud computing is a interesting technology that is established in the IT industry we need to consider several parameters and most vital of them is the security. While doing the survey on security problems in cloud environment we came to know that there are no existing security standards available for the security of cloud computing. In our future, we will try to implement security standards for cloud computing.

References

[1] Cloud Computing – A Practical Approach by Velte, Tata McGraw- Hill Edition (ISBN-13:978-0-07-068351-8)

[2] Wesam Dawoud, Ibrahim Takouna and Christoph Meinel, "Infrastructure as a service security: Challenges and solutions," in 2010 The 7th International Conference on Informatics and Systems, 2010, pp. 1-8

[3] Ibrahim AS, Hamlyn-Harris J, Grundy J (2010) Emerging Security Challenges of Cloud Virtual Infrastructure. In: Proceedings of APSEC 2010 Cloud Workshop, APSEC ’10

[4] Wentao Liu, "Research on cloud computing security problem and strategy," *Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on* , vol., no., pp.1216,1219, 21-23 April 2012

[5] Zhang Xin; Lai Song-qing; Liu Nai-wen, "Research on cloud computing data security model based on multi-dimension," *Information Technology in Medicine and Education (ITME), 2012 International Symposium on* , vol.2, no., pp.897,900, 3-5 Aug. 2012

[6] Almorsy, M.; Grundy, John; Ibrahim, A.S., "Collaboration-Based Cloud Computing Security Management Framework," *Cloud Computing (CLOUD), 2011 IEEE International Conference on* , vol., no., pp.364,371, 4-9 July 2011

[7] Mondol, J.-A.M., "Cloud security solutions using FPGA," *Communications, Computers and Signal Processing (PacRim), 2011 IEEE Pacific Rim Conference on* , vol., no., pp.747,752, 23-26 Aug. 2011 doi: 10.1109/PACRIM.2011.6032987

[8] Mohamed, E.M.; Abdelkader, H.S.; El-Etriby, S., "Enhanced data security model for cloud computing," *Informatics and Systems (INFOS), 2012 8th International Conference on* , vol., no., pp.CC-12,CC-17, 14-16 May 2012

Comparative Analysis of VoMPLS and Optimized VoMPLS

Shruti Thukral
IEC College of Engg and Technology Greater Noida, India
thukralshruti.10@gmail.com

Banita Chadha
IEC College of Engg and Technology Greater Noida, India
banit23@yahoo.com

***Abstract*— Voice over Internet Protocol (VoIP) is the most used service in today's scenario because of its low operational and infrastructural cost. Multi Protocol Label Switching (MPLS) is an extension to Internet Protocol (IP) to provide better Quality of Service (QoS). The Voice over Multi Protocol Label Switching (VoMPLS) is a technique of sending the voice packets directly to MPLS backbone. Our objective is to reduce the MPLS Header present in VoMPLS packet structure and optimize VoMPLS. This paper presents the comparative analysis of VoMPLS and optimized VoMPLS using the tool Network Simulator-2 (NS-2) under the four QoS parameters i.e. Delay, Jitter, Throughput and Packet Loss.**

Keywords—Multi Protocol Label Switching(MPLS), Quality of Service(QoS), Voice over Multi Protocol Label Switching (VoMPLS).

INTRODUCTION

In the last years, the exponential growth of communication services over the Internet has grabbed the interest of many researchers. Enterprises are depending on VoIP services in very growing rate. The usage of VoIP services reduced a huge amount of cost for their infrastructure. But providing the real time application on the Internet is a challenging task for the conventional IP networks as it uses the Best effort services. The main issue with VoIP was the difficulty of delivering high service quality as it does not provide Traffic Engineering. MPLS is an emerging standard technology works to solve the shortcoming of IP networks and also speeds up the network traffic flow. MPLS is not the replacement of the Internet Protocol but it adds the set of rules to the IP so that the traffic can be classified, marked and policed.

MPLS is the key development standardized by IETF. MPLS works in coordination with the layer 2 and layer 3 networks. As the name suggests it is able to work with multi kinds of protocols and existing infrastructures such as ATM, PPP, Frame Relay and HDLC with higher compatibility [3]. However, the reality is that the emphasis of MPLS has till date been only supporting the Internet Protocol [2]. It reduces the process time of transporting a packet by making the routing decision based on a simple label instead of the whole IP prefix look up. MPLS is very flexible in its signaling plane, which convinced a lot of voice service providers to apply this new technology on their backbone [3].

A Label Switch Router (LSR) is a MPLS node that is capable of forwarding layer 3 packets. This MPLS node or router can operate at the core of the network or at the boundary of the network [9]. If the LSR is at the core of the network then it is used to route the packets by looking up at the label and swaps the label before it is sent to the output port of the node. If the LSR works at the boundary of the network then it is termed as the Label Edge Router (LER). According to its functionality the LER can be categorized as Ingress LER and Egress LER. The Ingress router pushes the Label on the incoming packet and the Egress router pops the label from the packet and delivers it to the destination. The path formed between the two Label Edge Routers is known as Label Switched Path (LSP) and is used to forward the label packets through this path. This path is established by the signaling protocols in the MPLS domain. MPLS supports different signaling protocols such as Label Distribution protocol (LDP), Constraint-based routing Label Distribution Protocol (CR-LDP), Resource Reservation protocol- Traffic Engineering (RSVP-TE).

Quality of Service is defined as set of techniques to classify and manage network resources with the help of which certain

level of packet loss, bit rate, jitter, delay etc., can be guaranteed. It is a means to prioritize important traffic over less important traffic and make sure it is delivered. The different QoS requirements for the voice traffic can be fulfilled by MPLS when used in conjunction with DiffServ architecture and MPLS Traffic Engineering (TE) [1].

There are many possible arrangements in which voice may be carried in an MPLS environment and one of them is Voice directly over MPLS (VoMPLS) which is discussed in this paper.

This paper encompasses the five main sections; the first section describes the related work associated with MPLS. The second section describes the VoMPLS architecture, VoMPLS packets structure and explains the working of VoMPLS as compared to VoIP. The third section describes the proposed methodology to optimize VoMPLS. The fourth section explains the simulation topology to carry out the comparison of VoMPLS and optimized VoMPLS and shows the result under the four QoS parameters i.e. delay, jitter, packet loss and throughput. The last and the fifth section include the study conclusion and proposed future work.

RELATED WORK

In [4], the writers of this paper have compared the MPLS network with the traditional IP network in regards to its performance, using NS2 as the simulation tool. The study shows that the performance of the IP networks can be increased by the use of Traffic Engineering in MPLS network by utilizing the links which are underutilized over the traditional IP network. The MPLS- TE makes MPLS to be used with IP to provide better performance. In [8], the authors have has compared the quality of voice traffic with the video traffic in MPLS network concluding that, giving priority to the voice traffic makes it perform better over non prioritized video traffic. The study focuses on priority queuing and concludes that giving priority to the voice packets enhances performance of network to voice packets compared to the non-prioritized video packets. In [6], the author made a comparative analysis of MPLS over Non-MPLS networks and shows MPLS have a better performance over traditional IP networks. In this paper a comparative study is made on MPLS signaling protocols (CR-LDP, RSVP and RSVP-TE) for Traffic Engineering by discussing their functionality and classification. Simulation of MPLS and Non-MPLS network is done, performance is compared by considering the parameters such as packet loss, throughput and end-to-end delay on the network traffic. QualNet 4.0 simulator is used for simulation purpose. In [2],authors of this paper has showed that combined use of the MPLS DiffServ and MPLS TE is guaranteed to provide end to end QoS for multi service traffic in IP networks. QoS performance is analyzed for different type of services including VoIP, real time video and best effort data traffic. In [5], authors of this paper have investigated the impact of MPLS TE signaling protocols on real time voice, video, HTTP and FTP transmissions over MPLS networks. Two signaling protocols are compared i.e. CR-LDP and RSVP-TE and simulation showed that CR- LDP signaling protocol has a noticeable performance advantage as compared to the RSVP TE signaling protocol. In [7], this the paper mainly focuses on the analytical models to measure efficiency of voice over IP network with applications on MPLS network. In this paper network models are presented to support quality of service (QoS) requirements and traffic engineering standards supported by MPLS. The author uses mathematical expressions for evaluating the models for both IP and MPLS networks.

VOMPLS

In VoMPLS, MPLS is used as the core network. The voice packets without the IP encapsulation send directly to the MPLS networks. This is a very efficient transport mechanism for sending the voice packets. Fig.1. shows the VoMPLS reference architecture.

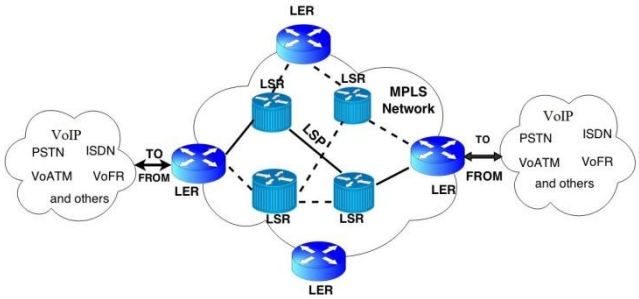


Fig.1. VoMPLS Reference Architecture

A typical VoMPLS multiplexing structure consists of a mandatory outer label, zero or more inner labels, and one or more VoMPLS primary subframes. The MPLS/VoMPLS packets are simply addressed by the use of labels. The main label, called the outer label, is mandatory, and all LSRs along the path read this label and forward the packets based on the label value [9]. The inner label and the CID are used for multiplexing different traffic flows into one MPLS packet. The use of MPLS therefore leads to more efficient use of the links. When multiplexing, each Subframe inside a single MPLS packet has the same outer label, while the inner label may differ and the CID is unique for the specific channels.

This reduces the amount of overhead, thus decreases the processing in each router.

As compared to IP 24 octets header, a simple MPLS header only consists of the outer label (4 octets), that is if there is no multiplexing involved. This may led to decreased processing time in the routers. VoMPLS routing and forwarding technique is more efficient technique than VoIP because the forwarding table in IP is quite large and as the size of the table increases, the look up time also increases whereas in MPLS label tables are small in size as compared to IP routing tables as MPLS network consists of specified and fixed paths that makes MPLS forwarding table confined. This has improved the quality of the voice transmission as it helps in reducing delay, jitter, congestion and packet loss. But Enterprises keep demanding better so our main is to optimize the performance of VoMPLS so as to give better Quality of Service to the end users.

TOWARDS AN OPTIMIZED VOMPLS

As we have discussed in Section III, that VoMPLS packet structure consists of a mandatory outer label, zero or more inner labels, and one or more VoMPLS primary subframes. The outer label in the VoMPLS packet structure is the simple MPLS header of 32 bits. The first 20 bits in this header defines the label value. This value can lie between 0 and 2^{20}-1. The next three bits i.e. 20-22 (EXP) bits are used for QoS. The Bit 23 is the Bottom of the stack bit (s) and set to 1 to denote the bottom label in the stack. The last 8 bits i.e. 24 to 31 used for Time To Live (TTL). TTL field is implemented as a counter and its value is decremented at each hop. If the TTL field reaches zero before the packet arrives at the destination then that packet is discarded. Maximum Value of the TTL field is 255 and the initial recommended value is 64. In this paper, we have reduced the MPLS header by reducing the TTL field by 2 bits and the simulated the results using NS-2.

SIMULATION TOPOLOGY AND RESULTS.

TestBed Design

The Simulation environment employed in this paper is based on NS-2. MPLS is setup as the core network. The network consists of 14 nodes i.e. 8 MPLS nodes and 6 IP nodes. All links were set up as duplex. The bandwidth and delay vary between the links. DropTail queuing is used which serve packets on First Come First Serve (FCFS) basis. The traffic connection was setup between 5 links i.e. node 5 and node 6, node 2 and node 4, node 4 and node 6, node 2 and node 5 and node 3 and node 1 using UPD with CBR of 1000 bytes packets.

First the simulations are carried with the original VoMPLS packet structure. Then using the same topology and environment the simulation are carried for the proposed VoMPLS packet structure. The comparison is then made by tracing the results from the trace file with the help of awk scripts.

Simulation Results

The four QoS parameter: delay, jitter, throughput and packet loss are used to compare VoMPLS and optimized VoMPLS. By reducing the header size VoMPLS has shown better results in terms of delay and jitter. It is able to send more number of packets with less delay. But there is no improvement in throughput and packet loss ratio. As Voice packets are more sensitive to delay and less sensitive to packets loss we can say that proposed or optimized VoMPLS is better.

Fig.2. shows the average delay versus simulation time. When the simulation is run for 100 seconds the delay is lower in VoMPLS but as we increases the simulation time the delay becomes lower in optimized VoMPLS.

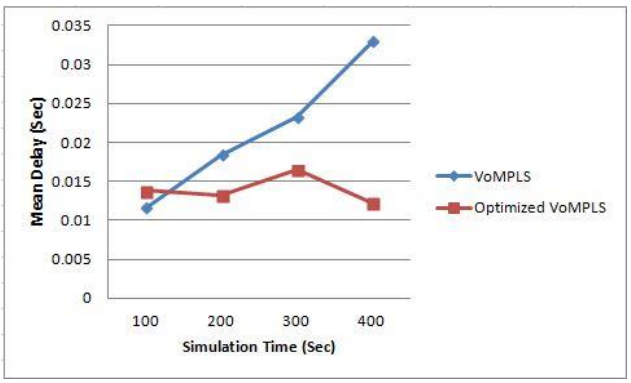


Fig.2. Mean Delay Comparison of VoMPLS and optimized VoMPLS

Fig.3 shows the average jitter versus simulation time. As the simulation time increases the jitter gets higher in VoMPLS.

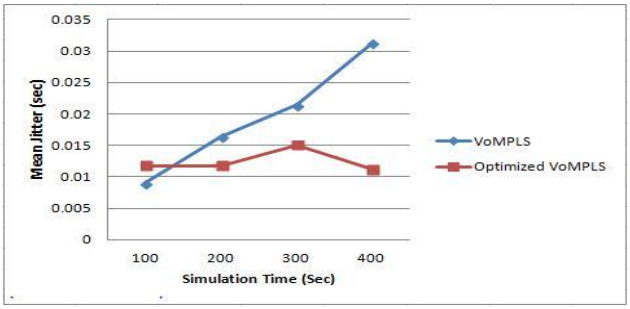


Fig.3. Average Jitter Comparison of VoMPLS and optimized VoMPLS

Fig.4 shows the throughput versus simulation time. Initially the throughput was better in VoMPLS but as the simulation time increases the throughput in both VoMPLS and optimized VoMPLS become same.

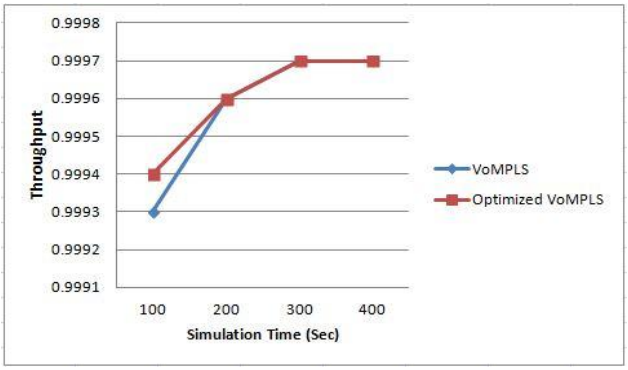


Fig.4. Throughput Comparison of VoMPLS and optimized VoMPLS

Fig. 5 shows packet loss ratio versus simulation time. There is very slight difference in the packet loss ratio. Optimized VoMPLS has a little better performance in packet loss.

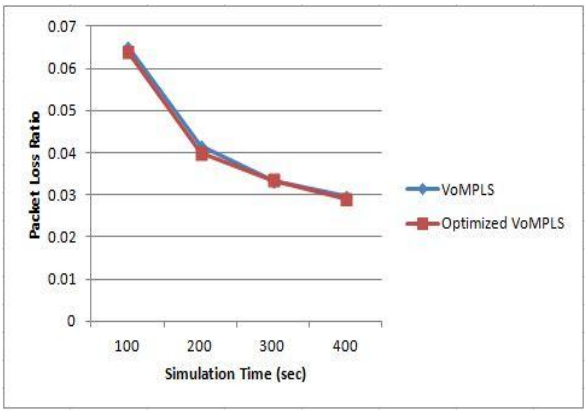


Fig.5.Packet Loss Ratio Comparison of VoMPLS and optimized VoMPLS

CONCLUSION AND FUTURE WORK

In this paper, we have proposed a methodology to optimize VoMPLS by reducing the outer label of the VoMPLS packet structure and compared it to the original VoMPLS using NS-2 and compared the results using the four QoS parameters. The proposed methodology is better has it has shown better results for delay and jitter but the optimized VoMPLS has no impact on throughput and packet loss ratio. VoMPLS can further be optimized by reducing the header size of VoMPLS primary Subframe which is of 4 octets.

References

[1] Amer Alkayyal, Stelios sotiriadis and Eleana Asimakopoulou, "Optimizing Voice over Multiprotocol Label Switching", IEEE, 2013, ISBN- 13972062, pp. 466-469.

[2] Dongli Zhang and Dan Ionescu, "QoS performance analysis in deployment of DiffServ –aware MPLS traffic engineering", IEEE computer society, 2007, pp. 963-967.

[3] Junaid Ahmed Zubairi. " Voice transport techniques over MPLS," IEEE, *pp. 25-29.*

[4] M. A. Rahman, A. H. Kabir, K. A. M. Lutfullah, M. Z. Hassan, and M. R. Amin, " Performance analysis and the study of the behavior of MPLS protocols", IEEE, *2008,* pp. 226-229.

[5] Mahmoud M. Al-Quzwini and Sarmad K. Ibrahim, " Performance evaluation of traffic engineering signal protocols in IPv6 MPLS networks", Scientific Research, 2012, vol.4, pp. 298-305

[6] M. Kr. Porwal, A. Yadav and S. V. Charhate, "Traffic analysis of MPLS and Non-MPLS network including MPLS signaling protocols and traffic distribution in OSPF and MPLS", IEEE computer society, 2008 pp.187-192.

[7] Nader F.Mir., Albert Chien, "Simulation of Voice over MPLS communications networks," IEEE computer society, Washington DC, 2002, pp. 389-393.

[8] O. Gure, B. K. Boyaci, and N. O. Unverdi,2010.Analysis of the service quality on MPLS networks, in Circuits and Systems for Communications (ECCSC), 2010 5th European Conference on, pp. 43-46.

[9] S. Rajagopalan1, E.R. Naganathan2, and P. Herbert Raj, "Ant Colony Optimization Based Congestion Control Algorithm for MPLS Network," IEEE, pp.214-223.

Security on Mobile Agent Based Web Crawlers

Manisha Singh Raghav
Galgotias College Of Engineering and Technology Greater Noida, India
raghavmanisha@gmail.com

Ayushi Chaudhary
Galgotias College Of Engineering and Technology Greater Noida, India
ayushichaudhary24@yahoo.com

Dev Gupta
Galgotias College Of Engineering and Technology Greater Noida, India
dev.gupta1056@gmail.com

***Abstract* - Mobile agents are programs that can be dispatched from one computer and delivered to a remote computer for execution. They also provide a single uniform paradigm for distributed object computing, encompassing synchrony and asynchrony, message-passing and object-passing, and stationary objects and mobile objects This paper deals with a system based on web crawler using mobile agent. The proposed approach uses Java Aglets for crawling the web pages and also describes Aglets framework which remains highly vulnerable to Denial of Service (DoS) attacks despite multilayered security provided by existing frameworks caused due to cloning.In this paper general security objectives for migrants are identified and corresponding mechanism for facing the identified threat of cloning attacks leading to DoS has been designed.**

Keywords – mobile agents , aglets, DoS , cloning .

INTRODUCTION

A Mobile Agent is an emerging technology that is gaining momentum in the field of distributed computing. The use of mobile agents can bring some interesting advantages when compared with traditional client/server solutions, it can reduce the traffic in the network, it can provide more scalability, it allows the use of disconnected computing and it provides more flexibility in the development and maintenance of the applications. Using mobile agent i.e. mobile crawlers, the method of selection and filtration of web pages can be done at servers rather than search engine side which can reduce network load caused by the web crawlers. In this paper we are using aglets platform for mobile agent working. Aglets are Java objects that can move from one host on the Internet to another.That is,an aglet that executes on one host can suddenly halt execution, be dispatched to a remote host, and resume execution there. When the aglet moves, it takes along its program code as well as its data. Conceptually, the aglet is a mobile agent because it supports the ideas of autonomous execution and dynamic routing on its itinerary.

Mobile Agent System

Mobile Agent System consists of two main components: mobile agents and mobile agent platforms (Aglet platform i.e. Tahiti server) . Mobile agents are software which is goal-directed and can automatically suspend their execution on one platform and migrate to another platform, where they resume execution to accomplish their tasks. Mobile agent platforms are execution environments for mobile agents on different computers, including the home platform and guest platforms. A home platform of a mobile agent is responsible for creating, initializing, dispatching, receiving, and eliminating a mobile agent. The home platform environment is the most secure environment.

Security

Security is a fundamental concern for a mobile agent system. Harrison et al. identify security as a “severe concern” and regard it as the primary obstacle to adopting mobile agent system.

The operation of a mobile agent system will normally be subject to various agreements wheather declared or tacit. These agreements may be violated , accidently or internally , by the parties they are intended to serve. A mobile agent system can also be threatened by parties outside of the agreements they may create rogue agents ;they may hijack existing agents ;or the may commandeer interpreters.

In this paper we are using aglets platform in order to support the development of mobile agents. The execution environment within which Aglets are executed is referred to as the Aglet's Context and is responsible for enforcing the security restrictions of the mobile agent.

The different states in Aglet life cycle are as follows[7]:

Activated: Aglet is loaded from storage and allowed to resume execution.

Deactivated: Aglet's execution is halted and its state is saved.

Cloned: Aglet is copied for concurrent execution.

Disposed: Execution of the aglet ceases permanently

Created: Aglet is initialized for execution

Dispatched: Aglet is sent to another execution context.

Retracted: Aglet is obtained from another execution context.

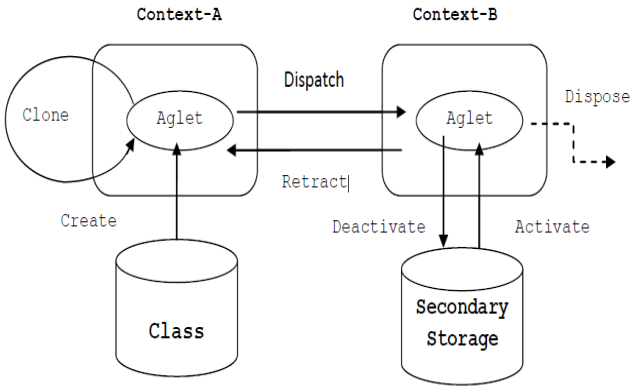


Figure 1: Aglet Life-cycle

The aglet framework remains highly vulnerable to Denial of Service (DoS) attacks despite multilayered security provided by existing frameworks. The first layer of security is provided by the Java Virtual Machine. The second layer of security is provided by the security manager of aglet platform and the final layer is Java's new Security API. Attacks against availability mainly attempt to overload the resources or make a particular facility unavailable at a certain time, thus making them unavailable to genuine entities. Attacks in this category are usually referred as Denial of Service (DoS) attacks.

In this paper, *we have demonstrated "detection of DoS attack on aglet platform caused due to cloning".*

Cloning in mobile agents

Cloning (Lange and Oshima, 1998) is a feature of mobile agent system which creates a new instance of same agent with same state. We define a mobile agent clone as the copied agent.To clone one of the agent, aglet uses clone() method declared in java.lang.Object class. The population of mobile agents in a networked system could impact their performance. An increase in population of mobile agents through cloning impact their performance whereas uncontrolled cloning can lead to excessive consumption of network resources resulting in chaos. . This causes problems connected with agent authentication, unexpected multiple transactions, and other security issues.

However, the system cannot reliably distinguish the original agents from the clone. This is because agents do not carry keys. Thus , if the code and data of the clone are to be authenticated , they must have the same cryptographic checksum as the original agent, as the private keys of the sender and author are not available to construct new ones. Thus the code and the signed data of the clone must be identical to the original. Thus , to distinguish between them at all , we must examine the unsigned portion of their state ,and there is no guarantee that these components ave not been tampered.

Clone Agent

It is impossible to distinguish an agent clone from its original agent, once it is generated . The clone assumes the role of the original agent itself when it executes and even the agent server which creates the agent cannot distinguish between the two[3]. This problem leads to the following problems :

- Impossibility to authenticate an unique agent
- Unexpected multiple execution of agents
- Disclosure of agent's internal information by parallel execution

Impossibility to authenticate an unique agent :

When an agent server receives a mobile agent, since the agent server cannot know whether it is clone or not, it cannot ensure that the agent is the only one instance of the agent in a given distributed system.

This may make the behaviour of the agent server meaningless to the true agent, if the latter is rejected and another instance of the agent isaccepted as a valid agent by the agent owner. Also, this may give the owner of the agent the opportunity to repudiate the agent or to say that it is not responsible for such agent execution Another authentication problem arises while communicating with the agent. When some object (agent server or another agent) wants to communicate with the agent, first it will find the location of the agent. If the object finds that the agent exists at several places simultaneously, it will be confused as to which agent it should communicate with.

Even though it selects one of them and communicates with it, it cannot ensure that the effect of the communication will be applied to that agent, i.e the communication may mean nothing to that agent's behaviour. Also from the viewpoint of the agent server, the effects of the communication by the agent may be repudiated by the agent owner or may be ignored by the agent owner since it has no responsibility for such communication[5].

Unexpected multiple execution of agents

An agent server may execute the same agent several times, which results in multiple execution of the same transaction. For example, if one agent buys an airplane ticket and an agent server knows the mission of this agent, the server may execute the agent several times by making clones so that the agent buys many tickets[5].

Disclosure of agent's internal information by parallel execution

When an agent server executes a mobile agent, the server can read all the code and data of the agent. This leads to serious problems pertaining to protection of mobile agents. This problem is not one that can be easily solved. But even if this problem is solved, in other words, if the mobile agent can conceal its code and data from an agent server, it may extract the agent's internal information which produces agent's action, and expect the next agent action from the outputs, produced through parallel execution of clones providing different input to each one of them[5].

CLONE ATTACK

It is a feature of mobile agent system which creates a new instance of same agent with same state. To clone one of the agent, aglet uses clone() method declared in java.lang.Object class. The recursive use of the clone() method results in a agent performing Denial of Service attack (Evens et al., 2007) on Aglet platform.[6] Those agents keep on cloning itself until platform resources are exhausted. After this any new request will cause "OutOfMemoryError" Exception to be thrown by JVM and further requests are either denied or server execution gets aborted.

What is "OutOfMemoryError" Exception?

The subclasses of Error (Boyland, 2005) represent errors that are normally thrown by the class loader, the virtual machine, or other support code. Application-specific code should not normally throw any of these standard error classes. This error is thrown when the JVM fails to allocate memory.

JVM Memory Allocation

Heap (Boyland, 2005) is the runtime data area from which memory for all class instances and arrays are allocated. It is created at the JVM start-up. Heap memory for objects is reclaimed by an automatic memory management system which is known as a garbage collector. Heap size is controlled with -Xms/-Xmx startup parameters.

If a computation requires more heap than the available memory by the automatic storage management system, the JVM throws an "OutOfMemoryError". Non-Heap Memory (Boyland, 2005) The Java virtual machine manages memory other than the heap which is referred as non-heap memory.

The JVM has a method area which is shared among all threads. The method area belongs to non-heap memory. It stores per-class structures such as a runtime constant pool, field and method data, and the code for methods and constructors. It is created at the JVM start-up. The method area is logically part of the heap but a JVM implementation may choose not to either garbage collector compact it. In addition to the method area, a JVM implementation may require memory for internal processing or optimization which also belongs to non-heap memory.

Clone Attack Mitigation Algorithm

Input: threshold: = maximum number of agents that can be created.

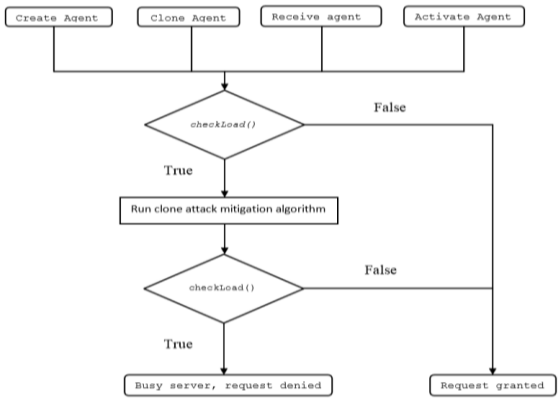
Output:cloned agents are disposed

Algorithm:

Step 1:Get the list of agents and its clone count.
Step 2: Repeat
➔ If clone count of agent > 60 % of threshold
Then dispose all cloned agents
➔ If clone count of agent > 25% and less than 60% of threshold
Retain 20% clone corresponding to that agent and dispose rest of them.
disposed clone count: = clone count + disposed clone count
Until agents count > 0
Step 3:Exit

Working of a checkload function

*Input:*threshold: = maximum number of agents that can be created
*Output:*True/False
Algorithm:
Step 1: Get the present agent count
Step 2: If agent count >= threshold and heap memory usage >= 80% of maximum heap memory
Return true
Step 3: Return false



Flow Chart- Clone Attack Mitigation

For our experiment purpose, we have restricted agent to clone maximum up to 70 % of the total available agent count and rest of them are reserved to high priority local agents for creation and to receive agents from other servers in the network. Whenever new request comes for execution, it will check the number of agents present in system using checkLoad function.

When the server is fully loaded and new agent request arrives, it checks for clone attack. If the attack is detected; it will either mitigate it using the aforementioned algorithm or it would display busy message. This might be the case for another type of DoS attack.

CLONE ATTACK ANALYSIS

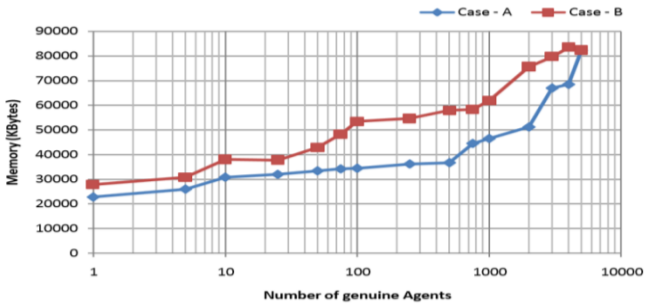
Here, we use CloneAttack agent which includes clone() method of class java.lang.Object. We have used execution environment. We then integrated clone attack mitigation algorithm within aglet platform. The graph in Figure depicts the situation after resolving the clone attack.

Case –A curve indicates the variation of memory usage with respect to number of genuine agents, after resolving clone attack.

Case – B curve indicates the variation of memory usage with respect to number of genuine agents, after detecting clone attack.

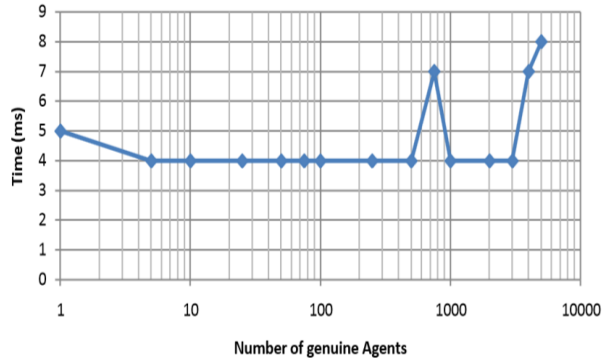
For example, at a point where number of genuine agents is equal to 1000; attack is detected. Memory usage is 107130056 Bytes and agents spawned after cloning is 5094. After mitigation the memory usage drops down to 68587536 Bytes and all cloned agents are disposed. Where at a point where number of genuine agents is equal to 5000; clone attack agents ≈131 are disposed. The total number of agents is 5000.

As the number of genuine agents approach 5000, the number of clones reduce. Hence, at 5000, the amount of memory consumed by both cases (A and B) is the nearly same.



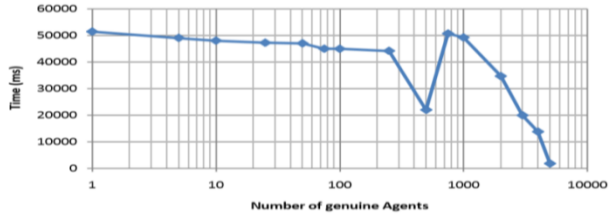
Number of genuine Agents Vs Memory Usage (KBytes)

The graph in below figure shows the variation of time requires for detection of attack as the number of genuine agents is increased. Detection time includes the time required for obtaining the list of agents from the system and detecting the clones out of them. Variation in the detection time with respect to number of genuine agents is negligible and can be assumed to be constant. As seen from the graph, the detection time remains constant (4 ms) till the number of genuine agents is 3000. Beyond that, the detection time increases linearly with increase in number of agents.



Number of genuine Agent Vs Attack detection time (ms)

The graph in below depicts the plot of Number of genuine agents vs. time for mitigation of the clone attack. On an average, as the number of agent increases, Mitigation time decreases. Because as the number of agents increase, the number of clones to be disposed off decreases. The graph is not purely linear because the nature of cloned agent also affects the mitigation time. If the cloned agent contains an infinite loop or highly complex computation like the factorization problem, cloned agent's response is slowed down and thus the mitigation time increases.



Number of genuine Agents Vs Mitigation Algorithm Processing Time (ms)

CONCLUSION

Mobile agents have gained a great deal of attention in research and industry in the recent past. Although mobile agents are a promising technology, the large-scale deployment of agents and the existence of hosts running agencies will not happen until proper security mechanisms are well understood and implemented. In this paper, security of mobile agents has been considered from the point of view of both the mobile agent and the agent platform.To avoid the DoS attacks caused due to cloning attacks the mitigation algorithm has been used and further performance evaluation is done based upon the memory usage and processing time in case of attacks as well as when no attack. Future Research on this field is envisaged through the definition of new architectures using such mechanism and deployment of new application in which protection is provided on mobile agent by digital signature. Also, the exact specification of the trust algorithm in mathematical terms with analysis of security properties for specific types of security mechanisms and their effect on trust may be considered. Moreover, the mobile agents can be made self-secure i.e. agents protect their code and data by carrying their own protection mechanisms.

FUTURE SCOPE

We have proposed a solution to overcome the Denial pf Service attack caused by cloning.Excessive message generation and too many agents in a platform can overwhelm the whole system.This work can be extended to prevent DoS attacks caused by other means viz. synchronized thread class and infinite object creation.Further future developments can include key distribution mechanism in agent architecture.We need to define which key distribution model best suits the security model and thus serving to the previous results which were capable of detecting as well as mitigating the DoS attacks thus resulting in reduced CPU and memory utilization.

References

[1]. Niraj Singhal, R. P. Agarwal, Ashutosh Dixit, A. K. Sharma,|| Information Retrieval from the Web and Application of Migrating Crawler||, International Conference on Computational Intelligence and Communication Systems,2011, pp. 476-480

[2]. Wayne Jansen and Tom Karygiannis, "Privilege Management Mobile Agents,Twenty-third

National Information Systems Security Conference, pp.362-370, October 2006.

[3]. William M. Farmer, Joshua D. Guttman, and Vipin Swarup,"Security for Mobile Agents: Issues and Requirements " The MITRE Corporation 202 Burlington RoadBedford,MA01730-1420 ffarmer,guttman,swarupg@mitre.org

[4]. DannyB.Lange1, Mitsuru Oshima1, Gunter Karjoth2, and Kazuya Kosaka1," Aglets: Programming Mobile Agents in Java" Tokyo Research Laboratory,IBM Japan Ltd and Zurich Research Laboratory ,IBM Swiss Ltd.

[5] Gunter Karjoth,Danny B.Langea nd Mitsuru Oshima "A Security Model for Aglets," IEEE Intenet ComputingVolume 1 Number4 ,July/ August1997,pages 68-77

[6] Version 0.2 Programming Mobile Agents in Java™ - With the Java Aglet API Danny B. Lange and Mitsuru Oshima©1997 http://www.cis.upenn.edu/~bcpierce/courses/629/papers/AgletsBook-elements.html

[7] Md. Abu Kausar and V. S. Dhaka ,Dept. of Computer & System Sciences, Jaipur National University, Jaipur, and Sanjeev Kumar Singh ,Dept. of Mathematics, Galgotias University, Gr. Noida, India ," Web Crawler Based on Mobile Agent and Java Aglets ",I.J. Information Technology and Computer Science, 2013, 10, 85-91 Published Online September 2013 in MECS (http://www.mecs-press.org/)

[8]. Naghavi M. and Sharifi M., (2012) ―A Proposed Architecture For Continuous Web Monitoring Through Online Crawling Of Blogs‖, International Journal of UbiComp (IJU), Vol. 3, No. 1..

[9]. Hurst M. and Maykov A., (2009) ―Social Streams Blog Crawler‖, In Procedings of the 2009 IEEE Interntional Conference on Data Engineering.

[10]. Aglet Development group, (2009). "The Aglet-2.0.2 User's Manual.

[11]. Danny B. Lange and Mitsuru Oshima, (1999). "Seven Good Reasons for Mobile Agents", Vol. 42, No. 3 Communications of the ACM, March 1999.

[12] Elhum Nusrat, Abu Shohel Ahmed, Gazi Mushfiqur Rahman, and Lafifa Jamal, (2008). "SAGLET- Secure Agent Communication Model", 11th International Conference on Computer and Information Technology (ICCIT 2008) 25-27 December, 2008, Khulna, Bangladesh

[13]. S.Venkatesan and C.Chellappan, (2008). "Protection of Mobile Agent Platform through Attack Identification Scanner (AIS) by Malicious Identification Police (MIP)", First International Conference on Emerging Trends in Engineering and Technology, 2008.

[14]. Naghavi M. and Sharifi M., (2012) ―A Proposed Architecture For Continuous Web Monitoring Through Online Crawling Of Blogs‖, International Journal of UbiComp (IJU), Vol. 3, No. 1.

[15]. Wayne Jansen and Tom Karygiannis, ―Privilege Management Mobile Agents, Twenty-third National Information Systems Security Conference, pp.362-370, October 2006.

[16]. Wayne Jansen and Tom Karygiannis, (2000). "NIST Special Publication 800-19 –Mobile Agent Security", National Institute of Standards and Technology Computer

Empirical Validation of OO Metrics for Change Proneness Prediction Using Open Source Software Systems

Anushree Agrawal
Ajay Kumar Garg Engineering College, Ghaziabad
anushreeagrawal.iet@gmail.com

Abstract - **Software is the heartbeat of modern day technology. In order to keep up with the pace of modern day expansion, change in any software is inevitable. Defects and enhancements are the two main reasons for a software change. The aim of this paper is to study the relationship between object oriented metrics and change proneness. Software prediction models based on these results can help us identify change prone classes of software which would lead to more rigorous testing and better results. In the previous research, the use of machine learning methods for predicting faulty classes was found. However till date no study determines the effectiveness of machine learning methods for predicting change prone classes. Statistical and machine learning methods are two different techniques for software quality prediction. We evaluate and compare the performance of these machine learning methods with statistical method (logistic regression). The results are based on three chosen open source software, written in java language. The performance of the predicted models was evaluated using receiver operating characteristic analysis. The study shows that machine learning methods are comparable to regression techniques. Testing based on change proneness of software leads to better quality by targeting the most change prone classes. Thus, the developed models can be used to reduce the probability of defect occurrence and we commit ourselves to better maintenance.**

Index Terms— Change proneness, Empirical validation, Object-oriented metric, Receiver operating characteristics Analysis, Software quality.

INTRODUCTION

In software industry, resources like time, cost and effort are always limited while developing and maintaining software. Extensive research has been conducted over the years to study the relationship between object oriented metrics. These studies help in efficient and effective utilization of resources. Maintenance is a very important phase of a software life cycle and is one of the most expensive phases as 40–70 % of the entire cost of software is spent on maintenance. Change proneness i.e. the probability that a particular part of the software would change is also very important and needs to be evaluated. Prediction of change prone classes can help in maintenance and testing. A change prone class needs to be tested rigorously, and proper tracking should be done for the particular class while changing and maintaining the software. In this work, we establish a relationship between various object oriented metrics and change proneness.

This paper is organized as follows. Section 2 summarizes related work. Section 3 summarizes the metrics studied and the dependent variable. Section 4 describes the Empirical data collection method. Section 5 states the research methodology. The results of the study are presented in Sect. 6 and Sect. 7 presents the conclusion of the work.

RELATED WORK

Software always keeps evolving and undergoes a number of changes, in order to enhance its functionality or to correct defects.

Han et al. [1] worked on improving the quality of design by predicting change proneness in UML 2.0 models. This was done using behavioral dependency measurement (BDM), a method used for rating classes according to probability of change. JFreeChart, a multiversion medium sized open source project was used for evaluation of the results. The results indicated BDM as an effective indicator for change proneness prediction.

Ambros et al. [2] used correlation and regression analysis in order to study the relationship between change coupling and software defects. Change coupling refers to interdependence of various artifacts of software on each other because they evolve together.

Sharafat et al. [3] proposed a probabilistic model to predict the probability of a change in each class. The probabilistic approach to determine whether a particular class will change, in the next generation of the software is based upon its change history as well as the source code. Source code, ranging over various software releases was analyzed using reverse

engineering techniques, to collect code metrics. The probability of internal change of a class,

i.e. the possibility that a class will be reformed, due to changes originating from the class itself is obtained from code metrics.

Chaumum et al. [4] defined a change impact model to study the consequences of changes made to classes of the system. A change impact model was defined and mapped in C?? language. According to their model, the impact of change depends on two main factors (a) its type, which can lead to different sets of impacted classes and (b) the type of link (association, aggregation, inheritance or invocation) between classes. A study to analyze the impact of one

change was carried out on the telecommunication system. They concluded that design of a system plays an essential role in ascertaining the system's reaction to incoming changes, and well-chosen OO design metrics can function as an indicator of changeability.

Design patterns are keys to common design complications. Bieman et al. [5] examined five evolving systems to analyze the relation between design patterns and change proneness. In four of the five patterns, classes were found to be less change prone while in one system pattern, classes were more change prone. The results guide us in learning software designs patterns that are more easily adaptable.

Tsantalis et al. [6] analyzed the effect of adding or modifying a class, on the change proneness of an object oriented design. It categorizes three axes, namely change inheritance, reference and dependency. The extracted probabilities help us to study the stability of design, over successive software versions and identify a level, beyond which remodeling of design cannot be pursued.

RESEARCH BACKGROUND

Independent and Dependent variable

In this section, we describe independent and dependent variable used in our study.

Independent variable: In this study, Object Oriented metrics are used as independent variables. Since single metric is insufficient to discover all the characteristic of software under development so we have used fifteen metrics. In this study we have selected only those metrics which are most significant to exhibit the software characteristics like inheritance, cohesion, coupling etc. All the metrics and values of these metrics are obtained by using a tool named understand for java. All the fifteen metrics i.e. independent variables are described in Table 1.

Serial No.	Metric name	Description
1	Coupling between object(CBO)	CBO is count of number of other classes to which a class is coupled.
2	Number of children(NOC)	NOC is defined as the number of immediate subclasses from a given class.
3	Number of class method	It is defined as the total number methods in a given class.
4	Number of class variable	It is defined as the total number of variables in a given class
5	Number of instance method(NIM)	It is the count of total number of instance method.
6	Number of instance variable(NIV)	It is defined as the total number of instance variable.
7	Number of local methods(NLM)	NLM is defined as the total number of local variable of a given class.
8	Response for a class(RFC)	It is the count of number of methods that can be executed when a message from an object of a given class is received.
9	Number of local private methods	It is defined as the total number of local private methods which are not inherited.
10	Number of local protected methods	It is the total number of local protected methods which are not inherited.
11	Number of local public methods	It is the total number of local public methods which are not inherited.
12	Lines of code(LOC)	Total number of lines of code in a given class.
13	Depth of inheritance tree(DIT)	DIT is defined as the maximum length from a class node to the root of the inheritance tree.
14	Lack of cohesion in methods(LCOM)	Total count of pair wise local methods in a class having no variable or attribute in common.
15	Weighted method per class(WMC)	WMC is defined as the total number of sum of cyclomatic complexity of all methods in a given class.

Table 1: object oriented metrics

Dependent variable: In software development, maintainability requires necessary modifications. So advance knowledge of change prone classes can help us to minimize extra maintainability cost of software. In this study, we have taken CHANGE as dependent variable. Change can be

analysed as number of lines added, number of lines deleted or number of lines modified. In this paper, we examine the relationship between change proneness and object oriented metrics. To examine the change proneness we use receiver operating characteristic (ROC) analysis.

Empirical data collection

In this section, we describe data sources and give detailed description of each data sources and data collection method.

We analyzed five open source software which are written in java. We found all five software from sourceforge.net. We downloaded two different version of each open source code used. In this study, we analyze changes in every class of both versions of all five software. Software we studied are ABRA , ABBOT, APOLLO, AVISYNC, JMETER and are summarized in table 2. Table 2 shows the programming language, version number, number of changed classes, number of unchanged classes, and total number of common classes and percentage of changed classes.

Datas-et	Prog. Lang.	V 1	V 2	No.of ch. cl.	Nu 0f. unch. classes	Comm. cl.	%
Abra	Java	0.9.8	0.9.9	33	147	180	18.3
Abbot	Java	1.0.0rc1	1.0.0rc3	86	241	327	26.3
Apoll-o	Java	0.1	0.2	69	183	252	27.4
Avisy-nc	Java	1.1	1.2	27	46	73	36.9
Jmete-r	Java	2.8	2.9	537	363	900	59.7

Table 2: description of each software

Data Collection Method

In this section we will explain how to collect data points for all five software. Since we have to examine all the changes in every class files of both versions (previous and current version) and values for all the metrics we have used in our study and then merge both the files (change report and metric file). To obtain complete dataset we follow some steps and these steps are:

Step 1: Metric generation process:

As we know metric is the basic unit to examine the characteristics of software. In this process we downloaded source code of two different version of five open source software (one previous and one current) as shown in Table 2 from sourceforge.net. We generated metrics for the first version of all five software (ABRA-0.9.8, ABBOT- 1.0.0rc1, APOLLO-0.1, AVISYNC-1.1, JMETER-2.8) with the help of understand tool for java. The metric file obtained in this contains metric for all classes (because in this study we are analysing changes in the classes of both version of software), methods and unknown classes which we discard while we make dataset. At the end of this stage we now have metric file for all software we have used above.

Step 2: Preprocessing step:

Since we have to find only common classes so in this step, we perform data filter to extract common classes which are common in both the versions of each software (current and previous version). A similar procedure was followed by Zhou et al. [9].

Step 3: change report generation:

To generate change report we used CMS tool for java. CMS tool works as follows: first we open CMS tool, then we click run button, it will display a popup window which demands both the versions of software. Then we click on compare button and finally it will generate change report of CSV extension. We repeat this process for other four software and we get change report of all five software.

Step 4: Merging files:

In this step, we combine metric file obtained in step 1 and change report file obtained in step 3 to yield complete dataset. Here we search common java classes in both the files and then merge them. At the end of this step we have complete dataset of all five software.

Descriptive statistics

Here we will describe statistics results of each software. Table 3, 4, 5, 6 and 7 shown below are the descriptive results that contains mean, median, mode, standard deviation, variance, minimum, maximum and percentiles for each metrics of all software used. From table 3, 4, 5, 6 and 7, we can see that the mean value of number of children (NOC) for software (ABRA-0.73, ABBOT-0.73, APOLLO-0.69, AVISYNC-0.56, JMETER-0.52) which is very low for each software, so we can conclude that number of children are very less i.e. inheritance is not much used in all five systems. LCOM metric which is defined as the total count of classes having no attribute or variable in common has greater value in all the systems (approximately 100). Similar results have been shown by other researchers [11, 13, 14].

Table 3: descriptive statistics result for ABRA dataset

	Mean	**Median**	**Mode**	**Std. Deviation**	**Variance**	**Minimum**	**Maximum**	**Percentiles**	
								25	75
CBO	3.27	2.00	0	4.286	18.367	0	24	1.00	4.00
NOC	.73	0.00	0	2.234	4.990	0	13	0.00	0.00
Cl. me.	.90	0.00	0	1.658	2.750	0	7	0.00	1.00
Cl. var.	1.03	0.00	0	2.574	6.625	0	23	0.00	1.00
NIM	7.99	5.00	0	11.161	124.559	0	67	2.00	9.00
NIV	3.04	2.00	0	5.065	25.658	0	36	0.00	4.00
Loc. me.	8.89	6.00	3	10.745	115.451	0	67	3.00	9.00
RFC	18.71	10.00	6	23.461	550.430	0	95	6.00	17.00
Lo.	.60	0.00	0	2.315	5.359	0	14	0.0	0.0

Pri. Met.								0	0
Lo. Pro. Me.	2.19	0.00	0	6.626	43.901	0	51	0.00	1.00
Loc. pu. me.	5.82	4.00	4	6.471	41.871	0	64	3.00	7.00
LOC	81.44	35.50	16	158.811	25220.941	2	932	18.00	63.75
DIT	1.81	2.00	1	.908	.824	1	4	1.00	2.00
LCOM	49.32	60.00	0	35.421	1254.644	0	100	0.00	80.00
WMC	17.77	8.00	5	31.917	1018.694	0	165	5.00	14.75

Table 4: descriptive statistics result for ABBOT Dataset

	Mean	Median	Mode	Std. Deviation	Variance	Minimum	Maximum	Percentiles	
								25	75
CBO	23.06	5.00	113	40.384	1630.893	0	113	2.00	13.00
NOC	.73	0.00	0	2.867	8.222	0	44	0.00	1.00
Cl. me.	1.98	0.00	0	5.829	33.972	0	55	0.00	3.00
Cl. var.	3.89	1.00	0	5.999	35.985	0	28	0.00	5.00
NIM	27.43	8.00	112	39.814	1585.173	0	112	3.00	29.00
NIV	11.51	2.00	0	18.765	352.122	0	52	0.00	10.00
Loc. me.	29.42	9.00	115	40.999	1680.907	0	115	4.00	29.00
RFC	60.05	30.00	115	64.276	4131.430	0	221	8.00	115.00
Lo. Pri. Met.	15.59	1.00	0	31.077	965.788	0	85	0.00	6.00
Lo. Pro. Me.	1.72	1.00	0	3.583	12.835	0	32	0.00	2.00
Loc. pu. me.	10.34	6.00	19	12.162	147.906	0	86	2.00	19.00
LOC	574.21	106.00	2656	949.358	0000 0.0	2	2656	39.00	485.00
DIT	2.24	2.00	1	1.387	1.923	1	6	1.00	3.00
LCOM	59.32	72.00	0	37.294	1390.825	0	98	19.00	93.00
WMC	86.20	19.00	369	133.556	17837.243	0	369	7.00	72.00

Table 5: descriptive statistics result for APOLLO dataset

	Mean	Median	Mode	Std. Deviation	Variance	Minimum	Maximum	Percentiles	
								25	75
CBO	5.74	5.00	0	5.242	27.475	0	35	2.00	9.00
NOC	.69	0.00	0	3.630	13.177	0	44	0.00	0.00
Cl. me.	.71	0.00	0	2.025	4.101	0	11	0.00	0.00
Cl. var.	1.33	0.00	0	2.826	7.984	0	14	0.00	1.00
NIM	8.29	5.00	5	8.804	77.512	0	82	4.00	11.00
NIV	3.69	2.00	0	4.201	17.649	0	30	1.00	6.00
Loc. me.	9.00	5.00	5	9.131	83.371	0	82	4.00	11.00
RFC	15.23	13.00	5	11.594	134.417	0	83	5.00	23.75
Lo. Pri. Met.	.39	0.00	0	1.018	1.035	0	7	0.00	0.00
Lo. Pro. Me.	.42	0.00	0	1.028	1.057	0	9	0.00	0.00
Loc. pu. me.	7.94	5.00	5	8.213	67.451	0	74	3.00	10.00
LOC	110.82	49.00	17[a]	144.418	20856.508	2	1024	26.00	130.00
DIT	1.85	2.00	2	.737	.543	1	4	1.00	2.00
LCOM	47.44	50.00	0	33.241	1104.949	0	100	13.00	77.75
WMC	18.73	12.00	5	22.862	522.678	0	229	5.00	24.00

Table 6: descriptive statistics result for AVISYNC dataset

	Mean	Median	Mode	Std. Deviation	Variance	Minimum	Maximum	Percentiles	
								25	75
CBO	3.74	1.00	0	5.273	27.806	0	27	0.00	8.00
NOC	.56	0.00	0	1.472	2.166	0	9	0.00	0.00
Cl. me.	.22	0.00	0	1.170	1.368	0	9	0.00	0.00
Cl. var.	2.27	1.00	0	3.568	12.729	0	17	0.00	2.00
NIM	8.05	6.00	1	7.612	57.941	0	32	1.00	11.00
NIV	2.08	2.00	0	2.707	7.326	0	14	0.00	3.00
Loc. me.	8.27	7.00	1	7.653	58.563	0	32	1.00	11.00
RFC	15.08	9.00	5[a]	12.246	149.965	0	44	6.00	24.00
Lo. Pri. Met.	1.85	0.00	0	4.300	18.491	0	23	0.00	2.00
Lo. Pro. Me.	.07	0.00	0	.585	.342	0	5	0.00	0.00
Loc. pu. me.	6.36	6.00	1	6.005	36.066	0	32	1.00	8.50

LOC	61.23	36.00	5	71.205	5070.209	4	359	6.50	87.50
DIT	2.26	2.00	1	1.334	1.779	1	5	1.00	3.00
LCOM	70.73	85.00	100	34.751	1207.646	0	100	59.00	98.00
WMC	12.05	9.00	1	13.197	174.164	0	68	1.50	15.00

Table 7: Descriptive statistics result for JMETER dataset

	Mean	**Median**	**Mode**	**Std. Deviation**	**Variance**	**Minimum**	**Maximum**	**Percentiles**	
								25	75
CBO	5.37	4.00	1	6.072	36.874	0	41	1.00	7.00
NOC	.52	0.00	0	2.710	7.347	0	51	0.00	0.00
Cl. me.	1.10	0.00	0	4.593	21.096	0	67	0.00	0.00
Cl. var.	3.94	2.00	1	7.539	56.844	0	75	1.00	4.00
NIM	10.02	6.00	1	12.856	165.267	0	111	3.00	13.00
NIV	3.25	1.00	0	5.928	35.143	0	55	0.00	4.00
Loc. me.	11.11	7.00	5	13.446	180.800	0	116	4.00	15.00
RFC	30.56	16.00	3	32.982	1087.840	0	206	6.00	43.00
Lo. Pri. Met.	1.84	1.00	0	3.175	10.082	0	20	0.00	2.00
Lo. Pro. Me.	.58	0.00	0	1.958	3.832	0	32	0.00	0.00
Loc. pu. me.	8.53	5.00	2	11.553	133.477	0	102	3.00	10.00
LOC	114.20	65.00	5	145.005	21026.482	2	1095	28.00	134.75
DIT	2.27	2.00	2	1.199	1.437	1	5	1.00	3.00
LCOM	67.00	76.00	0	29.875	892.494	0	100	58.00	88.00
WMC	21.45	12.00	5	28.657	821.238	0	230	5.00	26.00

RESEARCH METHODOLOGY

Performance evaluation measures:

Sensitivity: The total percentage of change prone classes that are correctly classified is known as sensitivity.

Specificity: The total percentage of change prone classes that are not correctly classified i.e. percentage of non-occurrences of correctly predicted classes.

Receiver operating characteristics (ROC)

*W*e evaluate the performance and accuracy of output of predicted model using area under curve (AUC). ROC curve (AUC) is defined as a plot of sensitivity on y-axis and 1-specificity on x-axis. The ROC curve, which is defined as a plot of sensitivity on the y-coordinate versus its 1-specificity on the x coordinate, is an effective method of evaluating the quality or performance of predicted models [7, 8]. While constructing ROC curves, we selected many cut-off points between 0 and 1, and calculated sensitivity and specificity at each cut off point. The optimal choice of the cut-off point (that maximizes both sensitivity and specificity) can be selected from the ROC curve [7, 8]. Hence, by using the ROC curve one can easily determine optimal cut-off point for a predicted model [12]. ROC curve can be drawn using SPSS tool.

Validation method:

In order to predict the accuracy of the model it should be applied to different data sets. We therefore performed a ten-cross validation of the models [10]. The ten- cross is performed using WEKA tool. In this tool, complete dataset is divided into ten subsets randomly and each time one of the ten subsets is treated as testing set and other nine subsets are treated as training sets. Hence we obtain change proneness for all ten subsets.

RESULT ANALYSIS

Univariate LR Results

Univariate is done as one to one correspondence. It is performed to examine significant and insignificant metrics. It is done by using SPSS tool and performed between one independent variable and one dependent variable. The same process is repeated of all metrics used. The same is performed for all software and we get univariate result for all software used. The univariate results of software ABRA, ABBOT, APOLLO, AVISYNC, JMETER are shown below in Table 8, 9, 10, 11 and 12.

In this section, we analyze significant and insignificant metrics based on metric sig. value. If sig. value of any is less or equal to 0.01 in three or more dataset then that metric is significant otherwise metric is insignificant. So from table 8, 9, 10, 11 and 12, we can see that CBO metric is significant because its sig. Value for ABRA dataset is 0.000, ABBOT- 0.001, APOLLO- 0.000 and JMETER- 0.000.

Table 8: univariate result for ABRA dataset

	B	**S.E.**	**Sig.**	**Exp(B)**
CBO	.215	.047	.000	1.240
NOC	.152	.070	.031	1.164
No. of class method	-.462	.221	.036	.630
No. of class variable	.071	.063	.256	1.074
NIM	.035	.015	.018	1.035
NIV	.043	.032	.181	1.044
No. of local methods	.033	.015	.031	1.033
RFC	.027	.007	.000	1.028
No. of local private methods	.021	.078	.790	1.021

No. of local protected methods	.109	.036	.003	1.115
No. of local public methods	-.024	.039	.535	.976
LOC	.002	.001	.046	1.002
DIT	.395	.204	.053	1.484
LCOM	.013	.006	.029	1.013
WMC	.010	.005	.050	1.010

Table 9: univariate result for ABBOT dataset

	B	S.E.	Sig.	Exp(B)
CBO	-.017	.005	.001	.983
NOC	.000	.044	.995	1.000
No. of class method	.118	.038	.002	1.125
No. of class variable	-.029	.023	.205	.972
NIM	-.011	.004	.005	.989
NIV	-.035	.010	.001	.966
No. of local methods	-.008	.004	.027	.992
RFC	.002	.002	.426	1.002
No. of local private methods	-.023	.007	.001	.977
No. of local protected methods	.091	.036	.011	1.096
No. of local public methods	.021	.010	.030	1.021
LOC	-.001	.000	.003	.999
DIT	.039	.090	.667	1.039
LCOM	.004	.003	.239	1.004
WMC	-.003	.001	.023	.997

Table 10: univariate result for Apollo dataset

	B	S.E.	Sig.	Exp(B)
CBO	.117	.029	.000	1.124
NOC	.005	.038	.904	1.005
No. of class method	.054	.066	.415	1.055
No. of class variable	.054	.047	.253	1.055
NIM	.027	.015	.079	1.028
NIV	.042	.032	.190	1.043
No. of local methods	.028	.015	.061	1.028
RFC	.040	.013	.001	1.041
No. of local private methods	.022	.137	.871	1.022
No. of local protected methods	.543	.150	.000	1.722
No. of local public methods	.021	.016	.195	1.021
LOC	.001	.001	.108	1.001
DIT	.015	.192	.938	1.015
LCOM	.010	.004	.023	1.010
WMC	.019	.007	.005	1.020

Table 11: univariate result for AVISYNC dataset

	B	S.E.	Sig.	Exp(B)
CBO	.142	.056	.012	1.152
NOC	-.168	.202	.405	.845
No. of class method	.129	.209	.538	1.137
No. of class variable	.071	.067	.294	1.073
NIM	.136	.042	.001	1.146
NIV	.453	.146	.002	1.573
No. of local methods	.138	.042	.001	1.148
RFC	.034	.020	.093	1.034
No. of local private methods	.186	.096	.052	1.205
No. of local protected methods	-4.138	8038.594	1.000	.016
No. of local public methods	.147	.054	.007	1.159
LOC	.011	.004	.008	1.011
DIT	-.589	.225	.009	.555
LCOM	.004	.007	.597	1.004
WMC	.093	.030	.002	1.098

Table 12: univariate result for JMETER dataset

	B	S.E.	Sig.	Exp(B)
CBO	.179	.020	.000	1.196
NOC	.212	.071	.003	1.236
No. of class method	-.038	.018	.032	.963
No. of class variable	.040	.013	.002	1.040
NIM	.061	.010	.000	1.063
NIV	.140	.022	.000	1.150
No. of local methods	.042	.008	.000	1.043
RFC	.013	.002	.000	1.013
No. of local private methods	.154	.030	.000	1.167
No. of local protected methods	.061	.041	.140	1.063
No. of local public methods	.039	.009	.000	1.040
LOC	.004	.001	.000	1.004
DIT	.215	.059	.000	1.240
LCOM	.018	.002	.000	1.019
WMC	.016	.003	.000	1.016

Model evaluation using ROC curve

Here we evaluate best model using ROC curve. The model having largest area under curve (AUC) will be the best model for a dataset. The tables below show the validation results on various datasets. Table 13 shows the validation result on ABRA dataset. Similarly Table 14, 15, 16 and 17 shows the validation result on ABBOT, APOLLO, AVISYNS and JMETER respectively. In table 13, NAIVE gave best result among all models having AUC 0.774, sensitivity and specificity are 0.727 and 0.728 respectively and its cut-off point is 0.054. In Table [14, 15], KSTAR shows the best result for both ABBOT and APOLLO software among all models having AUC 0.758, 0.779 respectively sensitivity and specificity are 0.709, 0.725 and 0.705, 0.723 respectively and

cut-off point is 0.256, 0.112. Table 16 has MLP model as the best model which outperformed other method has AUC 0.783, sensitivity and specificity are 0.667 and 0.605 respectively and its cut-off point is 0.378. Table 17 shows that RANDOM FOREST (RF) is best model because it has AUC 0.831, sensitivity and specificity are 0.795 and 0.741 respectively and cut-off point is 0.568.

These best models of each dataset can be used to predict change prone classes. The advance knowledge of change prone classes would help us to plan the test resources for the classes in phase of software development process. These change prone classes needs to be allocated more resources than other non-change prone classes because these classes needs to be tested many times. If a class is more change prone it means it needs greater effort in maintenance phase of software development. Thus if we will predict the change prone classes in beginning phases it will reduce the maintenance and testing efforts. Figure 1, 2, 3, 4 and 5 shows the ROC curve of best models of all five software.

Table 13: model evaluation result of ABRA dataset

Abra	AUC	CUTOFF POINT	SENSITIVITY	SPECIFICITY
NAÏVE	0.774	0.054	0.727	0.728
MLP	0.766	0.092	0.697	0.707
KSTAR	0.611	0.065	0.545	0.565
Bagging	0.742	0.102	0.727	0.721
RANDOM FOREST	0.642	0.104	0.576	0.592
PART	0.726	0.075	0.697	0.667
LR	0.756	0.139	0.727	0.721

Table 14: model evaluation result of ABBOT Dataset

ABBOT	AUC	CUTOFF POINT	SENSITIVITY	SPECIFICITY
NAÏVE	0.608	0.426	0.581	0.577
MLP	0.656	0.270	0.593	0.593
KSTAR	0.758	0.256	0.709	0.705
Bagging	0.755	0.245	0.674	0.676
RANDOM FOREST	0.707	0.162	0.686	0.647
PART	0.655	0.326	0.581	0.581
LR	0.675	0.266	0.593	0.589

Table 15: model evaluation result of APOLLO dataset

APOLLO	AUC	CUTOFF POINT	SENSITIVITY	SPECIFICITY
NAÏVE	0.672	0.118	0.638	0.628
MLP	0.660	0.215	0.638	0.639
KSTAR	0.779	0.112	0.725	0.723
Bagging	0.769	0.253	0.696	0.694
RANDOM FOREST	0.764	0.209	0.725	0.727
PART	0.721	0.299	0.638	0.656
LR	0.694	0.245	0.623	0.623

Table 16: model evaluation result of AVISYNC dataset

AVISYNC	AUC	CUTOFF POINT	SENSITIVITY	SPECIFICITY
NAÏVE	0.766	0.111	0.704	0.796
MLP	0.783	0.378	0.667	0.609
KSTAR	0.771	0.414	0.704	0.713
Bagging	0.760	0.689	0.630	0.630
RANDOM FOREST	0.742	0.281	0.778	0.609
PART	0.721	0.375	0.630	0.630
LR	0.717	0.326	0.741	0.609

Table 17: model evaluation result of JMETER dataset

JMETER	AUC	CUTOFF POINT	SENSITIVITY	SPECIFICITY
NAÏVE	0.722	0.108	0.672	0.672
MLP	0.762	0.610	0.732	0.722
KSTAR	0.797	0.629	0.758	0.755
Bagging	0.827	0.632	0.762	0.758
RANDOM FOREST	0.831	0.568	0.795	0.741
PART	0.790	0.654	0.708	0.736
LR	0.771	0.567	0.719	0.713

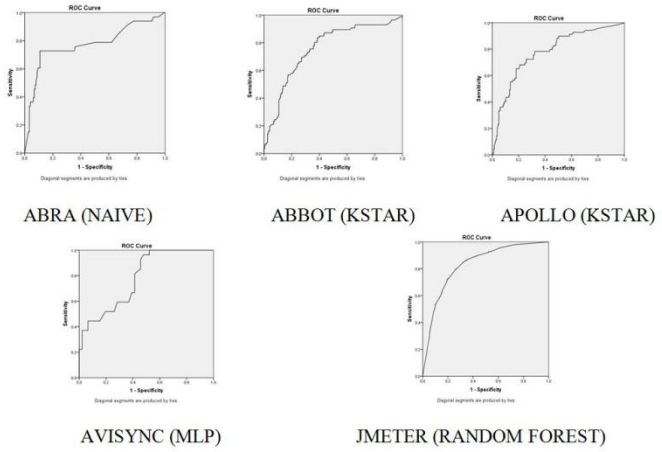


Figure 1: ROC curve for best models of each software

CONCLUSION AND FUTURE WORK

The goal of our research was to investigate the relationship between OO metrics and change proneness of a class. We also empirically analyze and compare and evaluate the performance of logistic regression and machine learning methods for predicting change prone classes. Based on studies of data sets obtained from five open source software ABRA, ABBOT , APOLLO , AVISYNC and JMETER we analyzed

the performance of predicted models using ROC analysis. Thus, the main contributions of this paper are summarized as follows: First, we performed the analysis on five freely available java software, i.e. we applied the study on five different data sets and the results are generalized and conclusive. Second, we took the changes in classes into account while predicting the change proneness of classes. Third, besides the common statistical methods, we applied machine learning methods to predict the effect of OO metrics on change proneness and evaluated these methods based on their performance.

The results established in our paper are valid for object oriented, medium and large sized systems. We plan to replicate our study to predict models based on machine learning algorithms such as genetic algorithms. In our future studies, we would like to emphasize on the economic benefit of a change proneness model.

References

[1] Han AR, Jeon S, Bae D, Hong J (2008) Behavioral dependency measurement for change proneness prediction in UML 2.0 design models, in computer software and applications 32nd annual IEEE international

[2] D'Ambros M, Lanza M, Robbes R (2009) On the relationship between change coupling and software defects in 16th working conference on reverse engineering, pp 135–144

[3] Sharafat AR, Tavildari L (2007) Change prediction in object oriented software systems: a probabilistic approach in 11th European conference on software maintenance and reengineering

[4] Chaumum MA, Kabaili H, Keller RK, Lustman F (1999) A change impact model for changeability assessment in object oriented software systems in third european conference on software maintenance and reengineering, pp 130

[5] Bieman J, Straw G, Wang H, Munger PW, Alexander RT (2003) Design patterns and change proneness: an examination of five evolving systems. In: The proceeding of 9th international software metrics symposium

[6] Tsantalis N, Chatzigeorgiou A, Stephanides G (2005) Predicting the probability of change in object oriented systems. IEEE Trans Softw Eng 31(7):601–614

[7] Singh Y, Kaur A, Malhotra R (2010) "Empirical validation of object-oriented metrics for predicting fault proneness." Softw Qual J 18(1):3–35

[8] El Emam K, Benlarbi S, Goel N, Rai SN (1999) "A validation of object-oriented metrics." In: Technical report ERB-1063, NRC

[9] Zhou Y, Leung H, Xu B (2009) Examining the potentially confounding effect of class size on the associations between object oriented metrics and change proneness. IEEE Trans Softw Eng 35(5):607–623

[10] Stone M (1974) Cross-validatory choice and assessment of statistical predictions. J R Stat Soc Ser A 36:111–114

[11] Briand L, Wust J, Daly J, Porter DV (2000) Exploring the relationships between design measures and software quality in object-oriented systems. J Syst Softw 51(3):245–273

[12] L.Erlikh, "Leveraging legacy system dollars for e-business", IT Professional, vol. 2, no. 3, pp. 17 –23, may/jun 2000.

[13] Chidamber SR, Darcy DP, Kemerer CF (1998) Managerial use of metrics for object-oriented software: an exploratory analysis. IEEE Trans Softw Eng 24(8):629–639

[14] Cartwright M, Shepperd M (2000) An empirical investigation of an object-oriented software system. IEEE Trans Softw Eng 26(8):786–796.

Analysis and Performance Evaluation of MPLS Network over Conventional IP Network

Shilpi Garg
HRIT Ghaziabad
shilpi12garg@gmail.com

Dr. Anu Chaudhary
AKGEC Ghaziabad
getanuchaudhary@yahoo.com

Abstract - **The key necessity of today's world is information gathering, processing and distribution that depend on two major technologies: Computer & Communications. There has been a merger of these two technologies giving birth to computer communication era. Multiprotocol Label Switching (MPLS) is an emerging technology and plays an important role in the next generation networks by providing Quality of service (QoS). It overcomes the limitations like excessive delays and high packet loss of IP networks by providing scalability and congestion control. The key feature of MPLS is its Traffic Engineering (TE) which is used for effectively measuring the performance of the networks and efficient utilization of network resources. MPLS provides lower network delay, efficient forwarding mechanism, scalability and predictable performance of the services which makes it more suitable for implementing real-time applications such as Voice and video. In this paper, performance of MPLS network is analyzed with conventional Internet Protocol (IP) network. The comparison is made based on the metrics such as Voice packet delay, voice packet lost probability, throughput with bandwidth and simulation time, voice packet send and received.**

Keywords: MPLS,LDP, LSP, Traffic Engineering, Forward Equivalence Class (FEC).

INTRODUCTION

MPLS is an Internet Engineering Task Force (IETF) specified frame work that provides efficient forwarding, routing and switching of traffic flow through the network. As data, video and voice networks are converging on one platform the need for MPLS is a natural progression. It is a technology for the delivery of IP services. It gives the ability to offer highly scalable, advanced IP services end-to-end with simpler configuration and management for both service providers and customers. MPLS belongs to the family of packet switching networks and was designed to overcome the limitations of IP based forwarding. In a traditional IP network each router performs an IP lookup, determines the next hop based on its routing table and forwards the packet to the next hop thereby creating a lot of overhead at each routers interface. However, MPLS on the other hand makes packet forwarding decisions which are based entirely on the contents of label without the need to examine the packet itself. MPLS works in between OSI data link layer and network layer and is summarised as Layer 2.5 networking protocol. MPLS is an innovative approach that uses label based forwarding paradigm. Labels indicate both routes and service attributes. At the ingress edge of MPLS network incoming packets are processed and labels are selected and applied. The core routers only read labels, applies appropriate services and forwards packets based on labels. The detailed analysis and classification happens only once at the ingress edge router. At the egress edge router, labels are removed and packets are forwarded to their final destination[4].

What service providers wanted was a ways to do traffic engineering without using ATM. Traditional IP networks have no means of tagging, cataloging, or monitoring the packets that cross them. MPLS technology works to solve those shortcomings of IP, placing labels on IP packets and providing the labeling function. MPLS is not designed to replace IP, it is deigned to add a set of rules to IP so that traffic can be classified, marked, and policed. Two major candidates that are in competition to become the dominant future network protocol and network architecture are Multiprotocol label switching (MPLS) and differential services (DiffServ). MPLS (Multiprotocol label switching) as a traffic-engineering tool has emerged as an elegant solution to meet the bandwidth management and service requirements for next generation Internet

Protocol (IP) based backbone networks [3]. Traditional IP networks offer little predictability of service, which is unacceptable for application such as telephony, as well as for emerging and future real time applications. One of the primary goals of traffic engineering is to enable networks to offer predictable performance.

MPLS HEADER AND ARCHITECTURE

MPLS is an emerging technology and most of the research is done in this area to evaluate how the performance networks can be improved when MPLS is added on Traditional IP networks. MPLS is a scalable, protocol-independent transport. In an MPLS network, data packets are assigned labels. Packet forwarding decisions are made solely on the contents of this label, without the need to examine the packet itself. This allows one to create end-to-end circuits across any type of transport medium, using any protocol. The primary benefit is to eliminate dependence on a particular OSI model data link layer technology, such as Asynchronous Transfer Mode (ATM), Frame Relay, Synchronous Optical Networking (SONET) or Ethernet, and eliminate the need for multiple layer-2 networks to satisfy different types of traffic. MPLS belongs to the family of packet-switched networks. Multiprotocol label switching (MPLS) is an extension to the existing Internet Protocol (IP) architecture. By adding new capabilities to the IP architecture, MPLS enables support of new features and applications. In MPLS short fixed-length labels are assigned to packets at the edge of the MPLS domain and these pre assigned labels are used rather then the original packet headers to forward packets on pre-routed paths through the MPLS network [2].

Multi Protocol Label Switching (MPLS) provides a framework for doing more flexible traffic engineering via its explicit routing capability. MPLS routing models with two different objectives that utilize MPLS explicit routing are presented and discussed. The objectives of this paper were to minimize the network cost and maximize the minimum residual link capacity. The model that maximizes the minimum residual link capacity is found to perform substantially better, in terms of network throughput and packet loss.

MPLS Header: MPLS operates by defining a label inside MPLS "Shim header" that is placed on the packet between layer 2 and layer-3 headers. The 32-bit MPLS header is organized as in Fig.1.

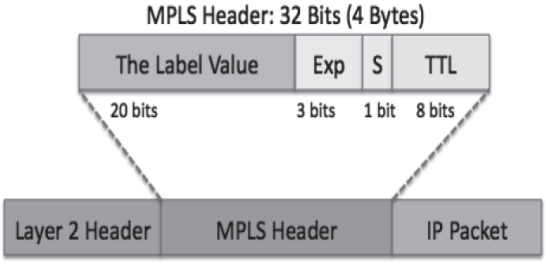


Figure 1. MPLS Header.

The header consists of 20-bit Label which is used to identify the Label switched path (LSP) to which the packet belongs in the MPLS domain. The labels on the packets are established by using Forwarding equivalency class (FEC). Following the Label field there are 3 bits EXP field which is called as Traffic class field (TC field) this is used for Quality of Service (QoS) related functions. Next field is called stack field which is 1 bit field and this is used to indicate bottom of label stack. The tail consist 8-bit TTL (Time to Live) field which had similar function that of TTL field in IP header.

Label: The label is a part of MPLS header called shim. It is placed between the data-link and IP headers. It identifies the path a packet should traverse. The shim is composed of 32 bits out of which 20 bits are allocated to the label also called label stack, 3-bits are experimental bits often used for specifying class of service. One bit is reserved for bottom of stack bit and is set if no label follows. 8-bits are used for time-to-live (TTL) used in the same way like IP.

- **Label forwarding information base:** A table created by a label switch-capable device (LSR) that indicates where and how to forward frames with specific label values.
- **LSP:** It refers to Label Switched Path. It is a unidirectional tunnel between a pair of routers routed across MPLS network.
- **LER:** It refers to Label Edge Router/Ingress router. It is a router that first encapsulates the packet inside an MPLS LSP and also makes initial path selection.
- **LSR:** It refers to Label Switched Router. A router which only does MPLS switching in the middle of an LSP.
- **Egress Router**: The final router at the end of LSP which removes the label.
- **Label switched:** When an LSR makes forwarding decision based upon the presence of a label in the frame/cell.
- **Label switch controller (LSC):** An LSR that communicates with an ATM switch to provide and provision label information within the switch.
- **Label distribution protocol (LDP):** It is one of the primary signalling protocols for distributing labels in MPLS network. It is a set of procedures and messages by which Label Switched routers (LSR) establish Label Switched Path (LSP) through a network by mapping network layer routing information directly to data link layer switched paths. By means of LDP LSR can collect , distribute and release label binding information to other LSRs in the MPLS network thus enabling hop-by-hop delivery of packets in the network along routed paths.

- **FEC:** It refers to forwarding equivalence class and is a group of IP packets that are forwarded in the same way. Packets within an FEC are equivalent in terms of forwarding such as, same destination, same path and same class of service. A LSP is assigned to each FEC that is defined using IP interior routing protocols (OSPF).

MPLS Architecture: The MPLS Architecture is divided between the Control Plane and the Data or Forwarding Plane. The components and processes critical operation of MPLS network in the Forwarding Plane Fig 2.

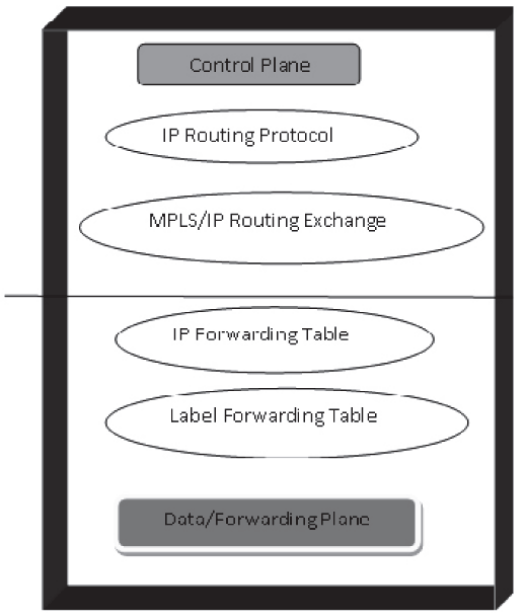


Figure 2. MPLS Architecture.

The MPLS architecture describes the mechanisms to perform label switching, which combines the benefits of packet forwarding based on Layer 2 switching with the benefits of Layer 3 routing. Similar to Layer 2 networks (for example, Frame Relay or ATM), MPLS assigns labels to packets for transport across packet- or cell-based networks. MPLS is also known as 2.5 layer networks which combines the feature of Packet switching and circuit switching. The forwarding mechanism throughout the network is label swapping, in which units of data (for example, a packet or a cell) carry a short, fixed-length label that tells communicating nodes along the packets path (FEC) how to process and forward the data. Based on switching between different architectures MPLS domain architecture is split into two separate components: the forwarding component (also called the data plane) and the control component (also called the control plane). The forwarding component uses a label-forwarding database maintained by a label switch to perform the forwarding of data packets based on labels carried by packets. The control
component is responsible for creating and maintaining label forwarding information (referred to as bindings) among a group of interconnected label switches. Every MPLS node must run one or more IP routing protocols (or rely on static routing) to exchange IP routing information with other MPLS nodes in the network. In this sense, every MPLS node (including ATM
switches) is an IP router on the control plane.

MPLS Operation

Step-1: The network automatically builds routing tables as MPLS capable router participate in interior gateway protocols (OSPF, IS-IS) throughout the network. Label distribution protocol (LDP) establishes label to destination network mappings. Label distribution protocol (LDP) uses the routing topology in the tables to establish label values between the adjacent devices. This operation creates Label Switching Paths (LSP) pre-configured maps between destination end points.

Step-2: A packet enters the ingress edge label switching router (LSR) where it is processed to determine which layer-3 service it requires, such as quality of service (QoS) and bandwidth management. The edge LSR selects and applies a label to the packet header and forwards it.

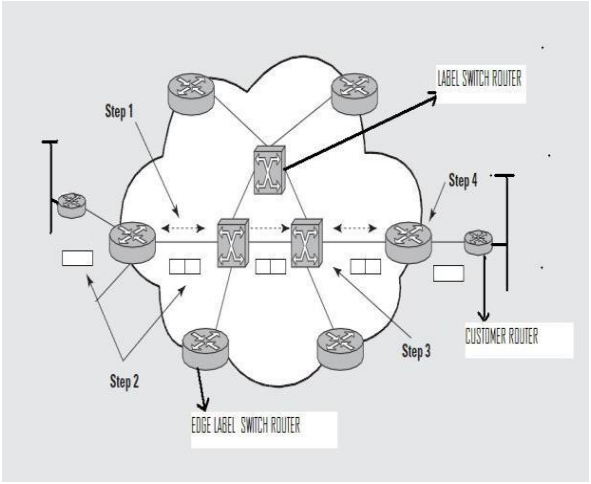


Figure 3

Step-3: The LSR reads the label on each packet replaces it with new one as listed in the table and forwards the packet.

Step-4: The Egress Edge Router strips the label, reads the packet header and forwards it to its final destination.

MPLS Domain

In the MPLS domain is described as "a contiguous set of nodes which operate MPLS routing and forwarding". This domain is typically managed and controlled by one administration. The MPLS domain can be divided into MPLS core and MPLS edge. The core consists of nodes neighboring only to MPLS capable nodes, while the edge consists of nodes neighboring both MPLS capable and incapable nodes. The MPLS offers many advantages over IP routing nodes in the MPLS domain are often called LSRs (Label Switch Routers). The nodes in the core are called transit LSRs and the nodes

in the MPLS edge are called LERs (Label Edge Routers). If a LER is the first node in the path for a packet traveling through the MPLS domain this node is called the ingress LER, if it is the last node in a path it's called the egress LER.

LABEL SWITCHING BENEFITS

- **Speed and delay-** Traditional IP – based forwarding is too slow to handle the large traffic loads in the Internet. Label switching is much faster because the label value that is placed in an incoming packet header is used to access the forwarding table at the router; that is, the label is used to index into table. This look up requires only one access to the table but in traditional routing table access might require several thousand lookups. Hence in MPLS packet is sent through the network much more quickly than with the traditional IP forwarding operation.
- **More scalability-** Scalability refers to the ability or inability of a system, in the case of Internet to accommodate a large and growing number of Internet users. Label Switching offers solutions to this rapid growth and large networks by allowing a large number of IP address to be associated with one or a few labels. This approach reduces the size of address (actually label) table and enables a router to support more users.
- **Simplicity-** MPLS is basically a forwarding protocol (or set of protocols). It is elegantly simple: forward a packet based on its label. How that label is ascertained is quite another matter.
- **Resource consumption-** Label switching networks do not need a lot of network's resources to execute the control mechanism to establish label switching paths for users' traffic.
- **Standards based-** MPLS is an Internet Engineering Task Force (IETF) standard available to all industry vendors to ensure interoperability in multi vendor networks.

SIMULATION RESULTS

1. IP Network without Traffic Engineering:

In the IP network traffic uses the shortest path (2_3_6_7_8) to forward traffic, which causes this path to overlap at the link from node 3 – 6 thus causing congestion on this link. The traffic from (2_3_6_7_8) exceeds the capacity of the shortest path, while a longer path between (2_3_4_5_7_8) is underutilized. When the path (2_3_6_7_8) of the network is busy, congestion is occurring within the network. Packet from link (3– 6) get dropped and delayed as buffer overflow because the resources in the network cannot meet all traffic demands.

2. MPLS Network with Traffic Engineering:

In MPLS an LSP is set up when a 'label request message' propagates from the ingress (node2) to the egress LSR (node8). When the requested path satisfies the constraints and labels are
allocated, then a "label-mapping message" propagates back from the engress LSR (node 8) to the ingress LSR (node 2) carrying details of the final traffic parameter reserved for the LSP. When LSP is setup, MPLS traffic engineering is applied to switch the traffic flow through an explicit rout (2_3_4_5_7_8), hence under-utilized path is also used for forwarding the traffic. Throughput at destination node is shown in figure4 and figure5.

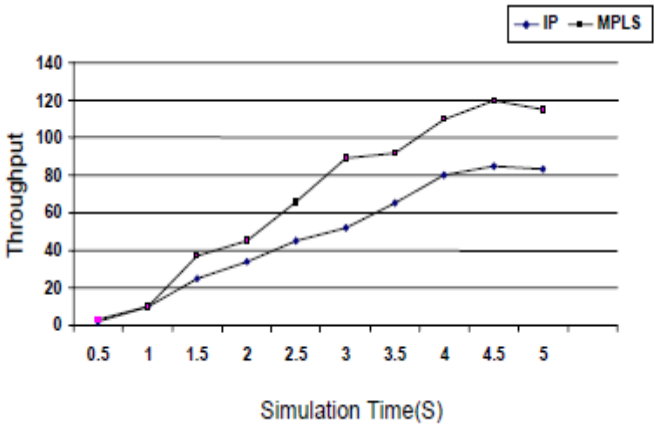


Figure4. Throughput V/s Simulation Time

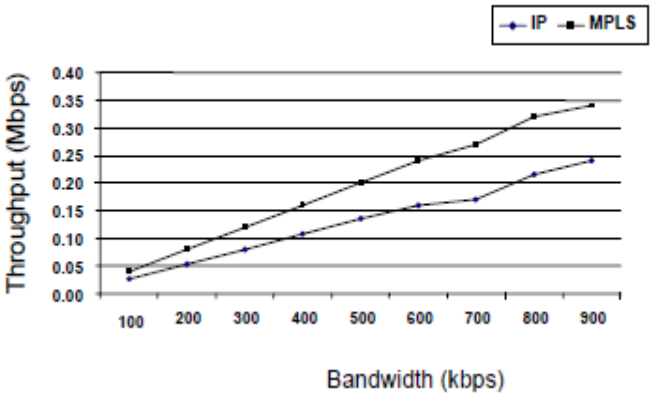


Figure5. Throughput V/s Bandwidth

CONCLUSION

An IP-based network is connectionless, MPLS based network defines definite paths for network traffic based on some Quality of Service level. Multi-Protocol Label Switching is helpful in
managing multimedia traffic when some links or paths are under and/or over utilized. Traffic engineering is the main strength of MPLS. The simulation study is an effort to quantitatively illustrate the benefit of using MPLS in implementing multimedia applications. Through simulation results and analysis, it is clear that

with proper MPLS Traffic Engineering applied to the network, the performance of the network is significantly improved.

References

[1] Anu Chaudhary, "A Study and Simulation of VoIP in MPLS Network" AKGEC INTERNATIONAL JOURNAL OF TECHNOLOGY, Vol. 5, No. 2

[2]. Anu Chaudhary, Satya Prakash Singh, "Performance Evaluation of VoIP in MPLS network using NS-2", INTERNATONAL JOURNAL OF COMPUTERS AND TECHNOLOGY, Vol. 13, No. 9, June 2014, ISSN 2277-3061.

[3]. Mahesh Kr. Porwal, Anjulata Yadav, S. V. Charhate, "Multimedia Traffic Analysis of MPLS and Non MPLS Network ", International Journal of Computer Science and Applications, Vol. 1, No. 2, August 2008, ISSN 0974-1003.

[4]. Rashed Q. Shawl, Rukhsana Thaker, Jasvinder Singh, "A Review: Multi Protocol Label Switching (MPLS)", International Journal of Engineering Research and Applications, ISSN: 2248-9622, Vol. 4, Issue 1(Version 2), January 2014, PP. 66-70.

[5] A. Ghanwani. "Traffic Engineering Standards in IP Networks Using MPLS" IEEE Coniniunications Magazinc, vol. 37, no. 12, pp. 49- 53. December – 1999.

[6] A. Viswanathan, R. Callon, "Multiprotocol Label switching Architecture" RFC 3031.

[7] D.O. Awduche,"MPLS and Traffic Engineering in IP networks", IEEE Communication Magazine, pp.42-47, December – 1999.

[8] D. Awduche, "Requirements for Traffic Engineering Over MPLS", RFC 2702, September – 1999.

[9] D. Awduche, J. Agogbua, M. O'Dell, "Requirements for Traffic Engineering over MPLS (RFC 2702)" http://rfc-2702.rfc-list.net/rfc-2702.htm September - 1999.

[10] R. Callon at al, "A Framework for MPLS", Internet Draft, September – 1999.

[11] UYLESS BLACK – MPLS and Label Switching Network.

[12] S. Smith, ―Introduction to MPLS‖, 2003, cisco press article.

[13] Y.Cheng, ―MPLS‖, 2003, white paper.

[14] H. Tamura , S. Nakazawa, K. Kawhara, Y.Oie, ―Performance Analysis for QoS Provisioning in MPLS networks‖, 2004, Kluwer academic Publisher.

[15] D. Bella, R. Sperber, ―MPLS –TP the new technology for packet transport networks‖ , White paper.

[16] MPLS networks Operations guide log reference by Juniper Networks, 2010.

[17] Cisco press article on MPLS , www.cisco.com

[18] Cisco Systems Inc.: Cisco Carrier Routing System (2006). http://www.cisco.com

[19] Alawieh, B. (2007). Efficient Delivery of Voice Services over MPLS Internet Infrastructure. IEEE, pp 483-486.

[20] Amer Alkayyal, Stelios Sotiriadis, Eleana simakopoulou, Nik Bessis, "Optimizing Voice over Multi-Protocol Label Switching (VoMPLS)", Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing IEEE, 2013.

[21] Antoine B. Bagula, "Hybrid routing in next generation IP networks", Computer Communications 29 (2006) 879–892, Elsevier.

[22] Alvarez, S. (2003). QoS in MPLS Networks. Cisco Systems.

[23] Chris Metz Cisco Systems, "Layer2 over IP/MPLS", pp 77-82, IEEE Internet computing, 2001.

[24] Gaeil Ahn and Woojik Chun ,"Design and Implementation of MPLS Network Simulator Supporting LDP and CR-LDP",IEEE Transactions on Communications, pp441-446 2000.

[25] Michael F. Finneran , "Designing MPLS Networks for VoIP", dBrn Associates, Inc., 2006.

[26] Robert Suryasaputra, Alexander A. Kist and Richard J. Harrist, "Verification of MPLS Traffic Engineering Techniques", IEEE Transactions on communication, pp 190-195, 2005.

A Review Paper on Data Mining Techniques and its Application

Mohammad Aamir
Ajay Kumar Garg Engineering College, Ghaziabad, India
aamirkhan1990@gmail.com

Prashant Kamal Mishra
Ajay Kumar Garg Engineering College, Ghaziabad, India
prashantkamal9@gmail.com

Shivangi Garg
Ajay Kumar Garg Engineering College, Ghaziabad, India
g.shivangi07@gmail.com

***Abstract*- Data mining is a modern technology to extracts the knowledge or information from a vast quantum of data which stores in multifarious diverse data base. Data Mining is the analysis of observational datasets to perceive the relationships and to encapsulate the data in ways that are both comprehensive and knowledgeable. Data mining is a type of sorting technique which is actually used to extricate hidden patterns from vast databases. This paper provides an insight on the techniques of data mining. These techniques include association, classification, clustering, summarization, regression and prediction. The paper also attempts to carry out a formal review of the application of data mining such as banking and finance, cloud computing, earthquake prediction, telecommunication and agriculture that are being widely used.**

Keywords: Data Mining, Knowledge Discovery Database, Association, Prediction, Clustering, Data Mining Application

INTRODUCTION

Data mining is the process of unearthing meaningful new relationship, patterns and trends by filtering through large volume of data stored in repositories by using pattern recognition techniques as well as mathematical and statistical approaches. For superior decision making, large repositories are made so that the data collected from divergent resources require proper mechanism to extricate knowledge from the databases. Data mining sometimes also called as knowledge discovery in databases (KDD) [2] and is a process to excerpt information and patterns from data in large databases. Data can be in the form of numbers, facts or text that can be processed by a computer. Data mining is the process of examining data from different panorama and determines its relationship, associations or patterns among all collected data and summarizing it into some kind of utilitarian information. Data mining software is a scientific tool for analyzing data. It entitles users to analyze data from different dimensions or angles, classify it and abridge the relationships so identified. With the advent of information technology in various fields the vast amount of data storage has increased in various ways like storing documents, records, sound recordings, images, scientific data, videos, and many new data formats. Data mining and knowledge discovery applications have important magnitude in decision making and it has become a requisite component in various organizations and fields. The fields of data mining has expanded rapidly in the areas of Statistics, Pattern Reorganization, Artificial Intelligence , Databases, Machine Learning and Computation capabilities etc.[4]

In the real world, enormous amount of data are accessible in education, medical, industry and many other fields. Such data may provide knowledge and information for decision making. For example, you

can find out sales data in shopping database or drop out student in any university. Data can be scrutinized, abridged and understand to meet the challenges. Data mining is a powerful concept for data survey and process of discovering interesting pattern from the vast amount of data which is stored in various databases such as data warehouse, World Wide Web and external sources. [3] The goals of data mining are fast atonement of data or information, to identify hidden patterns and those patterns which are not explored previously and knowledge Discovery from the databases are to slacken the level of complexity and time saving.[6]

KDD is an iterative process consisting of following steps [1]

1) ***Data cleaning***: It can also be termed as data scrubbing. It is a phase wherein noisy data and extraneous data are removed from the collection.

2) ***Data integration***: In this stage different data sources that are diverse can be amalgamated in a common source.

3) ***Data selection***: In this phase the data pertinent to the analysis is assured and redeem from the data collection.

4) ***Data transformation***: In this phase the selected data is transformed into appropriate forms for the mining procedure.

5) ***Data mining (pattern evaluation)***: This is a vital phase wherein proficient techniques are applied to extract patterns that are potentially useful. In this phase rigorously enthralling patterns that are representing knowledge are recognized with respect to the given measures.

6) ***Knowledge representation***: This is the final phase in which the unearth knowledge is visually represented to the user. This is a requisite step which uses techniques of visualization to help users comprehend and interpret the data mining results.

DATA MINING TECHNIQUES

There are a variety of major data mining techniques that have been developed and used in data mining projects in recent times including classification, regression, prediction, clustering, summarization and association which are used for knowledge discovery from database.[7]

2.1 Classification:

Classification technique is based on the supervised learning (i.e. desired output is known for a given input) by providing training to the multifarious data set. One can use classification technique to set up an idea of the genre of customer, object or item by describing diverse attributes to distinguish a particular class. For example, we can apply the classification rule on the past record of the student who left from the university and evaluate them. Using these classification rule (IF-Then) we can easily identify the performance of the student. [5]

2.2 Regression:

Regression technique seeks to determine the values of parameters for a function that causes the function to best fit in a set of data observations that you provide. Regression can be adapted as a measure for prediction. In the regression techniques end values are known. For example, you can predict the child behaviour based on his/her family history. [2]

2.3 Prediction:

It is one of the data mining techniques that unearth the relationship between independent variables and also the association between dependent and independent variables. Prediction is a broad topic which can also predict the malfunctioning of components parts of machinery can also recognize fraud and can even predict company's profits. Thus by studying past events or occurrences, one can make a prediction regarding to an event. [4]

2.4 Clustering:

Clustering is an accumulation of homogenous data objects into one cluster and heterogeneous data object in another cluster. It is a way of finding resemblance between data according to their characteristic. This technique is based on the unsupervised learning (i.e. desired output is not known for a given input). City planning, pattern

recognition and image processing are some examples of clustering. [3]

2.5 Summarization:

Summarization is an abstraction of data. It is a set of pertinent task that are used to get performed and gives an overview of data. For example, long distance race can be summarized in terms of total hours, minutes, and seconds. [1]

2.6 Association:

Association is probably the better known and most accustomed and straight forward data mining technique. Here, you make a simple connection between two or more items, often of the same type to discern the patterns. Example: Association technique is used in marketing analysis to recognize items which are often purchased within the same transactions. [2]

APPLICATION OF DATA MINING

Data mining technologies are adapted in various fields because of fast ingress of data and significant information from a vast amount of data. Data mining application can be seen in the fields of earthquake prediction, cloud computing, telecommunication, agriculture, banking and finance. Some of the prominent applications of data mining are listed below: [4]

3.1 Data Mining in Earthquake Prediction:

Data Mining Techniques are used to predict the earthquake from the satellite maps. Earthquake is the unexpected movement of the Earth's crust caused by the instantaneous release of stress accumulated along a geologic fault in the interior. There are two primary categories of earthquake predictions: forecasts (months to years in advance) and short-term predictions (hours or days in advance). [8]

3.2 Data Mining in Cloud Computing:

Data mining techniques are used in cloud computing to provide efficient, reliable and secure services to their users. With the implementation of data mining techniques in Cloud computing it will now allow the users to retrieve significant information from virtually integrated data warehouse that diminishes the costs of infrastructure and storage. [10]

3.3 Data Mining in Telecommunication:

The telecommunication industry which is working in a highly competitive zone and rapidly changing environment implements the data mining technology due to large amount of data and a very large number of customers to improve its marketing efforts, fraud detection, and management of telecommunication networks.[6]

3.4 Data Mining in Agriculture:

Data mining is fast emerging in agriculture field for crop yielding analysis with respect to four criterions namely production, year, rainfall, and area of sowing. Prediction of yield remains to be a very important agricultural problem that is to be solved based on the available data. The issue of yield prediction can be solved by employing Data Mining techniques such as Artificial Neural Network (ANN), K-Means and support vector machine (SVM).[9]

3.5 Data Mining in Banking and Finance:

Data mining has been widely used in the banking and financial markets. In the banking sector, data mining is used for the detection of fraudulent credit card usage patterns, to determine risk, and to examine the trends. In the financial markets data mining technique such as neural networks is used in price prediction, stock forecasting and so on. [11]

CONCLUSION

On the basis of the above review, this paper attempts to deal with diverse classification techniques that are used in data mining and a discussion on each of them. Each of these techniques can be used in various situations depending upon where one tends to be fruitful while the other may not be and vice-versa. When a new data set is available these classification techniques display how data can be determined and grouped. Each technique has got its own positives and negatives as emphasised in the paper. Thus based on the required conditions any one can select a technique to be used for data mining. Data mining is a technology that proffers great promise in helping organizations to uncoil

patterns hidden in their data that can be used to predict the behaviour of customers, products and processes. The paper also mentions a few applications where data mining technology can be applied to gain fruitful results. Thus from a vital perspective there exist a need to navigate the expeditiously growing universe of digital data which heavily depends on the ability to adequately manage and mine the raw data.

References

[1] B.N. Lakshmi, et al. "A Conceptual Overview of Data Mining" in the Proceedings of the National Conference on Innovations in Emerging Technology, Page(s): 27 - 32, 2011.

[2] Smita, et al. "use of data mining in various fields: A survey paper" in the Proceedings of the IOSR Journal of Computer Engineering (IOSR-JCE) Page(s): 18-21, 2014

[3] J. Han and M. Kamber. "Data Mining, Concepts and Techniques", Morgan Kaufmann, 2000

[4] Aakanksha Bhatnagar, Shweta P. Jadye, Madan Mohan Nagar" Data Mining Techniques & Distinct Applications: A Literature Review" International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 9, November-2012

[5] Nikita Jain, Vishal Srivastava "DATA MINING TECHNIQUES: A SURVEY PAPER" IJRET: International Journal of Research in Engineering and Technology, Volume: 02 Issue: 11 | Nov-2013,

[6] Dr. M.H.Dunham, "Data Mining, Introductory and Advanced Topics", Prentice Hall, 2002

[7] David L Olson, Dursun Delen "Advance data minig techniques" springer 2008

[8] G. V. Otari, Dr. R. V. Kulkarni, "A Review of Application of Data Mining in Earthquake Prediction" G. V. Otari et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (2) , 2012,3570-3574

[9] D Ramesh, B Vishnu Vardhan, "Data Mining Techniques and Applications to Agricultural Yield Data" International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 9, September 2013

[10] Ruxandra-Ştefania PETRE, "Data mining in Cloud Computing" Database Systems Journal vol. III, no. 3/2012

[11] Neelamadhab Padhy, Dr. Pragnyaban Mishra and Rasmita Panigrahi, "The Survey of Data Mining Applications and Feature Scope, International Journal of Computer Science, Engineering and Information Technology (IJCSEIT)", vol.2, no.3, June.

Theory on Age Invariant Face Recognition System

Aman Kumar
Golgotia's College Of Engineering And Technology,Greater Noida
varmaaman.mhb@gmail.com

***Abstract*– In modern times the age variation is a common problem in detecting the face for any security system & other purpose. Face recognition is identification of humans by unique characteristics of the faces and is one of the several types of existing biometrics systems. Face recognition is a passive, non-passive method for verifying the identity of a person.This paper focuses on all the techniques that are able to match faces of a person irrespective of their age. In this case we prefer two models, first is the generative model that was used in the past and second is the discriminative model that is better in performance compared to generative model.The discriminative approach addresses the face aging problem in a more direct way without relying on generative aging model.The discriminative model is used many algorithms like, SIFT (Scale Invariant Feature Transform), Neural network, PCA (Principle Component Analysis), MFDA (Multi Feature Discriminant Analysis) and others. It has many application like Missing person identification, passport photo verification, homeland security, surveillance.It used two data base module like MORPH and FG-NET for image matching.**

Keywords: Biometrics, face recognition, Discriminative Approach, Generative Approach

INTRODUCTION

The automated face recognition is the challenging problem to detect the face in many psychological states.

The age invariant face recognition system first takes the pattern of the particular face and then used the various algorithms to processing the pattern and then we match the image from the library. This type of face recognition is used to find the missing person, identification of passport and id proof. In case of attribute there can be two types (1) large Intra subject variation and (2) large inter user similarity. In case of large intra subject variation can be have the pose, illumination, expression**,** and aging. There is the figure of theis type of variation

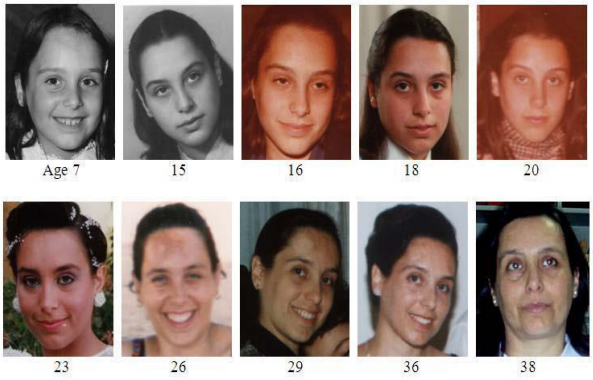


Figure 1. Example images showing intra-subject variations (e.g., pose, illumination expression, and aging) for one of the subjects in the FG-NET database

Some of the part like GOP(Gradient Orientation Pyramid) is used to feature representation ,combined with SVM(Support Vector Machine) is used to verifying the faces across age progression .both SIFT(Scale Invariant Feature Transform) and MLBP(Multi Local Binary Pattern) is used to image representation . this variation is matched on two data base domain MORPH and FG-NET .

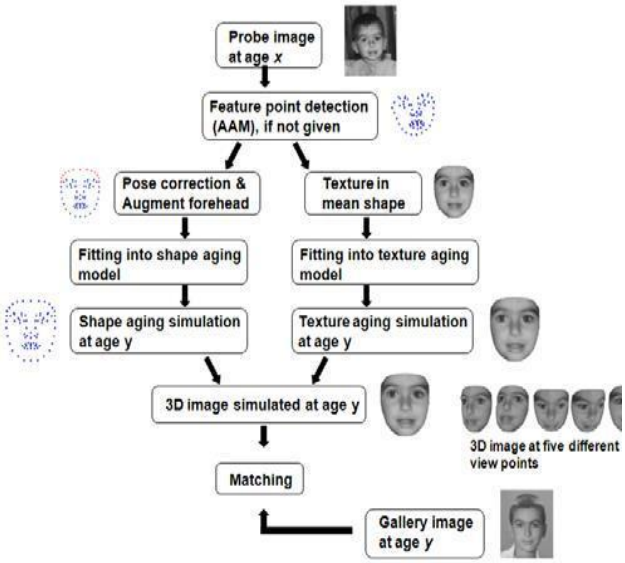


Figure 2. Schematic of the aging simulation process from age x to age y

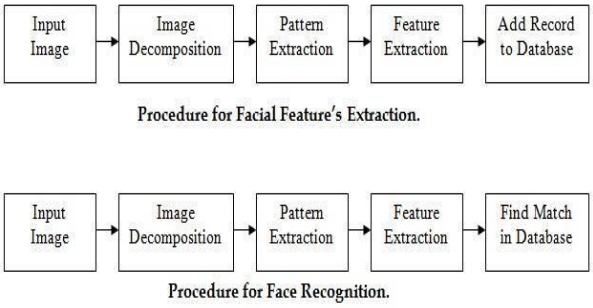


Figure 3: Structure of face recognition system

2 (a) History of Face Recognition System:

The first work on the automated facial recognition system is done by woodv Bledsoe, Helen chanwalf & Charles bison in 1964-65 . The subject of face recognition is as old as computer vision both because of the practical importance of topics and theories perhaps the most famous early example of a face.

FACE REGONITION SYSTEM

FACE recognition is an active field of research and has increased significantly since the early 1990s. This is mainly due to the fact that government agencies and businesses have realized. [1][2]

The vast range of commercial applications that one can provide with face recognition. These applications fall in many areas, such as entertainment, smart cards, information security and law enforcement.

For face recognition systems there are many contributing factors that can lead to these two errors and the most important ones are:

M. Variations in lighting conditions.
N. Variations in face pose.
O. Variations in facial expressions.
P. Total or partial occlusion of a face

Other factors that can also significantly affect the recognition accuracy and that should also be considered are:

a. Quality of face images.

b. Image resolution and face area size in images.

c. Colour information in face images.

recognition system is due to kononen who demonstrated that a simple neural network perform , take face recognition for aligned and normalized face image . The type of neural network be employed computed a face description by approximating the eigen vector of face images autocorrelation matrix theis eigenvector are new know Eigen faces .

Kirby & sirovich (1989) later introduced an algebraic manipulation which made it easy to directly calculation the Eigen faces and showed that fewer than 100 were required to accurately code carefully aligned & normalized face images.

Furk & pentland (1991) then demonstrated that me residual error when coding using the Eigen faces could be used both to detect face in clustered natural imaginary and to determine precise location and scale of face in an image.

Some example of Face recognition software are :-

Digicam (KDE) , iPhoto (apple), opencv(open sourse) , Photoshop Elements(adobe system) , Picasa(Google), picture motion (sony), window live photo gallery (microsoft) .

3. GENERATIVE MODEL

The previous model or generating model have simple stages like load input image & perform normal mathematical operation on image .it have less output status to comparison to the discriminative model.[3][4]

It contain the 79% accuracy of correct faces. The reason for the low performance of the generating model compared to the proposed discriminative model is that the automatic landmark point of detector, that is used for generating model.

Drawback of Generative model:

It contain following drawback.

(a) To select the face we observed many type of face expression like happy, angry, simple and so own. Then manipulation of that expression is difficult in generating model.

(b) If you have detect the back front of images then you generated problem because you can not detect the correct expression.

(c) Generative model have low frequency to match the image from MORPH and FG-NET data base module.

Figure 4 : various expression on face

4-Discriminative model (modern approach):

Some representation model like GOP (Gradient Orientation Pyramid) is used to feature represent & SVM (Support Vector Machine) for verifying faces across age progression.[5][6].

It contain following parameter

a) **Starting module**
b) Detecting facial feature
c) Component of discriminative model
d) PCA(Principle Component Analysis)
e) SIFT(Scale Invariant Feature Transform)
[1] MLBP(Multi Local Binary Pattern)
[2] Data base module(MORPH & FG-NET)
[3] System design and implementation
[4] Learning parameter (Neural Network) & testing parameter
[5] Experimental result
[6] Future work
[7] References

4(a) Starting Module: It is the basic module to implement the age variation face recognition system.it prefer the basic implementation of this system.it contain the following module
4(a) A1: Insert trained image

A2: Pre-processing for train image

A3: illumination normalization

A4: Face normalization / pose normalization

A5: Per-ocular region normalization

A6: Feature extraction.

The starting module also contains the training set. Training images have various illumination of the various person.[7][8]

The individual person subspace can be represented by matrix A1, A2……Ak, where each column in A1 is training sample from class.

There is the description of A1.

A1: Insert trained image: it is the basic module to implement the face recognition. In

this case we insert the input image for next processing step.

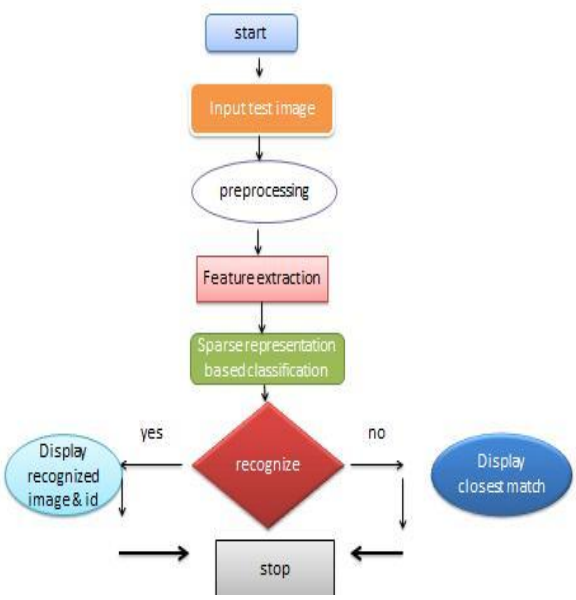


Figure 5: Inserted trained image

A2: Pre-processing for trained image:

To achieve good performance under illumination changes, methods based on normalization or illumination invariant description have been used. Several general purpose pre-processing algorithms have been used extensively for face illumination normalization. It commonly used is four segments approach based on histogram equalization algorithms.[9][10]

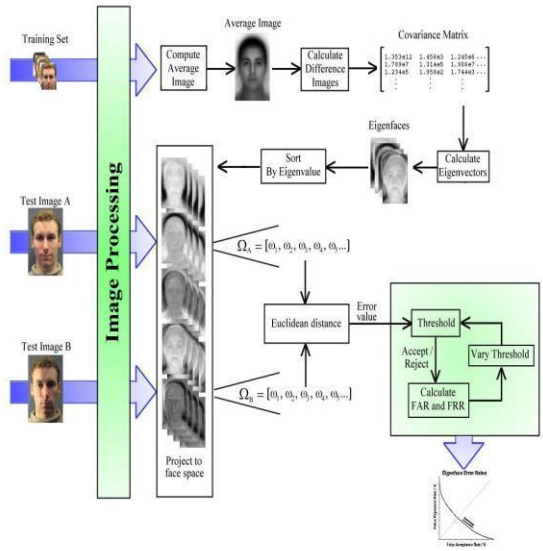


Figure: 6 Pre-processing of image

A3: illumination normalization:

It is achieved using the four segment approach.
The individual illumination normalization is done using histogram equalization.Pixel averaging is used to remove to remove noise produced at joining edges.It contains the gamma intensity correction:
$F(l(x,y))= l(x,y)^{1/\gamma}$

Original image $\gamma=2.2$

Figure 7: Gamma intensity correction

A4: Face normalization / pose normalization:

For the test image, the AAM (Active Appearance Models) is used to obtain the coordinate of vertices. These coordinate can be defined as the vertex location of the mesh that describes the shape of the facial components.

A5: Per ocular region normalization:

After face normalization or pose correction has been performed the eyes are already well aligned on the image and hence we perform crop to obtain the per ocular region containing both eyes.

A6: Feature extraction:

To perform feature extraction the PCA (Principle Component Analysis) is the most

commonly used method.in PCA each training image is projected on the face space and expressed in term of Eigen face coefficient.[11]

2 + =−1 ∟2 ⅃ + W2 +−1 + W2 −1 W(t)0 = (1; 1; 1; 1; 1) W(t)1 = (-1;-1;-1; 1; 1)

W(t)2 = (-1;-1; 1; 1;-1) W(t)3 = (1; 1;-1; 1;-1)

W(t)4 = (1;-1; 1; 1;-1).

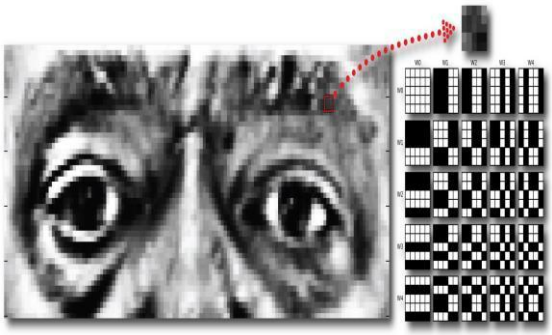


Figure 8 Feature extraction

4(b) Detecting Facial Feature:

In this detecting feature we first provide image pre-processing that contain the common feature like load image, convert to grey scale , resize the input image to 64px and 256px for detailed and coarse then make the histogram.[12][13]

Then localize the left eye, right eye, mouth, nose , eye canter mouth centre, nose centre and other heuristic . in this cases each contain the algorithms to implement the image.

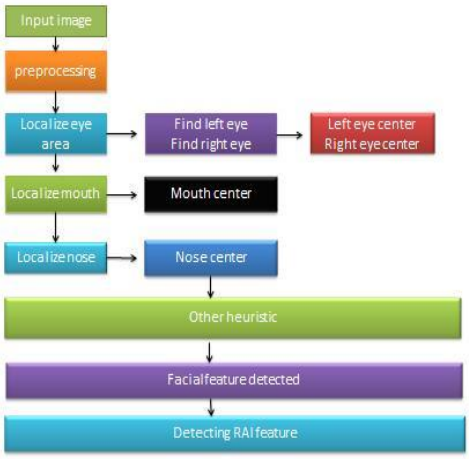


Figure 9: Block Diagram of Facial Detection System.

4(c) Component of Discriminative model:

It contain the two component

4(c) 1: DSLF (Density Sampled Local Description)

4(c):2: MFDA (Multi Feature Discriminant Analysis)

4(c) 1: DSLF (Density Sampled Local Description):

To comparison the global appearance feature to the local feature is more affective in representing face image.At diverse scale & orientation and robust to diametric distortion and illumination variation hence we contain local feature.[14].In this case we divide image into set of over lapping patches & then apply select local image descriptor to each patch.

Example:

Given a face image of size H*W

Then it divide into a set of s*s overlapping patches that overlap by a pixel the no. of horizontal (m) and vertical (n) patches are.[15][16]

N= (W-S)/r+1…… 1

M= (H-S)/r+1……..2

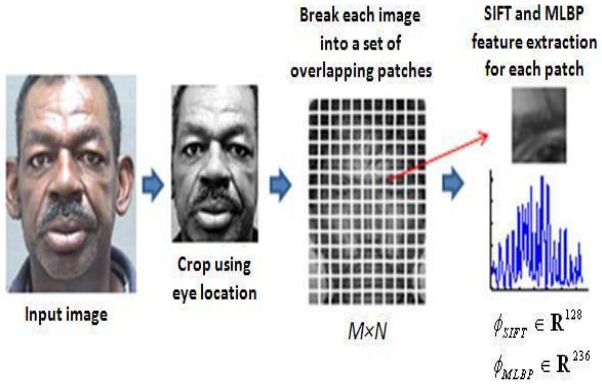


Figure 10: illustration of local feature representation of a face image.

4(c) 2: MFDA (Multi Feature Discriminant analysis)

It is the most popular discriminant analysis techniques for face recognition.

It used LDA based method. The LDA uses the within class scatter matrix to measure the class sepratibility. It matrix defined as.

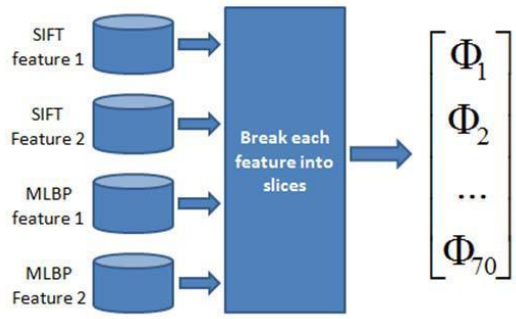


Figure 11: Break the local feature into slices there are total 70 slices for each face image

The possible way to overcome the above problems is to use random sampling techniques to improve the performance of LDA (Linear Discriminant Analysis). [17] LDA has been shown to be very successful in face recognition. However, if we directly use the LDA for discriminant analysis for age invariant face recognition, we will encounter the following problems. First, the high dimensionality of the input feature vector space in conjunction with relatively small size of the aging training set would drastically reduce the accuracy and stability of Sw.

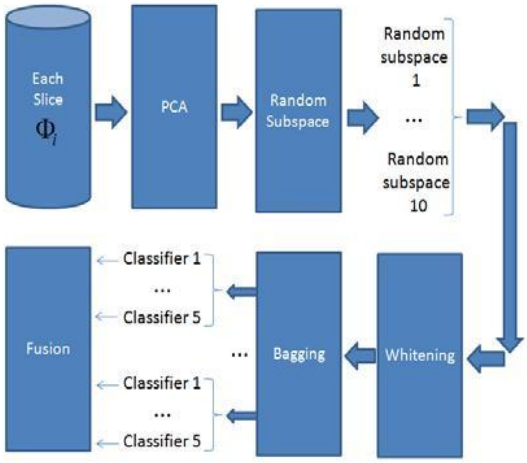


Figure12: Block diagram of MFDA (Multi Feature Discriminant Analysis)

4(d) PCA (Principle Component Analysis)

It is used to large data set .this shows also some parameter (gender, race, height, width). It used to handle the large no. of correlated variable in single dimension space. PCA (principle component analysis) rotates the original data space such that axes of new coordinate system point into the direction of highest variance of the data.[18] It used also the dimensionality reduction low variance can often be assumed to represent undesired background noise .the dimensionality of the data can therefore can be reduced. .

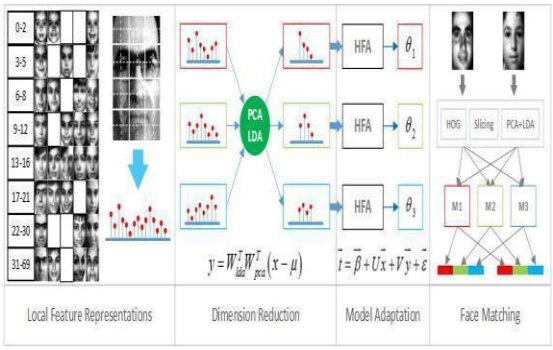


Figure: 13 PCA& LDA implementation

4(e) SIFT (Scale Invariant Feature Transform):

It is the algorithms in computer vision to detect and describe local feature in image. The algorithm was published by the David Lowe in 1992.It used in field of object recognition, face recognition, robotic mapping, gesture recognition, video tracking.[19][2]

SIFT (Scale Invariant Feature Transform) key point of objects are first extracted from a set of reference image and store a data base. An object is recognize in a new image by individually comparing each feature from the new image to this data base and finding candidate matching feature based on Euclidean distance of their feature vector. It used for feature matching and indexing.

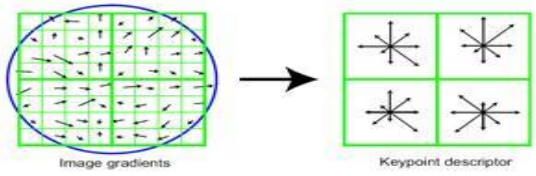


Figure: 14 Feature extraction in case of SIFT

4(f) MLBP (Multi Scale Local Binary Pattern):

It same like SIFT (Scale Invariant Feature Transform), it used to image representation. A novel discriminative face representation derived by the LDA (Linear Discriminant Analysis) of multi scale local binary pattern histogram is proposed for face recognition. The face image is first partitioned into several non-overlapping regions. In each region multi scale local binary pattern histograms are extracted and contracted into a regional feature [4][11]

4(g) Data base Module MORPH & FG-NET.

it is the type of the data base that is specially used to store the huge amount of images during the face recognition. It almost contains the 78000 face images of 20000 different subject captured of different ages.

MORPH album 2 data set is portioning into a training set and an independent test set. For training of data used used to load the MFDA

.we selected a subset of 20000 face images from 10000 subject within two per subject.[19]

FG-NET data base has only a small no. of subjects, it has many more image / subject than MORPH. Also FG-NET suffer from the fact there is a large variation in expression, pose, illumination among the images.[7]

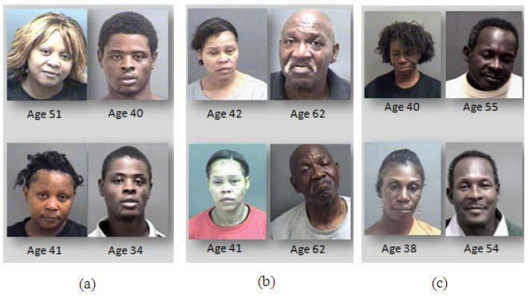


Figure 15: Images of various age present in data base

4(h) system design & implementation

To design the system architecture there are the following diagram. It contain two type of design first is system high level design and second is low level design.

In case of high level design it provide interface between many module like face recognition application, image processing, artificial neural network and graphics user interface. And they will connect with image acquisition and storage. But in case of low level design we can sow the DFD 0 level and DFD 1 level and 2 ,3 and so own.[5]

In this case we will show DFD 0 and DFD 1 level design. In case of high and low level design we implement the overall architecture & processing of data in form of graphical analysis and It is the simple approach to implement.[20][4]

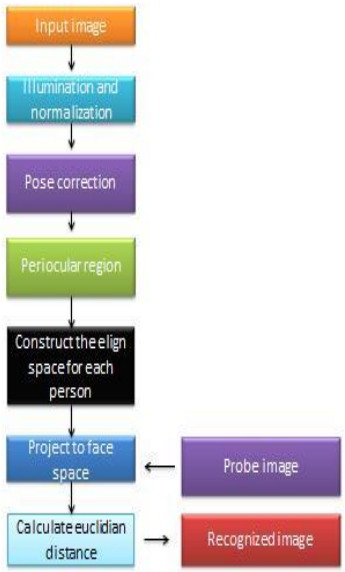


Figure 16: System design

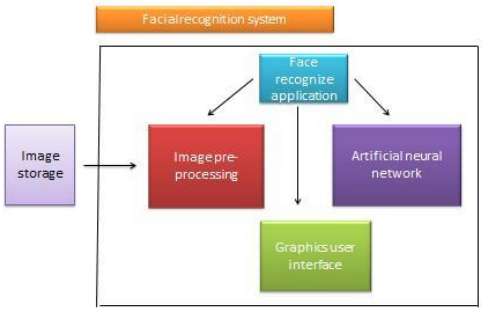


Figure: 17 System high level design

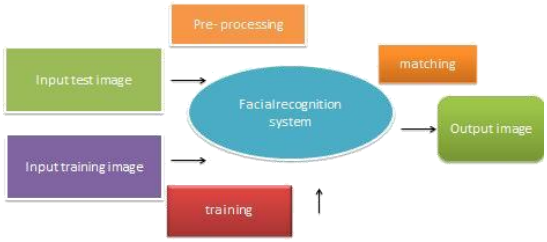


Figure: 18 System low level design

4(i) Learning Parameter (Neural network) &Testing Performance

In case to learn the system do decide the appropriate action used the neural network that will implement on the MATLAB. [22]

There is the testing in based on 4(1) performance testing 4(2) correctness testing

4(i) 1: Performance testing:

We check the performance through neural network .thus we first performed tests on the image portioned & pre- processing operation. One of those test include the resizing of an image with dimension of 150*200 pixels to have dimension. 120*160 ,60*80 ,30*40 15*20 pixel as respectively The result of the above tests are discipline in table 1 led us to use image with dimension 15*20 pixel in our system.

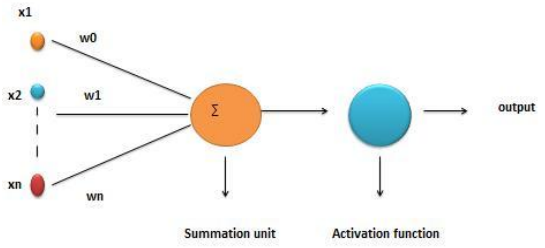


Figure 19: Artificial neural network for operation

4(i) 2 correctness testing:

To ensure that our system could in fact recognize faces by training and testing a neural network, we performed offline testing by using a face data base.

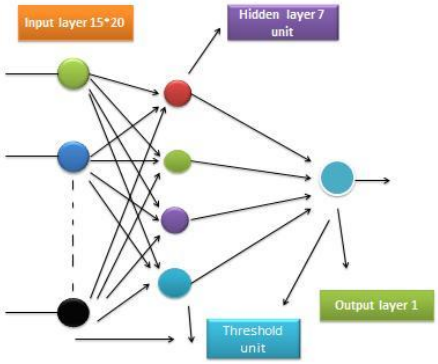


Figure 20 Neural network architecture with sigmoid threshold units.

Resize dimension	Time (ms)
120*160	11.433
60*80	1.695
30*40	0.135
15*20	0.043

Figure: 21 Table for image resizing operations

4(j) Experimental result:

The experimental result is shown in both data base module like MORPH and FG-NET data base. [11][14]

4(j)1 Result in MORPH data base

4(j)2 Result in FG-NET data base

The MORPH data base contains the 78000 face images of 20000 different subject captured at different ages. It gives the 84% accuracy of output.[10]

The FG- NET data base is the component of 1002 face images from 82 different subjects. It is the additional experiment on the FG-NET data base. In order to keep the training data separated the leave one out strategy is used in our study.

Some interesting results were obtained when we tried to do the age invariant age recognition.

- A database of 6 adult and 6 child images was used.[22]
- For a match of an adult image with all the child images in the database, 4 out of 6 images could be matched Successfully.
- For a match of a child image with all the adult images in the data base,again 4 out of 6 images could be matched successfully.
- There was no usefulness of the distance between eyes for face recognition.
- Most useful feature (definitely a RAI feature) seems to be the distance between the lips and nose.
- Another important feature is the distance between the lips and eyes.
- In our database, there was a mismatch for pair's number 2 and 4. Rest all matched in both the directions.
- Even though the database was very small, there seems to be a very good possibility of a successful age invariant
- Matching technique to be possible using feature analysis.

Figure 22: Two image of different age

Most likely match with image number 6 with a match values of 0.035333
All the match values:
0.0680 0.0405 0.1288 0.0502 0.0695 0.0353

4(k) Future work:

There seems to be a definite possibility for further extension of the work. I have already shown that certain Measures taken from the features of the face show a high match with the face at a different age.

Some possibilities that arise from our work: Get more features from the image. More features will improve the match. Other possible features can be eyebrows, ears, shape of face, etc. Improve the accuracy of match. A better and more accurate determination of feature location would help in getting the numerical measures more accurately. This would in turn improve our reliability.

Try an intra-feature match rather than taking inter-feature measures. This would involve considering shapes, sizes and aspect ratios of the features already extracted. A promising feature would be eyes. A direct template matching can be tried on the eyes. An automatic face correction algorithm can be implemented to correct and reorient certain images which are not usable directly.

A good way of testing the reliability of the system and even to get an idea of the reliable features, would be to match the faces of the same individual at the same age. This would eliminate a lot of unreliable and weak performing features.

References

[1] M. Albert, K. Ricanek , and E. Patterson, "A review of the literature on the aging adult skull and face: Implications for forensic science research and applications," J. Forensic Science Int'l, vol. 172, no 1, October 2007, pp. 1-9.

[2] N. Ramanathan and R. Chellappa, "Computational Methods for modeling facial aging: A survey," J. Visual Languages and Computing, vol. 20, no. 3, June 2009, pp. 131-144.

[3] Y. Fu and T. S. Huang, "Human age estimation with regression on discriminative aging manifold," IEEE Trans. Multimedia, vol. 10, no. 4, pp. 578-584, Jun. 2008.

[4] X. Geng, Z. Zhou, and K. Smith-Miles, "Automatic age estimation based on facial aging patterns," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 29, no. 12, pp. 2234-2240, Dec. 2007.

[5] G. Guo, Y. Fu, C. Dyer, and T. Huang, "Image-based human age estimation by manifold learning and locally adjusted robust regression," IEEE Trans. Image Process., vol. 17, no. 7, pp. 1178-1188, Jul. 2008.

[6] G. Guo, G. Mu, Y. Fu, and T. Huang, "Human age estimation using bio-inspired features," in IEEE Conf. Computer Vision and Pattern Recognition, 2009, pp. 112-119.

[7] Y. Kwon and N. da Vitoria Lobo, "Age classification from facial images," Computer
Vision and Image Understanding, vol. 74, no. 1, pp. 1-21, 1999.
[8] A. Lanitis, C. Draganova, and C.
Christodoulou, "Comparing different classifiers for automatic age estimation," IEEE Trans.
Syst., Man, Cyber, vol. 34, no. 1, pp., 621-628, Feb. 2004.
[9] A. Montello and H. Ling, "Age regression from faces uses random forests," in IEEE Int.
Conf. Image Processing, Cairo, Egypt, 2009.
[10] N. Ramanathan and R. Chellappa, "Face verification across age progression," IEEE
Trans. Image Process., vol. 15, no. 11, pp. 3349-3361, Nov. 2006.
[11] J. Wang, Y. Shang, G. Su, and X. Lin,
"Age simulation for face recognition," in Int.
Conf. Pattern Recognition, pp. 913-916, 2006.
[12] S. Yan, H. Wang, X. Tang, and T. Huang, "Learning auto-structured regressor from uncertain nonnegative labels," in Int'l Conf. Computer Vision, pp. 1-8, 2007.
[13] S. Zhou, B. Georgescu, X. Zhou, and D.
Comaniciu, "Image based regression using boosting method," in IEEE Int. Conf. Computer
Vision, 2005, vol. 1, pp. 541-548.
[14] A. Lanitis, C. Taylor, and T. Cootes,
"Toward automatic simulation of aging effects on face images," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 24, no. 4, pp. 442-455, Apr. 2002.
[15] J. Suo, S. Zhu, S. Shan, and X. Chen, "A compositional and dynamic model for face aging," IEEE Trans. Pattern Analysis and
Machine Intelligence, vol. 32, no. 3, pp. 385-401, March 2010.
[16] J. Suo, X. Chen, S. Shan, and W. Gao, "Learning long term face aging patterns from partially dense aging databases," in Int. Conf.
Computer Vision, pp. 622-629, 2009.
[17] N. Tsumura, N. Ojima, K. Sato, M. Shiraishi, H. Shimizu, H. Nabeshima, S.
Akazaki, K. Hori, and Y. Miyake, "Image-based skin color and texture analysis/synthesis by extracting hemoglobin and melanin information in the skin," ACM Trans. Graph., vol. 22, no. 3, pp. 770-779, 2003.
[18] U. Park, Y. Tong, and A. K. Jain, "Age Invariant Face Recognition, " IEEE
Transactions on Pattern Analysis and Machine Intelligence, vol. 32, no. 5, pp. 947-954, May 2010.
[19] K. RicanekJr and T. Tesafaye, "Morph: A
Longitudinal Image Database of Normal Adult Age-Progression," in Int'l Conf. Automatic
Face and Gesture Recognition, pp. 341-345, 2006.
[20] D. Lowe, "Distinctive image features from scale-invariant keypoints," Int'l Journal of
Computer Vision, vol. 60, no. 2, pp. 91-110, 2004.
[21] T. K. Ho, "The random subspace method for constructing decision forests," IEEE
Transactions on Pattern Analysis and Machine Intelligence, vol. 20, no. 8, pp. 832-844, 1998.
[22] L. Breiman, "Bagging predictors," Machine
Learning, vol. 24, no. 2, pp. 123-140, 1996.
[23] T. Ojala, M. Pietikainen, and T. Maenpaa, "Multi resolutiongray-scale and rotation invariant texture classification with local binary patterns," IEEE Transactions on Pattern
Analysis and Machine Intelligence, vol. 24, no. 7, pp. 971-987, 2002.

Analysis of Wormhole Attack in AODV based MANET Using OPNET SIMULATOR

Achint Gupta
IET, Alwar Rajasthan (INDIA)
achintgupta7792@gmail.com

Mohit Khandelwal
IET,Alwar Rajasthan (INDIA)
mohitonnet@gmail.com

Abstract - **Mobile ad hoc network (MANET) is a self-configuring network formed with wireless links by a collection of mobile nodes without using any fixed infrastructure or centralized management. The mobile nodes allow communication among the nodes by hop to hop basis and the forward packets to each other. Due to dynamic infrastructure-less nature and lack of centralized monitoring, the ad hoc networks are vulnerable to various attacks. The performance of network and reliability is compromised by attacks on ad hoc network routing protocols. In a wormhole attack an intruder creates a tunnel during the transmission of the data from one end-point of the network to the other end-point , making leading distant network nodes to believe that they are immediate neighbors' and communicate through the wormhole link. In this paper we have analyzed the effect of wormhole attack on AODV routing protocol based Mobile Ad-hoc Network using OPNET simulator using parameter like number of hops, delay, retransmission attempt, and data dropped.**

Keywords-AODV, MANET, OPNET, Wormhole attack.

INTRODUCTION

A mobile Ad hoc network is a collection of two or more devices or nodes using wireless communication and networking capabilities [1], [2], [3]. These nodes like laptop, computers, PDAs and wireless phones have a limited transmission range for direct transmission .If two such devices are located within transmission range of each other, they can communicate directly otherwise they will use intermediate nodes. Thus, a multi-hop scenario will occur in which several intermediate will be used before they reach the final destination. Each node performs the functions as a router. The success of communication depends on cooperation of other nodes. Since the transmission may use several nodes as intermediate nodes for transmission many routing protocols [3] have been proposed for the MANETS. Many of them assume that other nodes are trustable so they do not consider attack and security issues. The lack of The lack of Infrastructure, rapid deployment practices; make them vulnerable to a wide range of security attacks. The nodes that can move randomly, freely in any direction they will organize themselves arbitrarily in the network. The network topology changes rapidly, frequently and unpredictably which changes the status of trust among nodes .However most of these attacks are performed by a single malicious node in the network. Many solutions exist to solve such attacks [5], [6],[7] but they cannot prevent from the attacks such as wormhole attack. Routing

protocols is one of the interesting research areas. Many routing protocols such as AODV, OLSR, DSR etc has been developed for MANET. The rest of the paper is organized as follows. Section 2 describes about routing protocol and AODV. Section 3 of presents the wormhole attack. In section 4, simulation configuration is presented. Section 5 provides simulation results and analysis. Section 6 concludes the work.

ROUTING PROTOCOL & AODV

A. **Routing Protocol**

The nature of MANET's makes simulation modeling an important tool for understanding the operation in these networks. Multiple Ad-hoc network routing protocols have been developed in the recent years, in order to find an optimized Routes between source and destination. To make data transmission possible between two nodes, multiple hops are required due to the limited transmission range of the nodes. Due to the Mobility of the nodes the situation becomes even more complicated. Routing protocols can be categorized in three category named as proactive, reactive and hybrid protocols. Proactive routing protocols are typically table-driven such as Destination Sequence Distance Vector (DSDV). Reactive routing protocol does not regularly update the routing information. Information is updated only when there is some data need to be transmitted. Examples of reactive routing protocols are Dynamic Source Routing (DSR) and Ad Hoc On-Demand Distance Vector (AODV). Hybrid protocols are the combination of both reactive and proactive approaches such as Zone Routing Protocol (ZRP).

B. **AODV Routing Protocol**

Ad hoc On-Demand Distance Vector (AODV) [4] routing protocol is a reactive routing protocol that creates a path between source and to destination only when required. Routes are not established until any node sends route discovery message that the node want to communicate or transmit data with other node in the network . Routing information is stored in source node and destination node, intermediate nodes dealing with data transmission. This Approach reduces the memory overhead, minimize of the network resources, and runs well in high mobility scenario. The communication between nodes involves main three procedures known as path discovery, Path establishment and path maintenance. Three types of control messages are used to run the algorithm, i.e. Route Request (RREQ), Route Reply (RREP) and Route Error (RERR) [8]. The format of RREQ and RREP packet are shown in Table 1 and Table 2..

Table 1: RREQ Field

Source Address	Source Sequence	Broadcast Id	Destination Address	Destination Sequence	Hop Count

Table 2: RREP Field

Source Address	Destination Address	Destination Sequence	Hop Count	Lifetime

When the source node wants to send some data to the destination node, Source will issue the route discovery procedure. The source node will broadcast route request packets to all its accessible neighbors'. The intermediate node receiving request (RREQ) will check the request whether he is destination or not. If the intermediate node is the destination node, will reply with a route reply message (RREP). If not the destination node, the request will be forwarded to other neighbor nodes. Before forwarding the packet, each node stores the broadcast identifier and the node number from which the request came. Timer is used by the intermediate nodes to delete any entry when no reply is received for the request. The broadcast identifier, source ID are used to detect whether the node has received the route request message previously or not. It prevent from the redundant request receiving in same nodes. The source node may receive more than one reply, in that case it will determine later which message will be selected on the basis of hop counts. When any link breaks down due to the node mobility, the node will invalidate the routing table. All destinations will become unreachable because of loss of the link. Then it will create a route error (RERR) message. The node sends the RERR upstream to the source node. When the

source receives the Route reply message, it may reinitiate route discovery if it still requires the route.

WORM WHOLE ATTACK

In wormhole, an attacker creates a tunnel between two points in the network and creates direct connection between them as they are directly connected. An example is shown in Figure. 1. Here R and P are the two end-points in the wormhole tunnel. R is the source node and S is the destination node . Node R is assuming that there is direct connection to node P so node R will start transmission using tunnel created by the attacker .This tunnel can be created by number of ways including long-range wireless transmission ,With the help an Ethernet cable or using a long-range wireless transmission .Wormhole attacker records packets at one end in the network and tunnels them to other end-point in the network. This attack compromise the security of networks For example, when a wormhole attack is used against AODV, than all the packets will be transmitted through this tunnel and no other route will be discovered. If the tunnel is create honestly and reliably than it is not harmful to the network and will provides the useful service in connecting the network more efficiently. A potential solution is to avoid wormhole attack is to integrate the prevention methods into intrusion detection system but it is difficult to isolate the attacker using only software based approach because the packets sent by the wormhole are similar to the packets sent by legitimate nodes [9]. Choi et al. in [11] said that all the nodes should monitor the behavior of its neighbor nodes. Each node sends RREQ messages to destination by using its neighbor node list. If the source does not get back the RREP message from destination within a stipulated time, it consider the presence of wormhole attack and adds that route to its wormhole list .on-demand routing protocol (AODV) is being used in dynamic wireless ad hoc networks, a new route will be discovered in response to every route break [10]. The route discovery requires high overhead. This overhead can be reduced if there are 7multiple paths and new route discovery is required only in the situation when all paths break.

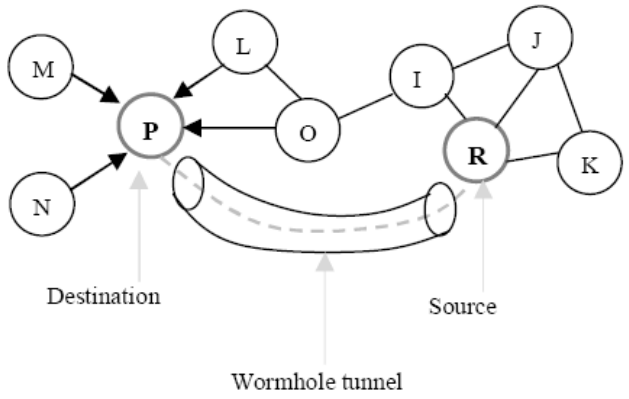


Fig. 1: Wormhole Attack

WORM WHOLE ATTACK

All the simulation work is performed in OPNET MODELER network simulator version 14.0.Simulation parameters are given in Table 3.

Parameters	**Description**
Examined Protocol CBR	AODV
Simulation Time	2000 sec.
Simulation Area	100×100 m
Seed value	191
Number of Nodes	16
Malicious Nodes present	02
Network traffic	CBR
Packet size	512 Byte

Table 1: Simulation Parameters

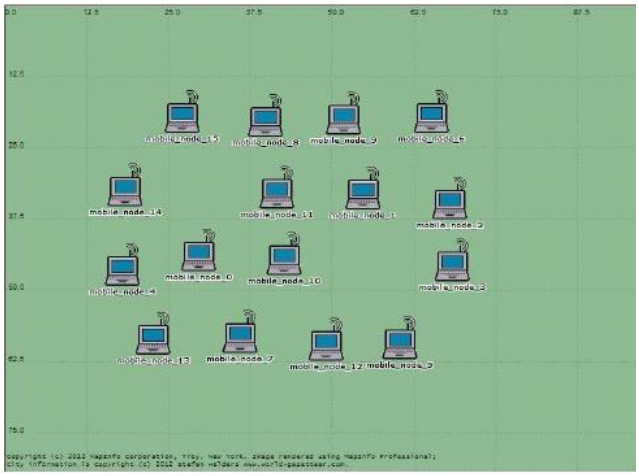


Fig. 2: Node Distribution in Network

Fig. 3: Node Distribution affected by Wormhole Attack

Wormhole attack scenario is shown in Figure 3.Wormhole tunnel is created in between node 0 and node 5. Due to wormhole all the traffic between node 0 and node 5 will go directly while other intermediate nodes between them are presented in the network.

SIMULATION RESULT AND ANALYSIS

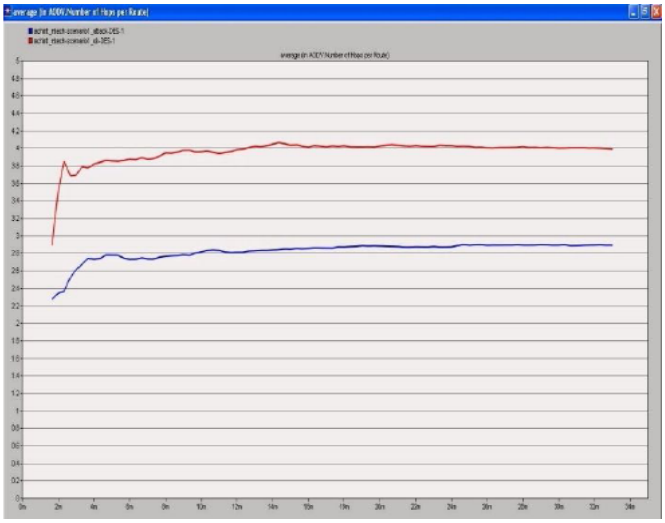


Fig. 4: Average number of hopes per route

Figure 4 shows the average route length using number of hops for the condition when there is no attack and when network is affected by wormhole attack'. The Simulation time is depicted by X direction and the number of hops by Y direction. No attack condition is depicted by red color where as attack condition is shown by blue color. Wormhole attack occurs in the network than wormhole affected node start sending packet by using the tunnel created by attacker without using intermediate nodes so number of hopes reduces as shown by blue color.

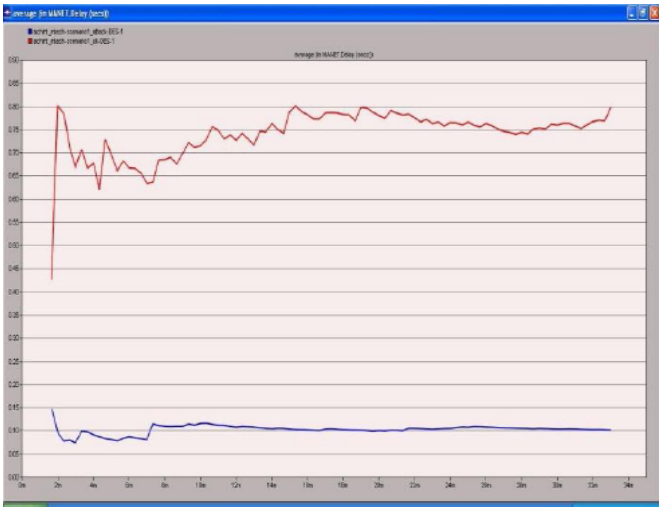


Fig. 5: Average delay in seconds

Figure 5 shows the average route discovery time for wormhole attack and no attack conditions. X direction showing the simulation time while Y direction showing average delay. No attack condition is depicted by red color; wormhole attack reduces the delay because the packets are delivered without using any intermediate nodes denoted by blue color.

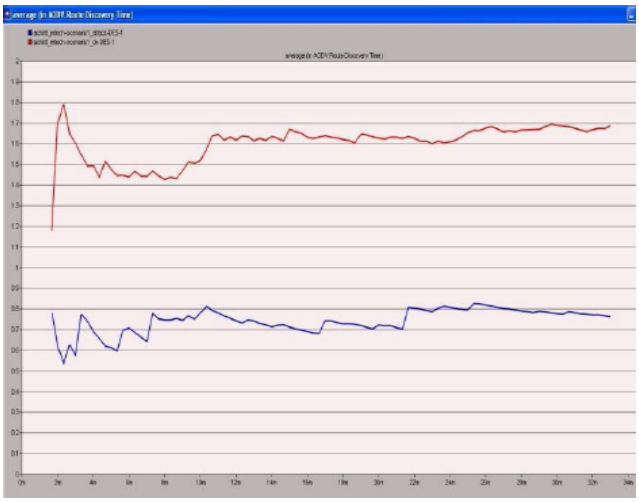


Fig. 6: Average route discovery time

Figure 6 shows the average route discovery time. X direction shows the simulation time and Y direction shows the average route discovery time. Due to worm hole attack wormhole affected route will be selected most of the times so route discovery time will be reduced as depicted by blue color where as when there is no attack all the routes will be checked to find optimum routes so route discovery time will be higher as compared to the worm hole condition as denoted by red color.

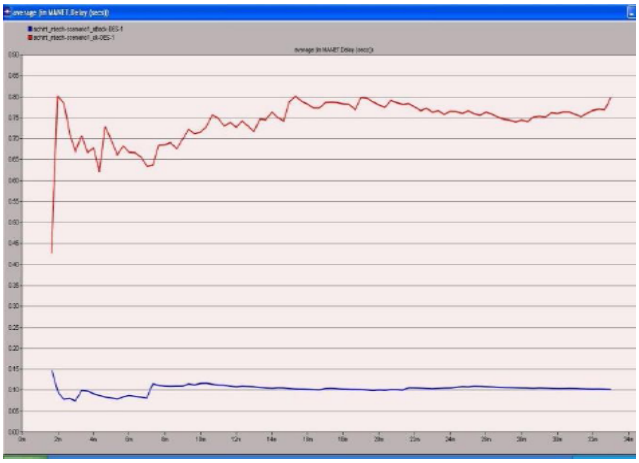


Fig. 7: Average route discovery time

Figure 7 shows the retransmission attempt. X direction shows the simulation time and Y direction shows number of attempt for retransmission. Due to worm hole attack wormhole affected route will be selected most of the times so packet may not reach their destinations so number of retransmission will be increased as shown in red color where as when there is no attack most of packets will be delivered to destination so number of retransmission will be less denoted by blue color.

Fig. 8: Average Throughput

Figure 8 shows the average through put during the transmission. X direction shows the Simulation time and as Y direction number of packets transmitted. Due to wormhole attack the packets reaching their destination reduced so throughput also reduced as denoted by blue color. Whereas throughput without attack is denoted by red color

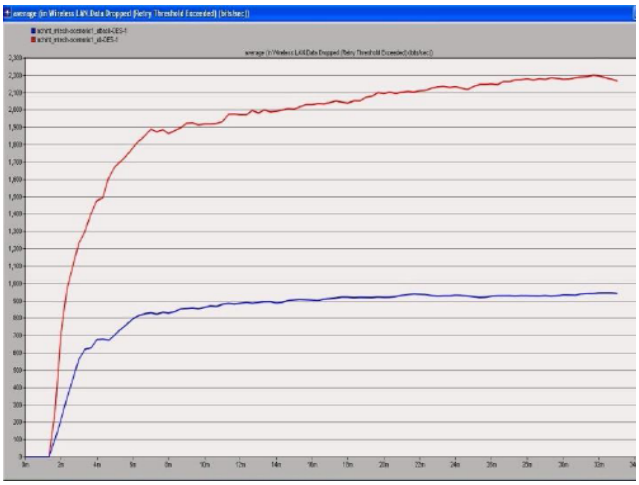


Fig. 9: Average Data Dropped

Figure 9 shows the average data dropped during the transmission. X direction shows the Simulation time and as Y direction depicts the number of packets loss during transmission When there is no attack in the system so packets Achint Gupta et al, International Journal of Computing, Communications and Networking, 1(2), September – October 2012, 63-67 67 @ 2012, IJCCN All Rights Reserved had to travel number of hops and data will be dropped than could not find their destination as denoted by red color while when data is transmitted by using wormhole tunnel number of hops are reduced so only packets will be dropped as shown by blue color.

Fig. 10: Average Traffic Received

Figure 10 shows the average traffic received during the transmission. X direction shows the Simulation time and as Y direction depicts the number of packets received. Red color shows when there is no attack whereas due to wormhole attack number of packed received also increase as denoted in blue color.

CONCLUSIONS

MANETs is insecure and vulnerable to various attacks so it require a reliable, efficient and a secure protocol that can be rapidly deployed and use dynamic routing. AODV is prone to various attacks like modification in the sequence numbers or hop counts, source route tunneling, spoofing and fabrication in the error messages. Wormhole attack is a real threat against AODV protocol in MANET. Wormhole attack can be easily launched even in networks with provides confidentiality and authenticity. The malicious nodes usually target the routing control messages related to routing information. Therefore trustworthy techniques for detection and prevention of wormhole attack should be used. Some existing solutions cannot work well in the presence of more than one malicious node, while some other requires special hardware. So, there is still a lot of scope of research to provide security to the MANETs.

References

[1] Perkins C. and Bhagwat P. **Highly dynamic destination-sequence distance-vector routing (DSDV) for mobile computers**, In Proceedings of ACM Conference on Communications Architectures, Protocols and Applications (ACM SIGCOMM)

[2] Perkins C. and Royer E. Ad hoc on-demand distance vector routing, In Proceedings of Second IEEE Workshop on Mobile Computing Systems and Applications, pp. 90-100 (1999)

[3] Perkins.C.E. **Ad hoc Networking**, Boston, Addison Wesley (2001)

[4] Harris Simaremare and Riri Fitri Sari. **"Prevention of impersonation attack in wireless mobile ad hoc Networks**, International Journal of Computer Science and Network Security (IJCSNS), Vol. 7, No. 3, p.118–123 (2007)

[6] Papadimitratos P. and Haas Z. J. **Secure routing for mobile ad hoc networks**, In Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (2002)

[7] Hu Y.-C., Johnson D. B. and Perrig A. **SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks**, In IEEE Workshop on Mobile Computing Systems and Applications (WMCSA), pp. 3–13 (2002)

[8] K. Lakshmi, S.Manju Priya, A.Jeevarathinam, K.Rama and K. Thilagam. **Modified AODV Protocol against Black hole Attacks in MANET**, International Journal of Engineering and Technology Vol.2 (6), 2010.

[9] S Upadhyay . and B.K Chaurasia. **Impact of Wormhole Attacks on MANETs**, International Journal of Computer Science & Emerging Technologies, Vol. 2, Issue 1, pp. 77-82 (2011)

[10] R. Maulik and N. Chaki. **A Comprehensive Review on Wormhole Attacks in MANET.** In Proceedings of 9 th International Conference on Computer Information Systems and Industrial Management Applications, pp. 233-238, 2010

[11] S. Choi , D. Kim, D. Lee and J. Jung. **WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc** Networks, International Conference on Sensor Networks Ubiquitous and Trustworthy Computing, pp. 343-348, 2 008.

Avant-Garde CPU Scheduling Algorithm

Priyam Maheshwari
GCET,Greater Noida
priyammaheshwari29@gmail.com

Akanksha Saxena
GCET,Greater Noida
akankshasaxena663@gmail.com

Shivesh Gupta
GCET,Greater Noida
shivesh.virgo@gmail.com

Abstract - **One of the fundamental function of an operating system is scheduling. CPU Scheduling is the basis of multi-programmed operating system. The scheduler is responsible for multiplexing processes on the CPU. Resource utilization is the basic aim of multi-programming operating system. In multiprogramming systems, several algorithms are available. But our work focuses on design and development aspect of new scheduling algorithm for multi-programming operating system in the view of optimisation. Avant-Garde CPU Scheduling Algorithm which acts as both pre-emptive and non-pre-emptive based on the arrival time. The prosed algorithm helps to improve the CPU efficiency in real time unit-processor-multi programming operating system. In this paper, the results of the existing algorithms (FCFS, SJF, Priority and Round Robin) are compared with the proposed algorithm.**

Keywords – Operating System, uni-processor, multi-programming, Scheduling, FCFS, SJF, Priority, Round Robin.

INTRODUCTION

The world went through a long period (late 80's, early 90's) in which the most popular operating systems (DOS, Mac) had no sophisticated CPU scheduling algorithms. They were single threaded and ran one process at a time until the user directs them to run another process. Determining which processes run when there are multiple runnable processes is called scheduling. It is important because it can have a big effect on resource utilization and the overall performance of the system.

The CPU is one of the primary resources, so its scheduling is essential to an operating system design[1].Sharing of computer resources between multiple processes is also called scheduling [2].

A process has five basic states namely NEW, Ready, Running, Waiting and Terminate [2] [3].A process migrates between various scheduling queues by different schedulers until it gets terminated.

The various schedulers present are long term, short term, mid-term schedulers. These queues mainly contain the ready queue which contains set of processes ready for CPU response. The second queue is the device or the I/O queue which contains all the processes that are waiting for the I/O [2] response.

Schedulers in general try to maximize the average performance of a system according to the given criterion [4].

Multiprogramming has many processes so there must be a way for the operating system and application processes to share the CPU. Another main reason is the need for processes to perform I/O operations in the computations. So the process of multiprogramming
systems is to allocate the CPU to another process whenever a process invokes an I/O operation [5].

The algorithm proposed in this article is both preemptive and non-preemptive in nature and attempts to give fair efficiency. We have compared the results of our scheduling algorithm with other algorithms. This algorithm both efficiently for both preemptive and non-preemptive.

SCHEDULING CRITERIA

A. CPU Utilization: It is the average fraction of time, during which the processor is busy [3, 6].

B. Throughput: It refers to the amount of work completed in a unit of time. The higher the number, the more work is done by the system [6].

C. Waiting Time: The average period of time a process spends waiting. Waiting time may be expressed as turnaround time less the actual execution time [6].

D. Turnaround time: The interval from the time of submission of a process to the time of completion is the turnaround time [6].

E. Response time: Response time is the time from submission of a request until the first response is produced [6].

F. Priority: give preferential treatment to processes with higher priorities [6].

G. Fairness: Avoid the process from starvation. All the processes must be given equal opportunity to execute [6].

SCHEDULING ALGORITHMS

First Come First Serve

The criteria of this algorithm is „the process that requests first, holds the CPU first" or which process enter the ready queue first is served first [3].This algorithm uses FIFO queue. It is the simplest CPU scheduling algorithm.

Characteristics

Permits every process to eventually complete, hence no STARVATION. Turnaround, waiting and response time is high. Throughput is low.

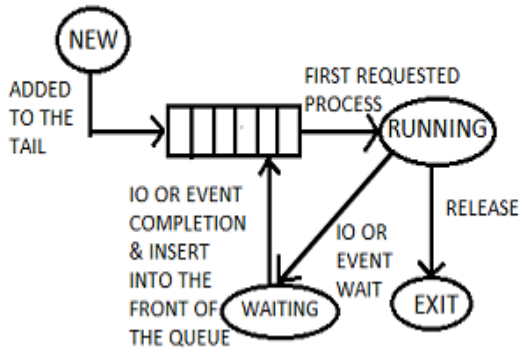


Fig 1

Shortest Job First (Non Pre-emptive)

The process is allocated to the CPU which has least burst time. Processes with the least burst time are in the head and longest in the tail of queue. If two process having the same CPU burst time FCFS is used to break up the tie [3].

Characteristics

Throughput is maximum. Minimizes the average waiting time. Difficulty in knowing the length of the next CPU request. Starvation of large processes is a serious liability.

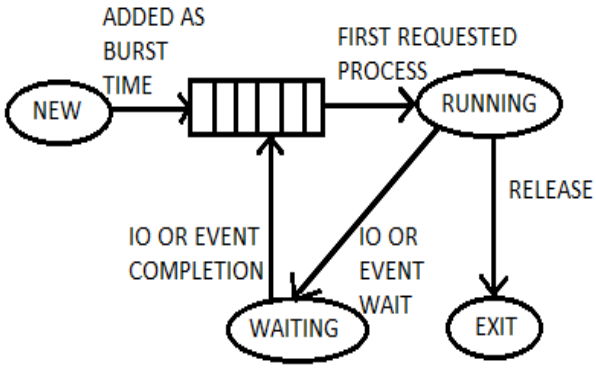


Fig 2

Round Robin

It assigns a small unit of time to each process called TIME SLICE or QUANTUM [2]. Ready processes are kept in the queue .Scheduler allocates the CPU to each process for a time interval of assigned QUANTUM. New processes are added at the tail of queue.

Characteristics

Setting the Quantum too short causes too many Context switches. Setting the Quantum too long causes poor response time. Deadlines are rarely met in pure RR system [8].

Priority Scheduling

Priority rank is assigned to each process. Lower priority process gets interrupted by the higher priority. If multiple processes having the same priorities are ready to execute, control of CPU is assigned to these processes on the basis of FCFS [1].

Characteristics

Starvation can happen to low priority process. The waiting time increases for the equal priority process[9].Higher priority process have smaller waiting and response time. An SJF algorithm is simply a priority algorithm where the priority is the inverse of the (predicted) next CPU burst. That is, the longer the CPU burst, the lower the priority and vice versa.

PROPOSED WORK- AVANTE-GARDE CPU SCHEDULING ALGORITHM

Objective is to introduce a new CPU algorithm called A AVANTE-GARDE CPU SCHEDULING ALGORITHM. This algorithm acts as both preemptive and no preemptive on the basis of the arrival time[9].This improves the CPU efficiency in real time uni-processor-multi programming OS. Scheduler is responsible for multiplexing[10].The results of existing algorithms are compared with the proposed algorithm.

1) This algorithm is both preemptive and non preemptive.
2) In this algorithm a new factor called condition factor(F).
3) F=Burst time Arrival time
4) F is arranged in the ascending order in the ready queue.
5) Process having shortest F is executed first and process with next shortest F is executed next.
6) This algorithm reduces waiting, turnaround and response time and increases CPU utilization and throughput
7)BT=Burst Time, AT=Arrival Time

Pseudo Code

Initialization variables
BT
AT
Num process[n]
Factor[i]
Turn[n]
Wait[n]
Temp
Current time
Wait time=0
Turn time=0
Avg waiting=0.0
Read BT[n] and AT[n]
Compute factor[i] BT[i] + AT[i]

Pseudo Code For Pre-emptive

Arrange the elements in ascending order based arrival time

For i 0 to n-1
For j 1 to n
If factor[i] > factor[j]
Temp BT[i]
BT[i] BT[j]
BT[j] temp
Temp AT[i]
AT[i] AT[j]
AT[j] temp
Temp factor[i]
Factor[i] factor[j]
Factor[j] temp
End for
For i 0 to n-1
For j i to n
If atime[i]==atime[j]
Then sort elements in ascending order based on factor[i] and factor[j]
If burst time!=0 && atime==current time
Begin
atime[i]=atime[i]+1
btime[i]=btime[i]-1
current time++
If btime[i]==0
Turn time=current time
End
For i 0 to n

```
Begin
Wait[i]=turn[i]-btime[i]-atime[i]
Turn[i]=turn[i]+atime[i]
        wait time=wait time +wait[i]
        turn time =turn time +turn[i]
End
Avgwait time=wait time/n
Avgturn time=turn time/n
```

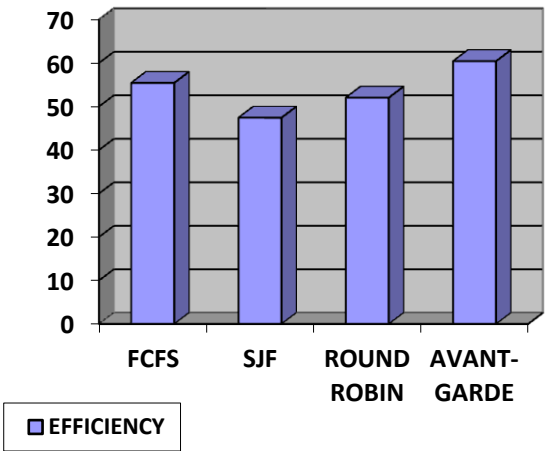
Pseudo Code For Non Pre-emptive

Arrange the elements in ascending order based condition factor

```
For i   0 to n-1
For j   1 to n
If factor[i] > factor[j]
Temp    BT[i]
BT[i]   BT[j]
BT[j]    temp
Temp    AT[i]
AT[i]   AT[j]
AT[j]   temp
Temp    factor[i]
Factor[i]    factor[j]
Factor[j]     temp
End for
For  i   0 to n
Begin
        wait[i]=wait[i]+burst[i]
        turn[i]=wait[i]+burst[i]
        wait time=wait time +wait[i]
        turn time =turn time +turn[i]
End
Avgwait time=wait time/n
Avgturn time=turn time/n
```

RESULT ANALYSIS

To compare the performance of the proposed scheduling algorithm it was implemented and compared with the existing scheduling algorithm.



CONCLUSION

Any CPU scheduling algorithm has limited accuracy. The only way to evaluate algorithm is to code it .The paper presents a new CPU scheduling algorithm called Avant-Garde CPU algorithm. It takes input from the user and compares the process set against different algorithm pairs. It provides analytical result with each set of graphs. The proposed algorithm is more efficient than FCFS, Round Robin and priority. It is also observed that proposed algorithm gives equal performance like a SJF algorithm. This algorithm gives good responsiveness and minimizes starvation for longer jobs. It also reduces the average waiting time of all processes.

References

[1] Hybrid Scheduling and dual queue scheduling Syed Nasir Shah,Ahmed Mahmood, Alan Oxley 2009- IEEE 978-1-4244-4520-2/09 Conference

[2] Abraham Silberschatz, Peter Baer Galvin, Greg Gagne, “Operating System Concepts”, Sixth Edition.

[3] Milan Milenkovic, “Operating Systems Concepts and Design”, McGraw-Hill, Computer Science Series, second edition.

[4] P. Balakrishna Prasad, “Operating Systems” Second Edition.

[5] M. Dietel, “Operating Systems”, Pearson Education, Second Edition

[6] Umar Saleem and Muhammad Younus Javed, “Simulation of CPU Scheduling Algorithm”.

[7] Sun Huajin', Gao Deyuan, Zhang Shengbing, Wang Danghui; "Design fast Round Robin Scheduler in FPGA"

[8] Md. Mamunur Rashid and Md. Nasim Adhtar, " A New Multilevel CPU Scheduling Algorithm", Journals of Applied Sciences 6 (9): 2036- 2039,2009

[9] Sukanya Suranauwarat, "A CPU Scheduling Algorithm Simulator", October 10-13, 2007, Milwaukee, WI 37th ASEE/IEEE Frontiers in Education Conference.

[10] Andrew S. Tanenbaum, Albert S. Woodhull, "Operating Systems Design and Implementation", Second Edition

[11] Milan Milenkovic, "Operating System Concepts and Design", McGraw-Hill, Computer Science Series, Second Edition

An Approach- TURN TOUCH

Shikha Jain
Ajay Kumar Garg Engineering College, Ghaziabad
Shikhajain646@yahoo.in

Bhawna Sachdeva
ABES Institute of Technology, Ghaziabad
bhawna.sachdeva@abesit.ac.in

***Abstract*- Now a day's touch Screen systems have really gained any ground. Everyone is using touch screen devices but the cost of touch screen laptops is very high. In this paper we proposed an alternative algorithm to convert any laptop or any device into a touch screen device by using two camera setup. TurnTouch is an implementation of touch screen. The camera's setup visually tracks a feature on a material and use the movement of the tracked feature to directly control the mouse pointer on a computer. The material could be an LED light or the tip of the stylus.[3] The material accordingly calculates the relative positioning of the feature with respect to the screen of the device to be operated upon. Both the cameras will then diffuse the image and integrates it to form a single image and successfully calculate the coordinates. These coordinates are then used to move the mouse pointer to the specific location, as calculated by the system. An algorithm has been proposed for converting any system into touch screen system.**

Keywords: Coordinate mapping, cam setup

INTRODUCTION

Digital image processing is the process of using computer algorithms to perform image processing on digital images. As a field of digital signal processing, digital image processing has many advantages over analog image processing. It allows a much wider range of algorithms to be applied to the input data and can avoid problems such as build-up of noise and signal distortion during processing. Since images are defined over two dimensions (perhaps more) digital image processing may be modeled in the form of multidimensional systems. Digital image processing allows the use of much more complex algorithms, and hence, can offer both more sophisticated performance at simple tasks, and the implementation of methods which would be impossible by analog means.The goal of this paper was to transform the normal LCD screen into a touch screen. This will be done with the help of two web cameras which will be filming the LCD and detecting the motion. This motion will then be transformed into adequate action like left mouse button click or a double click.

Application works by mapping Web Cam coordinates into LCD coordinates. This means that when Web Cam detects motion it knows its coordinates inside the image it has taken. Those coordinates are then transformed into LCD coordinates by using set of recalculated coordinates of the dots which are displayed during initialization phase. Motion is detected by using red color detection on normalized RGB color space.

The application uses two web cameras to focus on the LCD screen and then detect any red color that is present in the region of LCD coordinates. This red color is present on the material. Red color is used in demonstration but any vibrant color can be used to operate the touch screen, provided it is visible enough to be easily captured and differentiated by the camera

This paper is focused on the pattern of image processing and creating an application package that would be able to take input from two cameras. The package would process coordinates by calculating the

position of any object on the above screen using two cameras placed at certain fixed distance. These coordinates can be given as an input to the system so that it can take the mouse pointer towards those coordinates on the screen and a click operation can be performed.

If such a system can be developed, then it would reduce the user's cost for buying a touch screen. Rather, he can buy two cameras and install the package. This would be cost efficient for the user and with this method any computer screen would be able to function as a touch screen irrespective of the operating system used or the systems configuration. Such a system may bring out a revolution in the field of computing.

PROBLEM DEFINITION

Touch screens for computers is though a new terminology and there are not many computers having a touch screen. We are interested in developing computer vision systems that work under normal lighting to provide a method to detect the coordinates of the object pointing on the screen with the help of two webcams placed at some specific location and take our mouse pointer to click at that specific location (as pointed by the object).

This system would take continuous screenshots and calculate the respective coordinates. These coordinates would be further used to move the mouse pointer on the screen and perform click operations at various locations on the screen. This system should be able to integrate on any size of the computer screen without much change and difficulty. Also, the position of the webcam can be changed as per user's ease.

RELATED WORK

The "Camera Mouse" system has been developed to provide computer access for people with severe disabilities. [1] The system tracks the computer user's movements with a video camera and translates them into the movements of the mouse pointer on the screen. Body features such as the tip of the user's nose or finger can be tracked. [1] The visual tracking algorithm is based on cropping an online template of the tracked feature from the current image frame and testing where this template correlates in the subsequent frame. The location of the highest correlation is interpreted as the new location of the feature in the subsequent frame. Various body features are examined for tracking robustness and user convenience. A group of 20 people without disabilities tested the Camera Mouse and quickly learned how to use it to spell out messages or play games. Twelve people with severe cerebral palsy or traumatic brain injury have tried the system, nine of whom have shown success. They interacted with their environment by spelling out messages and exploring the Internet.[1]

Face as Mouse through Visual Face Tracking

This system introduces a novel camera mouse driven by 3D model based visual face tracking technique. [2] While camera becomes standard configuration for personal computer(PC) and computer speed becomes faster and faster, achieving human machine interaction through visual face tracking becomes a feasible solution to hand-free control. [2] The human facial movement can be decomposed into rigid movement, e.g. rotation and translation, and non-rigid movement, such as the open/close of mouth, eyes, and facial expressions, etc. We introduce our visual face tracking system that can robustly and accurately retrieve these motion parameters from video at real-time. After calibration, the retrieved head orientation and translation can be employed to navigate the mouse cursor, and the detection of mouth movement can be utilized to trigger mouse events. 3 mouse control modes are investigated and compared. An experiment in Windows XP environment verifies the convenience of navigation and operations using our face mouse. This technique can be an alternative input device for people with hand and speech disability and for futuristic vision-based game and interface. [2]

METHODOLOGY USED

The algorithm is proposed as follows:-

Basic Steps are

1. The basic camera setup
2. Coordinate mapping

3. Object Identification
4. RGB-HSV Conversion(Hue Saturation value)
5. Image Thresholding
6. Object tracking
7. Control computer mouse

Algorithms

Algorithm for capturing image:

1. start
2. create a grabber // for creating a frame
3. start grabber // to start web cam
4. if (imgage != null)
5. cvSaveImage // capture image
6. end if
7. Stop grabber
8. end

Algorithm for finding coordinates from captured image:

1. start
2. load captured image // cv.load("img .jpg")
3. void call
4. start
5. flag=0;
6. if(event== double click)
7. { flag=1;
8. x coordinate= x;
9. y coordinate=y;
10. }
11. end if
12 end
13. end

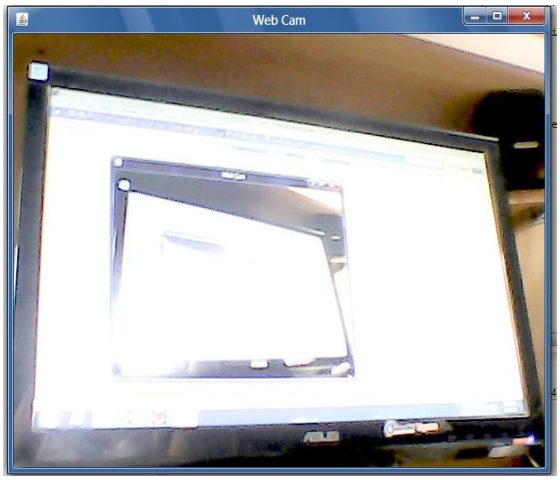
Algorithm for detecting and tracking red object:

1. start
2. create grabber // initialize the camera
3. start grabber // start taking pictures from camera
4. if (image! = null)
5. { hsv thresholding of image // finding red color object
6. get coordinates // find x and y position of red object
8. } end if
9. stop grabber
10.end

SIMULATION AND RESULTS

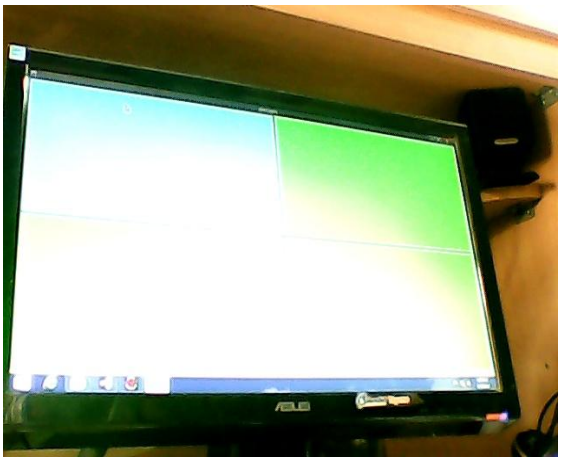
Java CV and Open CV libraries have been used. These libraries contain various classes that can be used for the processing and manipulation of the images. [5] Using Java CV we can directly use Open CV libraries in JAVA that was originally meant to be used in C/C++

1. Camera Setup



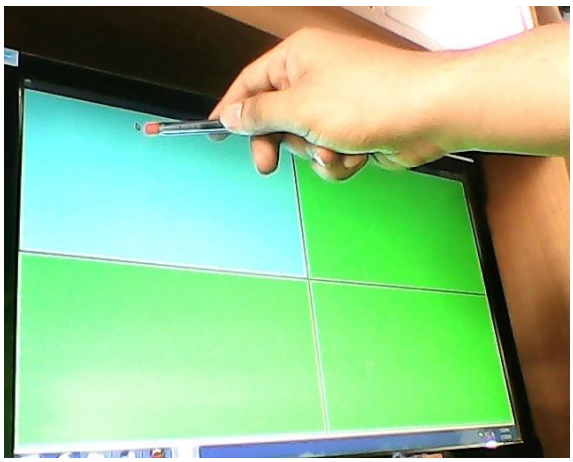
This is the initial step of the process. It involves setting up web cam so that it covers a full view of the screen such that all the four corners of the screen are visible easily and captured. This step would be always done for any new installation or when the position of the camera is changed. This method gives the user an ability to place the web cam at any position as per their comfort

2. Coordinate Mapping

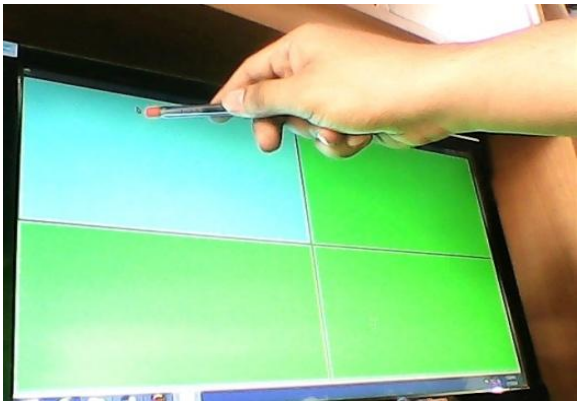


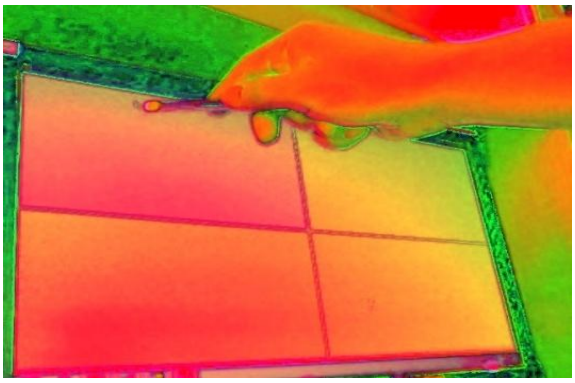
In this step we displayed the image from the web cam and the user was asked to click on some specific points so that the image coordinates could be mapped to screen coordinates. After clicking on the specific points the system could create a base for further calculations. This step involves mapping of the captured image coordinates to screen coordinates. Mapping is done using divide and conquer technique in which we divide the screen into 4 quadrants and by comparing the image pixel value with the centre pixel, we can get the resultant quadrant.

3. Object identification



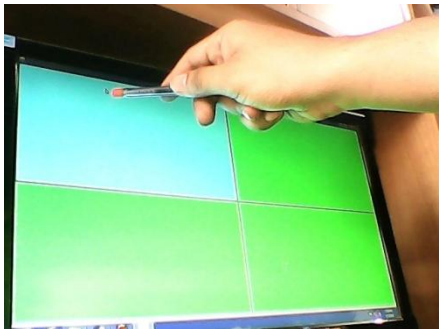
RGB-HSV Conversion (Hue Saturation Value)





Hue indicates the dominant color of an area, saturation calculates the colorfulness of an area in proportion to its brightness. Value indicates the color luminance. Separation between chrominance & luminance makes this color space popular in the skin color detection. The transformation of RGB to HSV is invariant to high intensity at white lights, ambient light and Surface orientations relative to the light source and hence, can form a very good choice for skin detection methods.

4. Image Thresholding



Thresholding is the simplest method of im

age segmentation from a grayscale image, thresholding can be used to create binary images. Image thresholding is a simple, yet effective, way of partitioning an image into a foreground and background. This image analysis technique is a type of image segmentation that isolates objects by converting grayscale images into binary images. Image thresholding is most effective in images with high levels of contrast.

CONCLUSION AND FUTURE WORK

The main aim of this paper was to transform the normal LCD screen into a touch screen. This was done with the help of two web cam which filmed the LCD and detected the motion. This motion was then transformed into adequate action like left mouse button click or a double click.

Application works by mapping Web Cam coordinates into LCD coordinates. This means that when Web Cam detects motion it knows its coordinates inside the image it has taken. Those coordinates are then transformed into LCD coordinates by using set of precalculated coordinates of the dots which are displayed during initialization phase. Motion is detected by using red color detection on normalized RGB color space.

Such a system was successfully developed and tested for various modules and different angles. The web cameras were placed at various distances from the screen and at various sizes of screen and were found to be properly working. Thus this system can be easily integrated for commercial purposes with a better quality of camera

References

[1] Betke, M. , Gips, J. , Fleming, P. The Camera Mouse: visual tracking of body features to provide computer access for people with severe disabilities, Published in: Neural Systems and Rehabilitation Engineering, IEEE Transactions on (Volume: 10 , Issue: 1)

[2] Tu, J., Huang, T. ; Hai Tao. Face as mouse through visual face tracking, Computer and Robot Vision, 2005. Proceedings. The 2nd Canadian Conference on, IEEE

[3] D. G. Evans, R. Drew, and P. Blenkhorn, "Controlling mouse pointer position using an infrared head-operated joystick", IEEE Trans. Rehab. Eng., vol. 8, no. 1, pp.107 -117 2000

[4] Yi-Fan Chuang Vision based finger detection and its application

[5] Kenneth Dawson-Howe Textbook on A Practical Introduction to Computer Vision with OpenCV, ISBN: 978-1-118-84845-6. 234 pages, May 2014, WILEY

Improving Hadoop MapReduce Performance by Optimizing Programs and Configuration

Ajay Mohan Verma
Birla Institute of Technology Mesra
ajaymverma@yahoo.com.in

Abstract - **MapReduce, a programming model for data processing is quite popular for developing distributed data processing. Hadoop executes MapReduce programs written in several languages; Java, Python, Ruby and C++. MapReduce programs are processed in parallel, entailing very large-scale data analysis for the users with enough machines at their disposal. Modern organizations are producing and collecting data at a high volume. Cloud platforms make MapReduce an attractive proposition for organizations lacking computing and human resources but requiring processing of large datasets. This large volume 'big-data' can be structured, semi-structured and unstructured and requires optimized processing for timely and cost-effective results. This paper is an attempt to summarize and analyze various techniques prevalent to improve performance of MapReduce by configuring the environment and optimizing programs. Though reader of the paper is assumed to have some background of Hadoop and MapReduce, yet covers many background concepts for easy grasp.**

Keywords – MapReduce, Hadoop, Optimization

INTRODUCTION

Hadoop MapReduce framework, which runs on top of HDFS (Hadoop Distributed File System), consists of a JobTracker running on the master node and many TaskTrackers running on slave nodes. 'Job' and 'Task' are two important concepts in MapReduce architecture. A MapReduce job contains a set of independent tasks. As a core component in MapReduce framework, the JobTracker is responsible for scheduling and monitoring all the tasks of a MapReduce job. Tasks are assigned to the TaskTrackers on which the map and reduce functions are executed. After receiving a job, MapReduce framework divides the input data of the job into several independent data splits. Then, each data split is assigned to one map task which distributes to the TaskTracker for processing using data locality optimization (i.e. keeping processing near the data being processed). Multiple map tasks can run simultaneously on the TaskTrackers and their outputs will be sorted by the framework and then fetched by reduce tasks for further processing. During the whole execution of a job, JobTracker monitors the execution of each task, reassigning failed tasks and altering state of the job in each phase. [5]

When a job is submitted to a Hadoop MapReduce cluster, the execution process of MapReduce job takes place in following three phases:

1. Prepare phase: a job begins with the 'start' state, conducting some initialization processing such as reading the input data splits information from HDFS and generating the corresponding map and reduce tasks on the JobTracker. After that, a special task called 'setup task' will be scheduled to a TaskTracker to setup the job execution environment. When the setup task is finished successfully, the job enters the running phase.

2. Running phase: in this phase, the job starts with 'run_wait' state. During this state, the job waits to be scheduled for execution by the MapReduce framework. When one of its tasks has been scheduled for execution on a TaskTracker, the job enters the 'runing_tasks' state to execute its entire map-reduce tasks. When the entire map and reduce tasks are completed successfully, the job moves to the 'suc_wait' state.

3. Finished phase: in this phase, another special task called 'cleanup task' is scheduled to clean up the running environment of the job. After the cleanup

task is done, the job moves to ‘succeeded’ state on successful completion.

A job can be killed by the client during prepare and running phases. It moves to ‘failed’ state on failures.

The Running phase consists of following 8 steps.

1. When the tasks are created, the JobTracker generates a ‘‘TaskInProcess’’ instance for each task. The tasks are still in the ‘unassigned’ state.

2. Each TaskTracker sends a heartbeat to the JobTracker for requesting tasks. In response, the JobTracker assigns one or several tasks to TaskTracker. The interval between two heartbeat messages is at least 3 seconds by default (i.e. TaskTracker waits for 3 seconds before sending next heartbeat for requesting task in case the TaskTracker is idle).

3. After receiving a task, the TaskTracker creates a ‘TaskTracker.TaskInProgress’ instance, running an independent child JVM (Java Virtual Machine) to execute the task, and then changing the task state of the TaskTracker to the ‘running’ state.

4. Each TaskTracker reports the information of its task to the JobTracker, and the JobTracker changing the task state to ‘running’ state. This is accomplished by the second round of heartbeat communication.

5. Once the task is completed in child JVM, the TaskTracker changes the task state to ‘commit_pending’. This is a state that waits for the JobTracker’s approval of committing the task.

6. This state change message is forwarded to JobTracker by the TaskTrackers through the next round of heartbeat communication. The JobTracker changes the task state to ‘commit_pending’ state to allow the TaskTrackers to commit the task results.

7. When getting the JobTracker’s approval, the TaskTracker submits the task execution results and then changes the task state to ‘succeeded’.

8. After that, the TaskTracker reports the ‘succeeded’ state to the JobTracker through the next heartbeat. Then the JobTracker changes the task state to ‘succeeded’.

As is obvious from the steps above, heartbeat mechanism degrades performance. To avoid this degradation some installations of Hadoop MapReduce have flag to set heartbeat mechanism to minimize the degradation. For example in Intel Hadoop, flag ‘mapreduce.tasktracker.outofband.heartbeat’ has been introduced as an option to allow TaskTrackers to send a heartbeat on task-completion to improve job latency.

There are several other ways to optimize MapReduce jobs. It is important to optimize as we are dealing with huge volume of data. While running MapReduce jobs sometimes we face resource constraints for example while running MapReduce in clouds environment we pay as per usage of resources. Sometime we require results more quickly to fulfill processing objectives. MapReduce jobs are often chained with more jobs so a deficient MapReduce job has cascading effect on the complete chain as they are related with one another.

The MapReduce model is to break jobs into tasks and run the tasks in parallel to make the overall job execution time smaller than it will otherwise be if the tasks ran sequentially. This makes job execution time dependent on slow running tasks making the whole job take significantly longer time than it will take otherwise.

Tasks may be slow for various reasons, including hardware degradation or configuration issues. Causes may be difficult to find as the tasks still complete successfully with a longer time than expected. Hadoop doesn’t fix slow-running tasks; rather, it detects when a task is running slower than expected and launches similar, equivalent, task as a backup. This is called *speculative execution* of tasks.

Speculative task is launched after all the tasks for a job are launched. Task, that has been running for some time and has failed to make average progress of other tasks associated with the job, is launched for speculative execution. When a task completes successfully, duplicate task if any that is running, is killed as that is not needed. If the original task completes before the speculative task, then the speculative task is killed else the original is killed.

Speculative execution is actually an optimization and not a feature to run jobs more reliably. If there are bugs that cause undesired outcome, then user cannot rely on speculative execution to avoid these bugs, since the same bugs will affect the speculative task.

There are several monitoring facilities available in Hadoop; these include logging, counters, and metrics, provide historical data that can be used to monitor

whether the cluster is providing the expected level of performance, and to help with debugging and performance tuning. Hadoop counters and metrics are useful channels for gathering statistics about a job for quality control, application-level statistics, and problem diagnosis. [3]

Some projects have applied MapReduce-inspired techniques to build a traditional relational database, but most have focused on improving MapReduce execution performance. Traditional database query optimizations are B+ Trees for selections and column-store-style techniques for projections, etc. MapReduce often does not apply them because free form user code of MapReduce makes it difficult to implement. [4]

OPTIMIZATION THROUGH CONFIGURATION OF ENVIRONMENT

There are around 200 configurable parameters in Hadoop. These parameters primarily relate to:

- The number of map tasks in job. Each task processes one split of the input data. These tasks may run in multiple slots based on the number of map execution slots available.
- The number of reduce tasks.
- Memory allocation to each map task to buffer its outputs.
- Memory allocation to each reduce task to buffer its inputs.
- Multiphase external sorting to group map output values by key.
- Should the output data from the map/reduce tasks be compressed before being written to disk? If Yes then how.
- Should the program-specified combiner function be used to pre-aggregate map outputs before their transfer to reduce tasks?

20 configuration parameters which are important ones from optimization view point are listed in table below:

Configurable Parameter	**Description**
dfs.block.size	Specifies the size of data blocks in which the input data set is split
dfs.replication	Specifies level of replication. By default it is 3.
io.sort.mb	The size of in-memory buffer (in MBs) used by map task for sorting its output
io.sort.factor	The maximum number of streams to merge at once when sorting files. This property is also used in reduce phase. It's fairly common to increase this to 100
io.sort.record.percent	Fraction of io.sort.mb for storing metadata for every key-value pair stored in the map-side buffer
io.sort.spill.percent	Usage threshold of map-side memory buffer to trigger a sort and spill of the stored key-value pairs
mapred.compress.map.output	Specifies whether to compress output of maps
mapred.map.tasks.speculative.execution	When a map task runs very slowly than expected due to hardware degradation or inappropriate software configuration, the Job Tracker runs another equivalent task as a backup on another node (i.e. speculative execution).
mapred.tasktracker.map.tasks.maximum	The maximum number of map tasks that will be run simultaneously by a task tracker
mapred.tasktracker.reduce.tasks.maximum	The maximum number of reduce tasks that will be run simultaneously by a task tracker
mapred.job.reuse.jvm.num.tasks	The maximum number of tasks to run for a given job for each JVM on a TaskTracker. A value of –1 indicates no limit: the same JVM may be used for all tasks for a job
mapred.reduce.parallel.copies	The number of threads used to copy map outputs to the Reducer
mapreduce.combine.class	The (optional) Combiner function to pre-aggregate map outputs before transfer to reduce tasks
mapred.reduce.slowstart.completed.maps	Proportion of map tasks that need to be completed before any reduce tasks are scheduled
mapred.reduce.tasks	Number of reduce tasks
mapred.job.shuffle.input.buffer.percent	% of reduce task's heap memory used to buffer output data copied from map tasks during the shuffle
mapred.job.shuffle.merge.percent	Usage threshold of reduce-side memory buffer to trigger reduce-side merging during the shuffle
mapred.inmem.merge.threshold	Threshold on the number of copied map outputs to trigger reduce-side merging during the shuffle
mapred.job.reduce.input.buffer.percent	% of reduce task's heap memory used to buffer map output data while applying the reduce function

min.num.spills.for.combine	Minimum number of spill files to trigger the use of Combiner during the merging of map output data

COST BASED OPTIMIZATION TO SELECT CONFIGURATION PARAMETER SETTINGS

Cost Based Optimization [3] is a model to asses benefits with respect to costs incurred and is worthwhile to be covered here.

Let us Consider a MapReduce job j = (p, d, r, c) that runs program p on input data d and cluster resources r using configuration parameter settings c. Job j's performance can be represented as: perf = F(p, d, r, c) Here, perf is some performance metric of interest for a job (e.g. execution time) that is captured by the cost model F. Optimizing the performance of program p for given input data d and cluster resources r requires finding configuration parameter settings that give near-optimal values of perf. [3]

MapReduce program optimization poses following challenges compared to conventional database query optimization:
Black-box map and reduce functions: Map and reduce functions are usually written in programming languages like Java, Python, C++, and R that are not restrictive or declarative like SQL. Thus, the approach of modeling a small and finite space of relational operators will not work for MapReduce programs.
Lack of schema and statistics about the input data: Almost no information about the schema and statistics of input data may be available before the MapReduce job is submitted. Furthermore, keys and values are often extracted dynamically from the input data by the map function, so it may not be possible to collect and store statistics about the data beforehand.
Differences in plan spaces: The execution plan space of configuration parameter settings for MapReduce programs is very different from the plan space for SQL queries. [3]
Cost-based Optimizer is for finding good configuration settings automatically for arbitrary MapReduce jobs. Two other components introduced are: a Profiler that instruments unmodified MapReduce programs dynamically to generate concise statistical summaries of MapReduce job execution; and a What-if Engine to reason about the impact of parameter configuration settings, as well as data and cluster resource properties, on MapReduce job performance. [3]

Profiler: The Profiler is responsible for collecting job profiles. A job profile consists of the dataflow and cost estimates for a MapReduce job j = (p, d, r, c): dataflow estimates represent information regarding the number of bytes and key-value pairs processed during j's execution, while cost estimates represent resource usage and execution time.
The Profiler makes two important contributions. First, job profiles capture information at the fine granularity of phases within the map and reduce tasks of a MapReduce job execution. This feature is crucial to the accuracy of decisions made by the What-if Engine and the Cost-based Optimizer. Second, the Profiler uses dynamic instrumentation to collect run-time monitoring information from unmodified MapReduce programs. The dynamic nature means that monitoring can be turned on or off on demand; an appealing property in production deployments. [3]

What-if Engine: The What-if Engine is the heart of cost-based optimization. Apart from being invoked by the Cost-based Optimizer during program optimization, the What-if Engine can be invoked in standalone mode by users or applications.
For example, consider question WIF1 from Table below. Here, the performance of a MapReduce job j = (p, d, r, c) is known when 20 reduce tasks are used. The number of reduce tasks is one of the job configuration parameters. WIF1 asks for an estimate of the execution time of job j0 = (p, d, r, c0) whose configuration c0 is the same as c except that c0 specifies using 40 reduce tasks. The MapReduce program p, input data d, and cluster resources r remain unchanged. The What-if Engine's novelty and accuracy come from how it uses a mix of simulation and model-based estimation at the phase level of MapReduce job execution. [3]

	What-if Questions on MapReduce Job Execution
WIF1	How will the execution time of job j change if I increase the number of reduce tasks from the current value of 20 to 40?
WIF2	What is the new estimated execution time of job j if 5 more nodes are added to the cluster, bringing the total to 20 nodes?
WIF1	How much less/more local I/O will job j do if map output compression is turned on, but the input data size increases by 40%?

Cost-based Optimizer (CBO): For a given MapReduce program p, input data d, and cluster

resources r, the CBO's role is to enumerate and search efficiently through the high dimensional space of configuration parameter settings, making appropriate calls to the What-if Engine, in order to find a good configuration setting c. The CBO uses a two-step process: (i) subspace enumeration, and (ii) search within each enumerated subspace. The number of calls to the What-if Engine has to be minimized for efficiency, without sacrificing the ability to find good configuration settings. Towards this end, the CBO clusters parameters into lower-dimensional subspaces such that the globally-optimal parameter setting in the high-dimensional space can be generated by composing the optimal settings found for the subspaces. [3]

OPTIMIZATION DURING VARIOUS PHASES OF JOB EXECUTION

Optimization in job before running: The data which is of no use in processing is filtered out. Compression is done to reduce traffic across network (e.g. traffic of data containing key value pairs). We may choose to compress incoming file for transmit and un-compress as needed. In such case compression/un-compression algorithms need to be efficient. Some times MapReduce programs can process compressed data.
There may be privacy requirements with respect to data and hence it is encrypted. In such cases data needs decryption before MapReduce processing. This may be additional processing for MapReduce which should be critically evaluated whether such encryption/ decryption could be avoided in MapReduce processing.
Task should be mapped on a node where the input data resides in HDFS (Hadoop Distributed File System). This is known as the *data locality optimization* since it doesn't use valuable cluster bandwidth. MapReduce job should ideally do smallest function i.e. does one simple process rather doing multiple processes. These simple MapReduce jobs should be chained efficiently for optimization.

Optimization while loading data: Often distributed Cache (Public or Private) is used with each node. This facilitates look up type of data to mapper and thus optimizes data processing.
Optimization during Map phase of job: Complex MapReduce jobs are broken into simple jobs. Logging and Counters features assist in understanding what happens in MapReduce jobs (mapper as well as reducers). We can enable various logging and counters through MapReduce API. We can also allow MapReduce API to skip error data. We can setup debugging and unit testing to have visibility on what is occurring during MapReduce processing.
Other optimization is monitoring and tuning for optimal spill ratio. When the contents of the buffer reach a certain threshold size, which is defined by io.sort.spill.percent, default 80%, a background thread will start to *spill* the contents to disk. Map outputs are continued to be written to the buffer while the spill takes place. If the buffer fills up in this process, the map blocks until the spill completes. This depends on type of Map task being performed. Goal is to keep number of spill records equal to number of map output records. Parameter io.sort.spill.percent can be tuned to make this happen.

Comparison of types is crucial for MapReduce. In its sorting phase, keys are compared with one another. To optimize this Hadoop provides RawComparator extension of Java's comparator.

There may be more than one representation, or mapping, for a language. All languages support a dynamic mapping, which can be used even when the schema is not known ahead of run time. Java calls this the *generic* mapping.
In addition, the Java and C++ implementations can generate code to represent the data for an Avro schema. Code generation, which is called the *specific* mapping in Java, is an optimization that is useful when we have a copy of the schema before we read or write data. Generated classes also provide a more domain-oriented API for user code than generic ones.
Java has a third mapping, the *reflect* mapping, which maps Avro types onto preexisting Java types, using reflection. It is slower than the generic and specific mappings, and is not good for new applications.

The parameter mapred.job.reuse.jvm.num.tasks specifies the maximum number of tasks to run for a given job for each JVM launched. This defaults to 1. No distinction is made between map and reduce tasks, but tasks from different jobs are run in separate JVMs. The method setNumTasksToExecutePerJvm() on JobConf can also be used to configure this property.
Tasks that are CPU-bound may also benefit from task JVM reuse by taking advantage of runtime optimizations applied by the HotSpot JVM. After running for some time, the HotSpot JVM builds up enough information to detect performance-critical sections in the code and dynamically translates the

Java byte codes of these hot spots into native machine code.
For long-running processes this works fine, but JVMs that run for seconds or a few minutes may not gain the full benefit of HotSpot. In these cases to optimize, it is better to enable task JVM reuse. [2]

In the map-side join case, where the two tables are bucketed in the same fashion, a mapper which processes a bucket of the left table knows that the matching rows in the right table are in its corresponding bucket, so it needs to only retrieve that bucket to affect the join. This optimization works, if the number of buckets in the two tables is multiples of each other. They don't need to have exactly same number of buckets.
To optimize further, data within a bucket should be sorted by one or more columns. This makes efficient map-side joins, because the join of each bucket becomes an efficient merge-sort. [2]

Optimization during Reduce phase of job: Any map outputs that were compressed (by the map task) have to be decompressed in memory in order to perform a merge on them. When all the map outputs have been copied, the reduce task moves into the merge *phase*, which merges the map outputs in the sorted order. This is accomplished in rounds.
For example, if there are 50 map outputs, and the *merge factor is* 10 then there will be 5 rounds. Each round will merge 10 files into one, so in the end there will be five intermediate files. Here Merge factor is controlled by the *io.sort.factor*, just like in the map's merge and the merge factor defaults to 10.
Rather than having a final round that merges these five files into a single sorted file, the merge saves a access to disk by directly feeding the reduce function in what is the last phase: the *reduce phase*. This final merge can be from a mix of in-memory and on-disk segments. [2]

To optimize we split the process into multiple reducers. Reducer threshold is configured to increase efficiency of reducer phase. Many times local reducer is applied to pre-aggregate on each mapper. This local reducer associated with mapper should neither try producing output which is to be produced by final reducer job nor impact the output of final reducer job.

Post process after processing is complete: When a reduce task is finished, Hadoop will try to close the RecordWriter. In this case, the process of closing may take a long time, because we will like to optimize the index before closing. During this time, Hadoop may conclude that the task is hung, since there are no progress updates, and it may attempt to kill it. For this reason, we first start a background thread to give progress updates, and then proceed to perform the index optimization. Once the optimization is completed, we stop the progress updater thread. The output index is now created, optimized, and is closed, and ready for use. [2]

CONCLUSION

Some optimization techniques are covered here. The technique which is to be applied in a particular situation varies per inputs and what we want to achieve. Performance of MapReduce jobs can be increased without increasing the hardware cost, by just tuning some parameters and optimizing programs as summarized above.

References

[1] Apache Hadoop. http://hadoop.apache.org

[2] Tom White. *Hadoop: The Definitive Guide, O' Reilly*

[3] H. Herodotou and S. Babu. Profiling, What-if Analysis, and Cost-based Optimization of MapReduce Programs. Proc. of the VLDB Endowment, Vol 4 No 11

[4] E. Jahani, M. J. Cafarella, and C. R´e. Automatic Optimization of MapReduce Programs. PVLDB, 4:386–396, 2011

[5] SHadoop: Improving MapReduce performance by optimizing job execution mechanism in Hadoop clusters, Rong Gu, Xiaoliang Yang, Jinshuang Yan, Yuanhao Sun, Chunfeng Yuan, Yihua Huang, J. Parallel Distrib. Comput. 74 (2014)

[6] Yahoo! Hadoop Tutorial

Survey on large scale networks based on Software defined networking (SDN)

Sumit Sharma
Ajay Kumar Garg Engineering College, Ghaziabad(U.P)
er.sumitsharma10@gmail.com

Abstract- **The explosion of mobile devices and content, server virtualization, and advent of cloud services are among the trends driving the networking industry to reexamine traditional network architectures. Many conventional networks are hierarchical, built with tiers of Ethernet switches arranged in a tree structure. This design made sense when client-server computing was dominant, but such a static architecture is ill-suited to the dynamic computing and storage needs of today's enterprise data centers, campuses, and carrier environments. Some of the key computing trends driving the need for a new network paradigm include:**

INTRODUCTION

Software-defined networking (SDN) is a network architecture that decouples the control and data planes, moving the control plane (network intelligence and policy making) to an application called a controller [1]

The fast growth of the Internet outside of research facilities led to the formation of large networks, turning the interest of researchers and developers in deploying and experimenting with new ideas for network services. However, it quickly became apparent that a major obstacle towards this direction was the high complexity of managing the network infrastructure. Network devices were used as black boxes designed to support specific protocols essential for the operation of the network, without even guaranteeing vendor interoperability. Therefore, modifying the control logic of such devices was not an option, severely restricting network evolution. To remedy this situation, various efforts focused on finding novel solutions for creating more open, extensible and programmable networks [5].
The first years of the 2000s saw major changes in the field of networking. New technologies like ADSL emerged, providing high-speed Internet access to consumers. At that moment it was easier than ever before for an average consumer to afford an Internet connection which could be used for all sorts of activities, from e-mail and teleconference services to large file exchanges and multimedia. This mass adoption of high-speed Internet and of all the new services that accompanied it had cataclysmic effects for networks, which saw their size and scope increase along with traffic volumes. Industrial stakeholders like ISPs and network operators started emphasizing on network reliability, performance and quality of service and required better approaches in performing important network configuration and management functions like routing, which at the time were primitive at best. Additionally, new trends in the storage and management of information like the appearance of cloud computing and the creation of large data centers made apparent the need for virtualized environments, accompanied by network virtualization as a means to support their automated provisioning, automation and orchestration. A result of this technological shift was the emergence of new improved network programmability attempts, with the most prominent example being SDN.

SDN means different things to different constituencies. For some, it's the networking manifestation of what Marc Andreessen terms "software eating the world." The main aim is to replace proprietary management and control technology and overpriced switches and routers with commodity hardware built from merchant silicon under the direction of centralized controllers running on virtual servers, themselves running on commodity hardware. In other words we can also say that SDN isn't just a low-level packet-pushing technology; it's about creating platforms for applications, configuration management and control that enhance network automation and agility, ultimately lowering operational costs. In this construct, SDN enables network service chains that extend to the top of the

network stack, "using software to virtually insert services into the flow of network traffic."

SDN encompasses low-level switching optimization and high-level application orchestration. When SDN gets in touch with private clouds, it enables fully virtualized data centers [2].

Software-defined networking (SDN) is an approach to computer networking that allows network administrators to manage network services through abstraction of lower-level functionality. This is done by eliminating the coupling of the system that makes decisions about where traffic is sent through the control plane from the underlying systems that forward traffic to the selected destination that relates the data plane. That's how the networking can be simplified. As a communication between control plane and data plane has to be established, to achieve the process SDN requires some method for the control plane to communicate with the data plane. One such mechanism, OpenFlow, is often misunderstood to be equivalent to SDN, in fact the OpenFlow protocol is a foundational element for building SDN solutions [3].

Software-defined networking (SDN) is not just the technology, but as of yet it is largely conceptual -- and those concepts vary depending on the approach. Teh various SDN architectures, OpenFlow, SDN APIs, and overlay networks are being introduced either as if they are interchangeable, or without ever mentioning the other options. It's not surprising that SDN leaves many folks in IT with no clutch of the "definition" at all.
The basis of SDN is virtualization, which in its most simplistic form allows software to run separately from the underlying hardware. Virtualization has made cloud computing possible and now allows datacenters to dynamically provision IT resources exactly where they are needed, on the cloud. To keep up with the speed and complexity of all this split-second processing, the network must also adapt, becoming more flexible and automatically responsive. The idea of virtualization to the network as well, separating the function of traffic control from the network hardware, resulting in SDN.

As virtualization, cloud, and mobility create more complex environments, networks must be able to adapt in terms of security, scalability, and manageability. That's why the legacy networks have serious limitations and old methods that simply will no longer work. Most enterprise networks, however, rely on fixed boxes and appliances requiring a great deal of manual administration. Changing or expanding these networks for new capabilities, applications, or users requires reconfiguration that is time consuming and expensive. Software-defined networks take a lesson from server virtualization and introduce an abstraction layer separating network intelligence and configuration from physical connections and hardware. In this way, SDN offers programmatic control over both physical and virtual network devices that can dynamically respond to changing network conditions using OpenFlow or some other programmable and controllable packet/flow processing protocol. There are several approaches to SDN that can be described: Though the technology is very much in the midst of its development, vendors and industry organizations are working to make the technology open and flexible while adhering to existing Internet standards. At its core, SDN promises to enable network technology innovation and versatility while reducing complexity and administrative overhead.
Software-Defined Network (SDN) has been interested in the field of network management [4].

- It enables flexible and uniform management.
- It has been expected to overcome the issues of network administrations.
- Reduction of human error by reducing human intervention.
- Providing high quality network with small cost by integrating network resource.

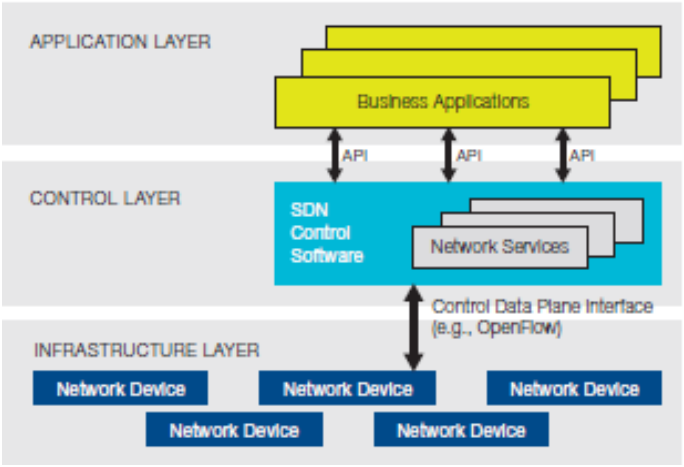


Figure: 2.1 Software Defined Network Architecture

ARCHITECTURE

SDN architecture consists of three layers. At the top is the application layer, which includes applications that deliver services, such as switch/network virtualization, firewalls, and flow balancers. These are abstracted from the bottom layer, which is the underlying physical network layer. In between lies the SDN controller, the most critical element of SDN.

The controller removes the control plane from the network hardware and runs it as software, but must integrate with all the physical and virtual devices in the network. In this way, the controller facilitates automated network management and makes it easier to integrate and administer business applications.

OPENFLOW ENABLES SDN

The OpenFlow protocol, originally developed at Stanford University, is being adopted as the basis of SDN strategies. But OpenFlow is not the only way to do SDN and should not be equated with it. The OpenFlow specification is managed by the Open Networking Foundation (ONF). The goal is to create a common "language" for programming network switches. OpenFlow is used between a controller and a switch to tell the controller about traffic flows and communicate to the switch how to forward those flows. OpenFlow switch is composed of two logical components. The first component contains one or more flow tables responsible for maintaining the information required by the switch in order to forward packets. The second component is an OpenFlow client, which is essentially a simple API allowing the communication of the switch with the controller.

The flow tables consist of flow entries, each of which defines a set of rules determining how the packets belonging to that particular flow will be managed by the switch (i.e. how they will be processed and forwarded). Each entry in the flow table has three fields: i) A packet header defining the flow, ii) An Action determining how the packet should be processed and iii) Statistics, which keep track of information like the number of packets and bytes of each flow and the time since a packet of the flow was last forwarded. Once a packet arrives at the OpenFlow switch, its header is examined and the packet is matched to the flow that has the most similar packet header field. If a matching flow is found, the action defined in the Action field is performed. These actions include the forwarding of the packet to a particular port in order to be routed through the network, the forwarding of the packet in order to be examined by the controller or the rejection of the packet. If the packet cannot be matched to any flow, it is treated according to the action defined in a table-miss flow entry.

The exchange of information between the switch and the controller happens by sending messages through a secure channel in a standardized way defined by the OpenFlow protocol. This way, the controller can manipulate the flows found in the flow table of the switch (i.e. add, update or delete a flow entry) either proactively or reactively as discussed in the basic controller principles. Since the controller is able to communicate with the switch using the OpenFlow protocol, there is no longer a need for network operators to interact directly with the switch.

OpenFlow first gained popularity with service providers including Google, and many hardware and software vendors, including Alcatel-Lucent, Brocade, Cisco, Dell, F5, HP, Juniper Networks, NEC, Plexxi, and VMware, support it as members of the ONF. The foundation has not released the standard as an open source spec, but instead allows members to license it for use in products.

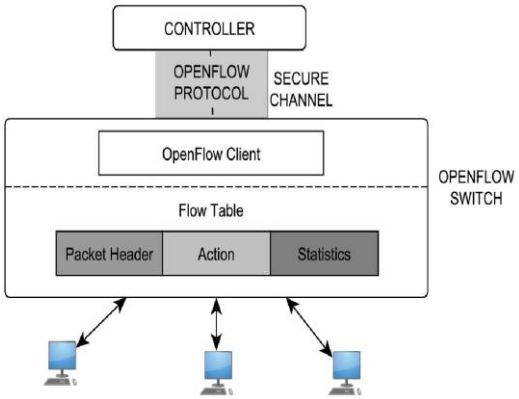


Fig. 3.1 The open flow model

SDN USING APIs

The Application programming interfaces (APIs) are an alternate way to provide the abstraction necessary for SDN along with a highly programmable infrastructure. APIs provide a channel by which instructions can be sent to a device to program it. Programmers can read API documentation to understand the device and code the appropriate commands into their applications. In SDN, APIs are called "northbound" or "southbound," depending on where they function in the architecture.

APIs that reside on a controller and are used by applications to send instructions to the controller are northbound, because the communication takes place north of the controller. Southbound APIs reside on network devices such as switches. These are used by the SDN controller to provision the network, with the communication taking place south of the controller.

SDN NETWORK OVERLAY

Another SDN option is a network overlay. In this case, rather than building an entire logical SDN network from

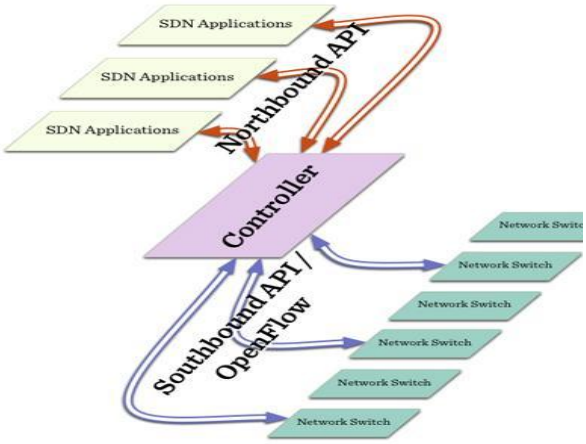


Figure 4.1 SDN using APIs

scratch, the SDN implementation is built as an overlay in order to leverage a physical network that already exists. The overlay is created using virtual switches inside hypervisors. These set up tunnels that make use of the underlying physical network, but don't need to actually configure the hardware to send traffic to its destination.
Emerging protocols including VXLAN, STT, and NVGRE make this possible by using network encapsulation. Several vendors, most notably VMware, offer overlay network solutions.

BENEFITS OF SDN

Why should SDN be considered, especially if it is still in development? The technology has the potential to make significant improvements to service request response times, security, and reliability. It could also reduce costs by automating many processes that are currently done manually and by allowing IT departments to replace (at least in some cases) high-margin devices with commodity hardware. SDN architecture is:

- *Directly programmable*: Network control is directly programmable because it is decoupled from forwarding functions.
- *Agile*: Abstracting control from forwarding lets administrators dynamically adjust network-wide traffic flow to meet changing needs.
- *Centrally managed*: Network intelligence is (logically) centralized in software-based SDN controllers that maintain a global view of the network, which appears to applications and policy engines as a single, logical switch.
- *Programmatically configured*: SDN lets network managers configure, manage, secure, and optimize network resources very quickly via dynamic, automated SDN programs, which they can write themselves because the programs do not depend on proprietary software.
- *Open standards-based and vendor-neutral*: When implemented through open standards, SDN simplifies network design and operation because instructions are provided by SDN controllers instead of multiple, vendor-specific devices and protocols.

The other benefits of applying the SDN principles in different types of networks, the unification of heterogeneous environments and the wide number of applications that this paradigm offers demonstrate its very high potential to become a major driving force commercially in the very near future especially for cloud-service providers, network operators and mobile carriers. It remains to be seen whether these predictions will be confirmed and to what extent SDN will deliver its promises.

CONCLUSION

Having seen the basic concepts of SDN and some important applications of this approach, the impact of SDN to the research community and the industry can be seen easily. While the focus of each interested party might be different, from designing novel solutions exploiting the benefits of SDN to developing SDN enabled products ready to be deployed in commercial environments, their involvement in the evolution of SDN helps in shaping the future of this technology.
Seeing what the motivation and the focus of current SDN-related attempts will provide us with indications of what will potentially drive future research in this field. By applying SDN principles the various organisations are able to choose the networking hardware according to the features it required, while it managed to develop innovative software solutions.

References

[1] White Paper Software-Defined Networking: Why We Like It and How We Are Building On It

[2] 2.http://www.networkcomputing.com/networking/sdn-vendor-comparison-launches/d/d-id/1234183?

[3] http://en.wikipedia.org/wiki/Software-defined_networking

[4] an implementation model and solutions for stepwise introduction of SDN By HIROKI NAKAYAMA

[5] fgfffggg

[6] McKeown, Nick, et al. "OpenFlow: enabling innovation in campus networks." ACM SIGCOMM Computer Communication Review 38.2 (2008): 69-74.

[7] Campbell, Andrew T., et al. "Open signaling for ATM, internet and mobile networks (OPENSIG'98)." *ACM SIGCOMM Computer Communication Review* 29.1 (1999): 97-108.

[8] Tennenhouse, David L., et al. "A survey of active network research." *IEEE Communications Magazine*, 35.1 (1997): 80-86.

[9] Van der Merwe, Jacobus E., et al. "The tempest-a practical framework for network programmability." *IEEE Network* 12.3 (1998): 20-28.

[10] "Devolved Control of ATM Networks," Available from http://www.cl.cam.ac.uk/research/srg/netos/old-projects/dcan/.

[11] Qadir, Junaid, Nadeem Ahmed, and Nauman Ahad. "Building Programmable Wireless Networks: An Architectural Survey." *arXiv preprint arXiv:1310.0251* (2013).

[12] Feamster, Nick, Jennifer Rexford, and Ellen Zegura. "The road to SDN." *ACM Queue* 11.12 (2013): 20-40.

Performance Enhancement through Adaptive Queue Management in MMDSR for MANET

Anupama Sharma
Ajay Kumar Garg Engg. College, Ghaziabad, India
anupama0027@gmail.com

Dr. Abhay Bansal
ASET, Amity University, Noida, India
abansal1@amity.edu

Dr. Vinay Rishiwal
IET, MJP Rohilkhand University, Bareilly, India
vrishiwal@mjpru.ac.in

***Abstract* - Communication technology is increasing very repidly now a days. Mobile users utilizes video streaming for e-learning and storing multimedia data. Vedio streming in MANET is having many issues and challenges. The most significant problems in video conferencing are the unpredictable nature of wireless medium and mobile networks in terms of bandwidth, end-to-end delay and loss variations. Our analysis is to find out an efficient procedure of vedio streming. We are assuming MMDSR as a base algorithm then intruducing AAQM with that to minimize the delay and packet loss. AAQM is a light weight algorithm aimed at maximizing the flow of packets through the router, by continuously computing the quotient between the number of arriving and departing packets. The algorithm applies probabilistic marking of incoming packets to keep the quotient between arriving and departing packets just below 1 to minimize the queue length and maximize the throughput. Minimizing the queue length means minimizing the delay and packet loss. This concept named AQM-MMDSR can enhance the performance of vedio streming in MANET.**

Keywords— MANET, AAQM, MMDSR.

INTRODUCTION

Mobile Ad hoc Network (MANET) has been an active area of researches for the last few years. The driving force behind all these researches is to provide the customers with the network support "at anywhere and at any time". MANETs are self-organizing and self-configuring. No infra-structure is needed to build and administer MANETs. It works in a multi-hop fashion. A mobile node not only transmits its own packets but also forwards packets for other mobile nodes [1][2]. MANETs have become a popular subject of active researches as the usages of the notebooks and 802.11/Wi-Fi network have become widespread [2]. In this modern age mobile modules (i.e., laptop, mobile phones, and PDA) have shown great improvements in terms of performance and memory capacity [6]. Advancements in technology have made it possible to utilize these small, mobile and wireless modules suitable for the formation and maintenance of MANETs at utmost efficiency [2],[5],[6]. Consequently, MANETs must adapt dynamically to be able to maintain on-going communications in spite of these changes [3]. MANETs may be used in a great variety of scenarios, such as universities, museums, emergency rescue or exploration missions, where video-streaming services are likely to be used. Here in this paper we have given an idea to modify MMDSR algorithm by introducing AAQM, which is a light weight algorithm aimed at maximizing the flow of packets through the router, by continuously computing the quotient between the number of arriving and departing packets. The

algorithm applies probabilistic marking of incoming packets to keep the quotient between arriving and departing packets just below 1 to minimize the queue length and maximize the throughput. Minimizing the queue length means minimizing the delay and packet loss.

A lot of studies have been done on Mobile Adhoc Network to improve its performance using different protocols. In this paper, we are presenting a combined concept of adaptive active queue management and multipath multimedia dynamic source routing to enhance the performane of vedio streming in mobile adhoc network. Paper is organized as follows: Section I discusses the introduction of video streaming over MANET. Section II provides the brief description of related works found in the literatures. Section III presents descriptions of the proposed concept. Section IV presents conclusion and future work.

RELATED WORK

Addressing video streaming performance in MANETs from different perspectives can be found in the literatures. In [7] the authors evaluate the performance of H.264 protocol using two routing protocols namely Neighbor-Aware Cluster Head (NACH) and Dynamic Source Routing (DSR) protocols.

Recently, many researchers have focused their efforts on providing mechanisms to improve the MAC (Medium Access Control) level to make configuration parameters evolve dynamically depending on events of the Ad Hoc network. Some proposals modify the MAC parameters to provide dynamic service differentiation based on access categories that modify the contention window sizes used in the back-off algorithm [8–10]. The proposal [11] dynamically adjusts the backoff interval according to the priority and collision rate to arrange a fair scheduling mechanism to access the medium. Proposal [12] has the same goal although based on modifying the waiting times of the stations to access the medium, resulting in a fair and efficient scheme. A dynamic TXOP (Transmission Opportunity) allocation in IEEE 802.11e is proposed in [13] to enhance the QoS experienced in the network. Similarly, in [14] the TXOP value dynamically changes depending on the number of packets remaining to be sent in the buffers. A sensing backoff algorithm is presented in [15], where every node modifies its backoff interval according to the results of the sensed channel activities.

PROPOSED CONCEPT

Formal description

This part contains a more formal description regarding how the AAQM algorithm works . The goal of the AAQM algorithm is to keep the packet arrival rate as close to the packet departure rate as possible in order to maximize the flow of packets through the queue. The packet arrival rate is determined by the end systems sending packets and can for this reason be controlled by probabilistic marking of arriving packets. The packet departure rate is determined by the packet size and bandwidth of the outgoing link. The packet arrival rate is denoted by A and the packet departure rate is denoted by B, both of which are measured over T seconds. The utilization U of the flow of packets through the queue is defined by following equation

$$U = A/B,\ B \neq 0$$

If in the equation above , $U>1$ the queue grows, which can result in a queue overflow and packet loss. Similarly, if, in the equation above , $U<1$ the queue shrinks, which could result in a link underutilization and wasted bandwidth. Therefore to maximize the flow, U should be as close to 1 as possible. The required benefit is that when $U=1$ a packet arrives for each departing packet causing the link to be fully utilized, and if U is just below 1 the queue will simultaneously shrink minimizing both loss and delay. Now, if the total running time of the algorithm is divided into N non-overlapping time slots of size T seconds then the utilization of each time slot n is given by following equation

$$Un = An/\ Bn,\ Bn \neq 0,\ n = 1... N$$

Now the packet marking probability P will be adjusted depending on the value of U during each time slot n . If $U>1$ then P can be increased to reduce the arrival rate and thus decrease U. Likewise, if $U<1$ then P can be decreased to increase the arrival rate and thus increase U. Following equation shows how the packet marking probability is adjusted.

$$P\ n + 1 = P\ n + f\ (\ U\ n\ ),\ n = 1... N$$

$$P\ 0 = 0$$

The function f is given by the next equation and, depending on U, increases or decreases the

packet marking probability P.

$$f(x) = \{ -P \text{ for } x < 1 \text{ and } P\,2 \text{ for } x > 1$$

P1 and P2 are constants that need to be determined beforehand.

MMDSR, is the algorithm in which we are going of apply this AAQM concept, this MMDSR uses extension of DSR as a routing protocol to find available path in the network. In this scenario the number of path should not exceed more than three paths at a same time, due to excessive overhead increase and small improvement. According to our framework, there are three paths and three type of frame (I, P and B) which a priority defined for each frame. The most important video coded frame (I–frame) send through the best path, while the second important frame (P -frame) send through second

best path and then the last frame which is B-frame send through the last path. In case of two paths, I frames would send through the best path and then P and B frame send through the second available path. And if there is only one path available , all the frames should be sending together through the same available path. So we see that there are many queues of frames if these queue can be maintained efficiently then sure the performance of this protocol can be enhanced, which is our main aim.

CONCLUSION AND FUTURE WORK

Concept of AAQM is introducted with MMDSR algorithm this will enhance the performance of MMDSR. AAQM actively manage the queues on routers hance reduce packet loss and delay which is critical QoS parameters in video streaming, so performane will definitely enhance. In future work we will try to implement the proposed concept so that the purpose of this work can be shown with proof.

References

[1] S. Corson and J. Macker. “Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Consideration”, available at http://www.ietf.org/rfc/rfc2501.txt

[2] E.M. Royer, C-K. Toh, “A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks”, IEEE Personal Communications Magazine, April 1999, pp. 46-55. Traffic”, In Proceedings of the 8th International Multi topic Conference, 2004, pp. 516-521.

[3] S. Corson and J. Macker. “Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Consideration”, available at http://www.ietf.org/rfc/rfc2501.txt

[4] IEEE 802.11e standard with Quality of Service enhancements, http://standards.ieee.org/ get ieee 802/ download/802.11e-2005.pdf

[5] A. Shrestha, F. Tekiner. “On MANET Routing Protocols for Mobility and Scalability” In the Proceedings of the International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT 2009), Higashi Hiroshima, Japan, 8-11, December 2009, pp. 451-456.

[6] H. Tafazolli, “A Survey of QoS Routing Solutions for Mobile Ad Hoc Networks”, IEEE Communications Surveys & Tutorials, Vol. 9, No. 2, pp. 50–70, 2007.

[7] Carlos T. Calafate, M. P. Malumbres, P. Manzoni,” Performance of H.264 compressed video streams over 802.11b based MANETs,” In the Proceedings of the 24 th International Conference on Distributed Computer System Workshops, March 2004, pp. 776-781

[8] Choi, E., Lee, W., & Shih, T. (2007). Traffic Flow based EDCF for QoS enhancement in IEEE 802.11e wireless LAN. In 21st Int. conference on advanced networking and applications.

[9] Nafaa, A., Ksentini, A., & Mehaoua, A. (2005). SCW: sliding contention window for efficient service differentiation in IEEE 802.11 networks. In IEEE Communications Society, WCNC.

[10] Gannoune, L., Robert, S., Tomar, N., & Agarwal, T. (2004). Dynamic tuning of the maximum contention windows (Cwmax) f or enhanced service differentiation in IEEE 802.11 wireless adhoc networks. In Vehicular technology conference, VTC2004, pp. 2956–2961.

[11] Ferng, H., Liau, H., & Juang, J. (2007). Fair scheduling mechanism with QoS consideration for the IEEE 802.11e Wireless LAN. National Taiwan University of Science and Technology. Taipei: Taiwan.

[12] Razafindralambo, T., & Guérin-Lassous, I. (2008). Increasing fairness and efficiency using the MadMac protocol in ad hoc networks. Ad Hoc Networks, Vol. 6, Issue 3. Amsterdam: Elsevier.

[13] Andreadis, A., & Zambon, R. (2007). QoS enhancement with dynamic TXOP allocation in IEEE 802.11e. In IEEE PIMRC.

[14] Muhamad, Z., Suzuki, T., & Tasaka, S. (2007). A multimedia priority dynamic scheduling scheme for audio-video transmission with user-level QoS guarantee by IEEE 802.11e HCCA. In I EEE PIMRC.

[15] Haas, Z., & Deng, J. (2003). On optimizing the backoff interval for random access schemes. IEEE Transactions on Communications, 51(12), 2081–2090.

Artificial Neural Networks for Pattern Recognition

Parul Gupta
Ajay Kumar Garg Engineering College, UP
parulgupta182@gmail.com

Rashmi Tyagi
Ajay Kumar Garg Engineering College, UP
rashmityagi0007@gmail.com

Abstract- **Among the various techniques that have come so far in the field of pattern recognition the statistical approach has been most intensively studied and practiced.**

And recently, the advancements in artificial neural network techniques for pattern recognition have been receiving significant attention. Artificial Neural Network can be viewed as computing models whose architecture and function are similar to that of the biological neural network consisting of many hundreds of simple processing units wired together in a computing system communication network. These models are expected to deal with problem solving in a manner different from conventional computing system with the means of creating a distinction between pattern and data to emphasize the need for developing pattern processing systems to address pattern recognition tasks.

The objective of this paper is to introduce the basic principles of ANN, present an overview of the current well-known approaches based on artificial neural networks for solving various pattern recognition problems. From the overview it will be evident that the current approaches are still far short of our expectations and experience, and there is great scope for creating better models inspired by the principles of operation of our biological neural network.

Keywords. Artificial neural network; pattern recognition;

INTRODUCTION

The current technologies like Artificial Intelligence systems, knowledge-based systems, expert systems etc., work in areas of computing science concerned with designing intelligent computing systems that exhibit the characteristics similar to human behavior in performing some simple tasks. In these tasks we look at the performance of a machine and compare it with the performance of a person. We attribute intelligence to the machine if the performances match. However, the term intelligence is not very well defined and therefore, has been less understood. Consequently tasks associated with intelligence such as learning, intuitions, creativity and inference do not lead to the intended meaning.

The way the tasks are performed by a machine and a human being are very different from each other as human intelligence comes from the fact that they perceive everything as a *pattern,* whereas for a machine all are *data.* Even in daily life any data consisting of integers (like telephone numbers, bank account numbers, car numbers), humans tend to see a pattern and store it in the same form. Recalling the data is also fed from a stored pattern. If there is no pattern, then it is very difficult for a human being to remember and recall the data later. Thus storage and recall operations in humans and machines are performed by different mechanisms. The pattern nature in storage and recall automatically gives robustness and fault tolerance for a human system.

BASIC CONCEPT OF ANN

Artificial neural network is an information processing paradigm that is inspired by the way biological nervous system process information. The key

element of this paradigm is the nobel structure of the information processing system. The main focus behind designing an artificial neural network (ANN) is to design a computing system that can behave and function exactly like a biological neural network and perform complex tasks by remembering patterns.

The main characteristics of neural networks include their ability to learn complex nonlinear input-output patterns, use sequential training procedures, and adapt themselves to the data. During training, the network is trained to associate input pattern with outputs. A pattern could be a fingerprint image, a handwritten cursive word, a human face, or a speech signal etc. Now, the given input pattern may belong to one of the two classes:

Supervised classification (e.g., discriminant analysis) in which the input pattern is identified as a member of a predefined class, or

Unsupervised classification (e.g., clustering) in which the pattern is assigned to a hitherto unknown class.

The characteristic differences in information handling by human beings and machines, and in their functions for understanding and recognizing information in the form of patterns and data have led us to identify several pattern recognition tasks which human beings perform naturally and effortlessly but the machine does not for which we have no simple algorithms to implement these yet tasks on a machine

Q. **Pattern association**: Pattern association involves storing a set of patterns or pattern pairs in such a way that when test data are presented, the pattern or pattern pair corresponding to the data is recalled.

   This is purely a memory function performed for patterns and pattern pairs. Typically, it is desirable to recall the correct pattern even though the test data are noisy or incomplete. The problem of storage and recall of patterns is called auto association.

   Since this is content addressable memory function, the system should recall the stored pattern closest to the given input. So, is also necessary to store as many patterns or pattern pairs as possible in a given system as the test data are generated from the same source as the training data in an identical manner.

d. **Pattern mapping**: In pattern mapping, given a set of input patterns and the corresponding output pattern or class label, the objective is to capture the implicit relationship between the patterns and the output, so that when a test input is given, the corresponding output pattern or the class label is retrieved. The system performs some kind of generalization as opposed to memorizing the information which can also be viewed as a pattern classification problem belonging to supervised learning category. Typically, in this case the test patterns belonging to a class are not the same as the training patterns, although they may originate from the same source. Pattern mapping generally displays interpolative behavior, whereas pattern classification displays accretive behavior.

III. **Pattern grouping**: In this case, given a set of patterns, the problem is to identify the subset of patterns possessing similar distinct features and group them together. Since the number of groups and the features of each group are not explicitly stated, this problem belongs to the category of unsupervised learning or pattern clustering. Note that this is possible only when the features are unambiguous as in the case of hand-printed characters or steady vowels. In the pattern mapping problem the patterns for each group are given separately, and the implicit, although distinct, features have to be captured through the mapping. In pattern grouping on the other hand, patterns belonging to several groups are given, and the system has to resolve the groups. Moreover, in that case the test data are also generated from an identical source as the training data.

IV. **Feature mapping**: In several patterns the features are not unambiguous. In fact the features vary over a continuum, and hence it is

difficult to form groups of patterns having some distinct features. In such cases, it is desirable to display the feature changes in the patterns directly. This again belongs to the unsupervised learning category. In this case what is learnt is the feature map of a pattern and not the group or class to which the pattern may belong.

V. **Pattern variability**: There are many situations when the features in the pattern undergo unspecified distortions each time the pattern is generated by the system. This can be easily seen in the normal handwritten cursive script. Human beings are able to recognize them due to some implicit interrelations among the features, which themselves cannot be articulated precisely. Classification of such patterns falls into the category of pattern variability task.

WORK DONE

The feed forward neural network was the first and arguably most simple type of artificial neural network devised. In this network the information moves in only one direction — forwards: From the input nodes data goes through the hidden nodes (if any) and to the output nodes. There are no cycles or loops in the network. Feed forward networks can be constructed from different types of units, e.g. binary McCulloch-Pitts neurons, the simplest example being the perceptron. Continuous neurons, frequently with sigmoidal activation, are used in the context of backpropagation of error.

The most commonly used family of neural networks for pattern classification tasks is the feed-forward network, which includes

Multilayer Perceptron and *Radial-Basis Function (RBF) networks*. Another popular network is the *Self-Organizing Map (SOM), or Kohonen-Network*, which is mainly used for data clustering and feature mapping network is used, it identifies the input pattern and tries to output the associated output pattern.

McCulloch-Pitts model (MCP) was the first mathematical model an extremely simple artificial neuron by Warren McCulloch and Walter Pitts, 1943. The inputs could be either a zero or a one. And the output was a zero or a one. And each input could be either excitatory or inhibitory. Now the whole point was to sum the inputs. If an input is one, and is excitatory in nature, it added one. If it was one, and was inhibitory, it subtracted one from the sum. This is done for all inputs, and a final sum is calculated. The activation of a McCulloch Pitts neuron is binary and the neurons are connected by directed weighted paths. A connection path is excitatory if the weight on the path is positive else it's inhibitory. All excitatory connections to a neuron have the same weights. It includes the weights of the inputs. The effect that each input has at decision making is decided by the weights of the input. It has the ability to adapt to a particular situation.

Mcalled perceptrons. The basic concept ultilayer perceptron (MLP) is a network of simple neurons of a single perceptron was introduced by Rosenblatt in 1958. The perceptron computes a single output frommultiple real-valuedinputs by forming a linear combination according to its input weights and then possibly putting the output through some nonlinear activation function. It has four layers comprising of one input layer, two hidden layers and one output layer has been used. The input layer has nineteen (19) neurons (as there are nineteen feature vectors from MFCC processor) and uses linear transfer function. The output layer has one neuron (as binary decision is to be made) and uses linear transfer function. It is trained using back propagation algorithm. The network is trained by using a built in train function .This function trains the network on training data (Supervised Learning).

The learning process involves updating network architecture and connection weights so that a network can efficiently perform a specific classification/clustering task. The increasing popularity of neural network models to solve pattern recognition problems has been primarily due to their seemingly low dependence on domain-specific knowledge and due to the availability of efficient learning algorithms for practitioners to use. In addition, existing feature extraction and classification algorithms can also be mapped on neural network architectures for efficient (hardware) implementation.

The recognition problem here is being posed as a classification or categorization task, where the classes are either defined by the system designer (in supervised classification) or are learned based on the similarity of patterns (in unsupervised classification). self organizing map (SOM) or self-organizing feature map (SOFM) is trained using unsupervised learning to produce a low-dimensional (typically two-dimensional), discretized representation of the input space of the training samples, called a map. Self-organizing maps are different from other artificial neural networks in the sense that they use a neighborhood function to preserve the topological properties of the input space. Like most artificial neural networks, SOMs operate in two modes: training and mapping. "Training" builds the map using input examples while "mapping" automatically classifies a new input vector. A self-organizing map consists of components called nodes or neurons. Associated with each node is a weight vector of the same dimension as the input data vectors, and a position in the map space.

The usual arrangement of nodes is a two-dimensional regular spacing in a hexagonal or rectangular grid. The self-organizing map describes a mapping from a higher-dimensional input space to a lower-dimensional map space. The procedure for placing a vector from data space onto the map is to find the node with the closest (smallest distance metric) weight vector to the data space vector.

SOM may be considered a nonlinear generalization of Principal components analysis (PCA). It has been shown, using both artificial and real geophysical data, that SOM has many advantages over the conventional feature extraction methods such as Empirical Orthogonal Functions (EOF) or PCA.

Originally, SOM was not formulated as a solution to an optimization problem. Nevertheless, there have been several attempts to modify the definition of SOM and to formulate an optimization problem which gives similar results.

DEVELOPMENTS

Interactive Voice Response (IVR) with pattern recognition based on Neural Networks was proposed by Syed Ayaz Ali Shah, Azzam ul Asar and S.F. Shaukat in 2009. It made use of various techniques including Mel Frequency Cepstral Coefficient (MFCC) and Multi Layer Perceptron (MLP).

Xinyu Guo, Xun Liang & Xiang Li proposed a stock price pattern recognition approach based upon the artificial neural network.

Shahrin Azuan Nazeer, Nazaruddin Omar, Khairol Faisal Jumari and Marzuki Khalid (2007) used ANN approach in face recognition.

In 2006, ANN method was used for Electrocardiogram (ECG) pattern recognition by Lin He, Wensheng Hou, Xiaolin Zhen and Chenglin Peng.

Young-Sang Han, Seong-Sik Min, Won-Ho Choi and Kyu-Bock Cho (1992) [11] implemented ANN for fault detection of induction motor (IM).

In 1997, Nallasamy Mani and Bala Srinivasan applied artificial neural network approach for optical character recognition (OCR).

A rain attenuation model based on artificial neural network was proposed by Hongwei Yang, Chen He, Wentao Song, Hongwen Zhu in 2000.

CONCLUSION

While investigating the works chronologically we have noticed that though there are some merits and demerits of each individual work the application of ANN in each pattern recognition case always performed better. The computing world has a lot to gain from neural networks because of their ability to learn from examples that makes them flexible and powerful. The parallel architecture gives them very fats computation time which can prove to be very effiective in real-time system

References

[1] ARTIFICIAL NEURAL NETWORKS FOR PATTERN RECOGNITION by B Yegnanarayana

[2] USE OF ARTIFICIAL NEURAL NETWORK IN PATTERN RECOGNITION by Jayanta Kumar Basu, Debnath Bhattacharyya, Tai-hoon Kim

[3] NEURAL NETWORKS by Christos Stergiou and Dimitrios Siganos

[4] PATTERN RECOGNITION AND NEURAL NETWORK by Yann LeCun and Yoshua Bengio

[5] USING NEURAL NETS TO RECOGNIZE HANDWRITTEN DIGITS by Michael Nielsen

[6] A.K. Jain, J. Mao, and K.M. Mohiuddin, "ARTIFICIAL NEURAL NETWORKS: A TUTORIAL"

[7] NEURAL NETWORKS by Simon Hayken

[8] MCCULLOCH PITTS NEURONS by Michael Marsalli

Face Recognition An Application Of Artificial Neural Network And Its Solution

Rupal Grover
Ajay Kumar Garg Engineering College, Ghaziabad, Uttar Pradesh
rups.grover1118@gmail.com

Ritu Nigam
Ajay Kumar Garg Engineering College, Ghaziabad, Uttar Pradesh
ritu.nigam2106@gmail.com

Abstract - Face detection is one of the most relevant applications of image processing and biometric systems. Artificial neural networks (ANN) have been used in the field of image processing and pattern recognition. There is lack of literature surveys which give overview about the studies and researches related to the using of ANN in face detection. Therefore, this research includes a general review of face detection studies and systems which based on different ANN approaches and algorithms. The strengths and limitations of these literature studies and systems were included also.

KeyWords: Face recognition, Neural network, Artificial neural network, the back propagation algorithm,biometrics.

INTRODUCTION

Face recognition is a visual pattern recognition problem. In detail , a face recognition system with the input of an arbitrary image will search in database to output people's identification in the input image. A face recognition system generally consists of four modules as depicted: detection, alignment, feature, extraction, and matching,where localization and normalization are processing steps before face recognition is performed.

Artificial neural networks were successfully applied for solving signal processing problems in 20 years.Researchers proposed many different models of ANN with Tanh activation function is proposed that combines AdaBoost to detect human faces so that face detecting rate is rather high. for face alignment module, a multilayer perceptron (MLP) with linear function is proposed , and it creates 2D local texture model for the active shape model(ASM) local searching . For feature extraction module, a method for combination of geometric feature based method and ICA method in facial feature extraction is proposed . For face matching , a model which combines many artificial neural networks applied for geometric features classification is proposed. this case study demonstrate how to solve face recognition in the neural network paradigm.

Human have been using physical characteristics such as face, voice , gait , etc to recognize each other for thousands of years. with new advances in technology , biometrics has become an emerging technology for recognizing individuals using their biological traits. our face recognition technology uses faces as unique verification information . we offer facial recognition that works in a wide range of operating environment to most common public places. almost in any face recognition application , a face detection stage is needed . although face detection posses also a very challenging problem, ,many techniques have been proposed with enough success to consider face

detection a very mature field of research. however , although it is clear that face detection is far from being solved, it will not be considered in this position paper. face recognition can be divided into two basic applications: identification and verification . In the identification problem, the face to be recognized is unknown and is matched against faces of a database containing known individuals. In the verification problem the system confirms or rejects the claimed identity of the input face.

FACE RECOGNITION PROCESS:-

There are 4 steps in recognition process:-

1. ACQUIRING A SAMPLE:

2.EXTRACTING FEATURES:

3.COMPARISON TEMPLATES:

4.DECLARING A MATCH:

ACQUIRING A SAMPLE*:-* In a complete full implemented biometric system, a sensor takes an observation . the sensor might be a camera and the observation is a snapshot picture in our system, a sensor will be ignored , and a 2D face picture "observation " will supplied manually.

EXTRACTING FEATURES*:-*For this step, the relevant data is extracted from the predefined captured sample.. this is can be done by the use of software where many algorithms are available . The outcome of this step is a biometric template which is a reduced set of data that reprents the unique features of the enrolled user's face.

COMPARION TEMPLATES*:-* This depends on the application at hand. For identification purposes, this step will be a comparison between a given picture of the subject and all the biometric templates stored on a database. For verification , the biometric of the claimed identity will be retrieved an this will be compared to a given picture.

DECLARING A MATCH*:-* The face recognition system will return a candidate match list of potential matches. In this case, the intervention of a human operator will be required in order to select the best fit from the candidate list.

* A facial recognition system is a computer application for automatically identifying or verifying a person from a digital image or a video frame from a video source. One of the ways to do this is by comparing selected facial features from the image and a facial database.

It is typically used in security systems and can be compared to other biometrics such as fingerprint or eye iris recognition systems.

why we choose face recognition over other biometrics?

There are a number of reasons to choose face recognition. This includes the following:

1. It requires no physical inetraction on behalf of the user.

2.It is accurate and allows for high enrolment and verification rates.

3. It does not require an expert to interpret the comparison result.

4. It can use your existing hardware infrastructure, existing, camaras and image capture devices will work with no problems.

5. It is the only biometric that allow you to perform passive identification in a one to many environment.

The face is an important part of you are and how people identify you. except in the case of identical twins, the face is arguably a person's most unique physical characteristics. While humans have the innate ability to recognize and distinguish different faces for million of years, computers are just now catching up.For face recognition there are 2 types of comparasions. the first is verification . This is where the system compares the given individual with who that individual says they are and gives a yes or no decision. The second is identification . This is where the system compares the individual to all the other individuals in the database and gives a ranked list of matches. All identification or authentication technologies operate using the following stages:=

1. CAPTURE: A physical or behavioural sample is captured by the system during enrollment and also in identification or verification process.

2.EXTRACTIONS*:* Unique data is extracted from the sample and a template is created.

3.COMPARISONS:The template is then compared with a new sample.

4.MATCH/NON MATCH: The system decides if the features extracted from a new sample are a match or a non match.

*Face recognition starts with a picture, attempting to find a person in the image. This can be accomplished using several methods including movement , skin tones or blurred human shapes. The face recognition system locates the head and finally the eyes of the individual. A matrix is then developed based on the characteristics of the individuals's face. The method of defining the matrix varies according to the algorithm(the mathematicial process used by the computer to perform the comparison). This matrix is then compared to matrices that are in a database and a similarity score is generated for each comparison.

Artificial intelligence is used to simulate human interpretation of faces. In order to increase the accuracy and adaptibility, some kind of machine learning has to be implemented.

There are essentially 2 methods of capture. One is video imaging and the other is thermal imaging. Video imaging is more commom as standard video cameras can be used. The practise position and the angle of the head and the surrounding lighting conditions may affect the system performance. The complete facial image is usually captured and a number of points on the face position of the eyes, mouth and the nostrils as a example. More advanced technologies make 3D map of the face which multiplies the possible measurements that can be made.

Thermal imaging has better accuracy as it uses facial temperature variations caused by vein structure as the distinguishing traits. As the heat pattern is emitted from the face itself without source of external radiations these systems can capture images despite the lighting conditions, even in the dark.

Face recognition technologies have been associated generally with very costly top secure applications. Today the core technologieshave evolved and the cost of equipments is going down dramatically due to the integration and the increasing processing power. Certain application of face recognition technology are cost effective, reliable and highly accurate. As a result there are no technological or financial barriers for stepping from the pilot project to widespread deployment.

ALGORITHMS USED FOR FACE RECOGNITION: Algorithms measure key points of the face (nose, eyes,mouth,jaw,etc), head angle, skin tone,lighting,and create a template based on these measurements. the file is then compared to other files(still photos or video captures) that are enrolled into software's database, searching for a match based on the "similarity rating" percentage.The closer the characteristics match, the higher the similarity rating. The software can also identify individuals over time for various facial expressions.

Face recognition software allows a user to create their own biometric face identification security for Windows.

The software uses a neural network Back Propogation Algorithm combined with more Artificial Intelligence tool added for imaging optimization

ADVANTAGES OF FACE RECOGNITION:-

- Simultaneous multipleface processing.
- Live face detection.
- Face image quality determination.
- Multiple samples of the same face.
- Fast face matching.

PROBLEMS AND SOLUTION:

Face recognition has been and will continue to be a very challenging and difficult problem. inspite of the great work done in the last 30 years, we can be sure that the face recognition research community will have work to do during, atleast, the next 30 years to

completely solve the problem. Strong and coordinated effort between the computer visions , signal processing and psychophysics and neurosciences communities are needed.

Face recognition is a both challenging and important recognition technique. Among the biometric techniques, face recognition approach possesses one great advantage, which is its userfriendliness.In this paper we have given the introductory surveyfor the face recognition technology. We hope that this paper can provide readers better understanding and we encourage the readers who are interested in this topic to go to the references for more detailed study.

CONCLUSION

The computer based face recognition industry has made much useful advancement in the past decade, however , the need for the higher accuracy system remains. Through the determination and commitement of industry , government evolutions and organised standards bodies, growth and progress will continue raising the bar for face recognition system. Computer based face recognition system is very useful for the police, industries, and for government for various security regions.

This project gives a more accuracy than other traditional way of recognize the face and less time consuming. It has numerous applications in areas like surveillance and security control systems , content based image retrieval , video conferencing and intelligent human computer interfaces.

References

[1] W. Zhao, et al (2000) “Face recognition: a literature survey”, Technical Report CAR-TR-948, University of Maryland, October 2000.

[2] Turk M & Pentland A (1991) “Eigenfaces for recognition”, Journal of Cognitive Neuroscience, Vol.3, pp71–86.

[3] Phil Brimblecombe (2002) “Face Detection using Neural Networks”, H615 – Meng Electronic Engineering, School of Electronics and Physical Sciences, URN: 1046063.

[4] Bouchra Abboud, et al (2004) “Facial expression recognition and synthesis based on an appearance model”, Signal Processing: Image Communication, Vol. 19, Issue. 8, pp723-740.

[5] P. Viola & M.J. Jones (2001) “Robust real-time object detection”, Technical Report CRL/2001/01, Cambridge Research Laboratory, USA, February 2001

[6] Ming-Hsuan Yan, et al (2002), “Detecting Faces in Images: A Survey”, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 24, No. 1, pp34-58, January2002

[7] Minyoung Kim, et.al (2008) “Face tracking and recognition with visual constraints in real-world videos”, IEEE Conference on Computer Vision and Pattern Recognition, pp23-28, June.

[8] Brunelli R & Poggio T (1993) “Face recognition: features versus templates”, IEEE Transaction Pattern Analysis and Machine Intelligence, Vol. 15, No.10, pp1042–1052.

Accuracy Evaluation of Recommender System Models

Vidushi
Ajay Kumar Garg Engineering College Ghaziabad, India
vidushiji.v@gmail.com

Rahul Dagar
Goibibo.com, Gurgaon, India
rahuldagar@outllook.com

***Abstract*— The vast and exponentially increasing information on the Internet as well as increasing number of visitors to websites lead to the need new methods that can assist user to find resources of his interest therefore helping them to take some important decisions. Such systems which overcome excess information overload by doing information filtering in accordance with the user's interest and assist him in decision making process are called recommender system. But with the current scenario of so much diversity in data recommender systems needed to face some key challenges. Foremost important among various challenges is producing accurate recommendation while handling vast growth of number of participants efficiently. To address this key challenge many approaches were proposed to develop an accurate recommender system. In this paper we will try and evaluate different algorithms proposed to develop such systems and will analyze their performance on the basis of the accuracy achieved.**

Index Terms— recommender system; accuracy; best fit recommendations;

INTRODUCTION

Nowadays the amount of information generated and retrieved have become increasingly enormous. A huge gap exists in the amount of information being converted to knowledge. This gap exists by having many ways people pour data into the Internet but not many techniques to process the data to knowledge. For example, digital libraries contain tens of thousands of journals and articles [1]. However, it is difficult for users to pick the valuable resources they want. Therefore there is a need of new technologies that can guide users to take a decision and pick a resources of interest among the huge pool of information available.

One of the most successful such technologies is the Recommender system. Recommender systems are gaining popularity both commercially and in the research community, where many algorithms have been suggested for providing recommendations. These algorithms typically perform differently in various domains and tasks. Therefore, it is important from the research perspective, as well as from a practical view, to be able to decide on an algorithm that matches the domain and the task of interests [5].

Applications of Recommender Systems

Recommender systems can now be found in many modern applications that expose the user to a huge collections of items. Such systems typically provide the user with a list of recommended items they might prefer, or supply guesses of how much the user might prefer each item. These systems help users to decide on appropriate items, and ease the task of finding preferred items in the collection [5].

Recommender systems have become serious business tools that are re-shaping the world of E-commerce.

For example, The Book Matcher feature of Amazon allows customers to give direct feedback about books they have read. Customers rate books they have read on a 5-point scale from

"hated it" to "loved it." After rating a sample of books, customers may request recommendations for books they might like. At that point a half dozen non-rated texts are presented which correlate with the user's indicated tastes [8]. The DVD rental provider Netflix1 displays predicted ratings for every displayed movie in order to help the user decide which movie to rent. The problem of identifying and recommending individuals who have expertise to solve a specific problem is an important application of recommender systems [3].

An application designer who wishes to add a recommendation system to her application has a large variety of algorithms at her disposal, and must make a decision about the most appropriate algorithm for her application. Typically, such decisions are based on offline experiments, comparing the performance of a number of candidate algorithms over real data. The designer can then select the best performing algorithm, given structural constraints [5].

Security and Privacy Issues to Recommender Systems

Privacy Risks: In most systems, users need to register before they can enjoy personalized recommendation. The registration process often requires them to provide some personal information like their names, birth dates, postal code and email.

Since not every user want their information to be disclosed or misused, the recommender should then protect itself against exposition of users' information or misuse of that information [1].Shilling Attack*:* In cases where anyone can provide recommendations, people may give tons of positive recommendations for their own materials and negative recommendations for their competitors [2].

Another type of attack that may affect recommender is the so called Sybil attack in which a dishonest user may create multiples users account in other to improve the recommendation of another user or another item [1].

LITERATURE SURVEY ON VARIOUS RECOMMENDATION APPROCHS

A recommender can provide personalized recommendation (recommend things based on the individual's past behaviour), Social recommendation (recommend things based on the past behaviour of similar users) and Item recommendation (recommend things based on the item itself). Recommender system can be built with many approaches. Some of them are listed below:

e. Random prediction algorithm is an algorithm that randomly chooses items from the set of available items and recommends them to the user. Since the item's selection is done randomly, the accuracy of the algorithm is based on luck; the greater the number of items is the chance of good selection lowers. Random prediction has a great probability of failure. Thus, it has never been taken seriously by any researcher or vendor and only serves as reference point, helping to compare the quality of the results obtained by the utilization of a more sophisticated algorithm [1].

f. Frequent sequences can help build recommender systems. For example, if a customer frequently rates items we can use the frequent pattern to recommend other items to him. The only problem is that this method will only be efficient after the customer makes minimum purchases [1].

g. Collaborative filtering is the most successful approaches to building recommender systems. It uses the known preferences of a group of users to make recommendations or predictions of the unknown preferences for other users. The fundamental assumption of *CF* is that if users *X* and *Y* rate *n* items similarly, or have similar behaviors (e.g., buying, watching, listening), and hence will rate or act on other items similarly [9]. *CF* techniques use a database of preferences for items by users to predict additional topics or products a new user might like. In a typical *CF* scenario, there is a list of *m* users *{u*1, *u*2, . . . , *um}* and a list of *n* items *{i*1, *i*2, . . . , *in}*, and each user, *ui*, has a list of items, *Iui*, which the user has rated, or about which their preferences have been inferred through their behaviors. The ratings can either be explicit indications, and so forth, on a 1–5 scale, or implicit indications, such as purchases or click-through [7].

Before we can understand how CF algorithms work, we need to understand this similarity.

Similarity

In computer science, a similarity measure or similarity function is a real-valued function that quantifies the similarity between two objects. Although no single definition of a similarity measure exists, usually similarity measures are in some sense the inverse of distance metrics .Hence there is not a single way to calculate and find the similarity or dissimilarity among various objects.

Some of them are discussed
below. Euclidean Distance

The basis of many measures of similarity and dissimilarity is Euclidean distance. The distance between vectors X and Y is defined as follows:

$$d(x,y) = \sqrt{\sum_{i}^{n} (x_i - y_i)^2}$$

In other words, Euclidean distance is the square root of the sum of squared differences between corresponding elements of the two vectors. Note that the formula treats the values of X and Y seriously: no adjustment is made for differences in scale. Euclidean distance is only appropriate for data measured on the same scale. As you will see in the section on correlation, the correlation coefficient is (inversely) related to the Euclidean distance between standardized versions of the data.

Euclidean distance is most often used to compare profiles of respondents across variables. For example, suppose our data consist of demographic information on a sample of individuals, arranged as a respondent-by-variable matrix. Each row of the matrix is a vector of *m* numbers, where *m* is the number of variables. We can evaluate the similarity (or, in this case, the distance) between any pair of rows. Notice that for this kind of data, the variables are the columns. A variable records the results of a measurement. For our purposes, in fact, it is useful to think of the variable as the measuring device itself.

Jaccard similarity

The Jaccard similarity (Jaccard 1902, Jaccard 1912) is a common index for binary variables. It is defined as the quotient between the intersection and the union of the pairwise compared variables among two objects.

Equation

$$d^{JAS}(i,j) = \frac{J11}{J01 + J10 + J11}$$

In the equation d^{JAD} is the Jaccard distance between the objects *i* and *j*. For two data records with *n* binary variables *y* the variable index *k* ranges from 0 to *n*-1. Four different combinations between $y_{i,k}$ and $y_{j,k}$ can be distinguished when comparing binary variables. These combinations are (0/0), (0/1), (1/0) and (1/1). The sums of these combinations can be grouped by:

- J_{01}: the total number of variables being 0 in y_i and 1 in y_j.
- J_{10}: the total number of variables being 1 in y_i and 0 in y_j.
- J_{11}: the total number of variables being 1 in both y_i and y_j.
- J_{00}: the total number of variables being 0 in both y_i and y_j.

As each paired variable belongs to one of these groups it can be easily seen that:

$J_{00} + J_{01} + J_{10} + J_{11} = n$. As the Jaccard similarity is based on joint presence, J_{00} is discarded.

Cosine Similarity

The cosine similarity between two vectors (or two documents on the Vector Space) is a measure that calculates the cosine of the angle between them. This metric is a measurement of orientation and not magnitude, it can be seen as a comparison between documents on a normalized space.What we have to do to build the cosine similarity equation is to solve the equation of the dot product for the $\cos\theta$

$$\text{similarity} = \cos(\theta) = \frac{A \cdot B}{\|A\|\|B\|} = \frac{\sum_{i=1}^{n} A_i \times B_i}{\sqrt{\sum_{i=1}^{n} (A_i)^2} \times \sqrt{\sum_{i=1}^{n} (B_i)^2}}$$

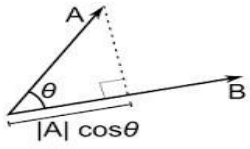


Fig 1

And that is it, this is the cosine similarity formula. Cosine Similarity will generate a metric that says how related are two documents by looking at the angle instead of magnitude. The similarity measure discussed above needs any object to be first converted as vector.

To get started with that first we need to generate a thesaurus which is a set of all unique tokens. After that every document is converted into vector form. Each document vector length is equivalent to the total number of unique tokens in the thesaurus and each element in the document vector is used to store weight value associated with the corresponding token [13]. To find these weights, tf*idf technique is used due to its successful and wide-scale application in the past.

Term frequency, Tik, for the document i and the term k, is the number of times term k appears in the document divided by total number of words in the document. Each T_{ik} is then computed. The modulation of the frequency involved multiplying with a `correcting' factor Ik, the inverse document frequency. It is calculated using log (N/nk), where N is the total number of documents in a representative document base in which n documents contain the term k. For example consider a document containing 100 words wherein the word *cow* appears 3 times [14]. Following the previously defined formulas, the term frequency (TF) for *cow* is then (3 / 100) = 0.03. Now, assume we have 10 million documents and *cow* appears in one thousands of these. Then, the inverse document frequency is calculated as log (10 000 000 / 1 000) = 4. The tf*idf score is the product of these quantities: 0.03 × 4 = 0.12. In this way all the documents are reduced into their vector forms.

Some algorithms compute the similarity between users, others look at the similarity between items, others at the similarity between categories of items. On this basis the collaborative filtering techniques can be further categorized as:

User-based Collaboration Filter In this model, following steps are taken:

(d) Find a group of users that is “similar” to user X

(e) Find all all items liked by this group that hasn’t been seen by user X

(f) Rank these items and recommend to user X

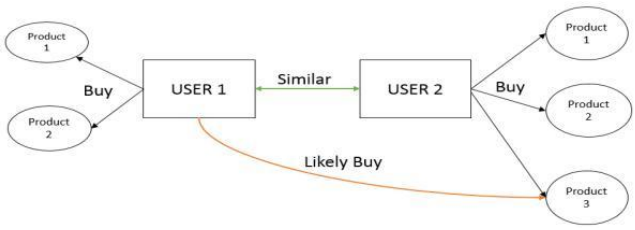


Fig 2

This introduces the concept of user-to-user similarity, which is basically the similarity between 2 row vectors of the user/item matrix. The algorithm considers that users who are similar (have similar attributes) will be interested on same items [10]. User based algorithms are three steps algorithm; the first step is to profile every user in order to find which ones are similar to the target user, the second step is to compute the union of the items selected by these users and associate a weight with each item based on its importance in the set and the third and final step is to select and recommend items that have the highest weight and have not been already selected by the active user [9]. The most important step is the first one; creating the union of items liked by others or selecting the most important of them is easily done when the set of similar users is known [11]. Thus the overall performance of the algorithm will depend on the method used to find users that are similar to the target user. There are many methods by which it can be done. The k-Nearest Neighbors algorithm is the most used because of its efficiency [9].

Item-based Collaboration Filter If the user/item matrix is transposed and then item to item similarity is computed and following steps were undertaken:

a) Find the set of items that user X likes (from interaction data)

b) Find a group of items that is similar to these set of items that we know user X likes

c) Rank these items and recommend to user X

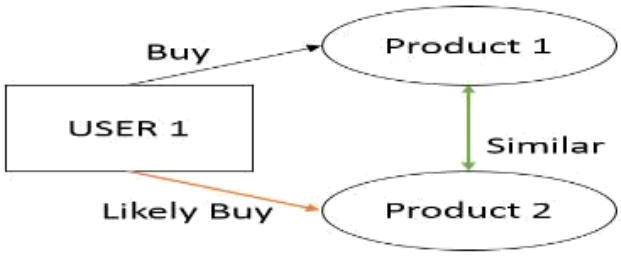


Fig 3

Item-based algorithms are two steps algorithms; in the first step, the algorithms scan the past information of the users; the ratings they gave to items are collected during this step. From these ratings, similarities between items are built and inserted into an item-to-item matrix M. The element xij of the matrix M represents the similarity between the items in row i and the item in column j. Afterward, in the final step, the algorithms selects items that are most similar to the particular item a user is rating.

d) Content based algorithms are algorithms that attempt to recommend items that are similar to items the user liked in the past. They treat the recommendation's problem as a search for related items. Information about each item is stored and used for the recommendations. Items selected for recommendation are items that content correlates the most with the user's preferences. For example, whenever a user rated an items, the algorithm constructs a search query to find other popular items by the same author, artist, or director, or with similar keywords or subjects. Content based algorithms analyze item descriptions to identify items that are of particular interest to the user [1].

REAL LIFE IMPEMENTATIONS AND ITS CHALLENGES

Amazon.com

We focus on recommender systems in the *book* section of Amazon.com.

Customers who bought: Like many E-commerce sites, Amazon.com™ (www.amazon.com) is structured with an information page for each book, giving details of the text and purchase information. The Customers who Bought feature is found on the information page for each book in their catalog. It is in fact two separate recommendation lists. The first recommends books frequently purchased by customers whom purchased the selected book. The second recommends authors whose books are frequently purchased by customers who purchased works by the author of the selected book [8].

It has used Item-based Collaboration Filter technique for recommendation. It suggest other products a customer might be interested in based on a single other product that customer has expressed interest in. These systems are Automatic and Ephemeral, since they require neither action from nor identification of the customer.

Book Matcher: The Book Matcher feature allows customers to give direct feedback about books they have read. Customers rate books they have read on a 5-point scale from "hated it" to "loved it." After rating a sample of books, customers may request recommendations for books they might like. At that point a half dozen non-rated texts are presented which correlate with the user's indicated tastes. Feedback to these recommendations is provided by a "rate these books" feature where customers can indicate a rating for one or more of the recommended books [8].

Book matcher is different, since it is triggered by the user asking for recommendations by giving the ratings to various books read explicitly and then asking for recommendations on that basis. This type of recommendation approach can be said as Manual because it requires some customer effort.

CDNOW

Album Advisor: The Album Advisor feature of CDNOW™ (www.cdnow.com) works in two different modes. In the single album mode customers locate the information page for a given album. The system recommends 10 other albums related to the album in question. In the multiple artist mode customers enter up to three artists. In turn, the system recommends 10 albums related to the artists in question [8].

This type of recommendation comes under manual attribute based recommendation. Attribute based recommender systems recommend products to customers based on syntactic properties of the products. The above example where the user has to input the name of the artists, which is an example of an attribute-based recommendation. Attribute-based recommendations are often manual, since the customer must directly request the recommendation by entering his desired syntactic product properties.

My CDNOW: My CDNOW enables customers to set up their own music store, based on albums and artists they like. Customers indicate which albums they own, and which artists are their favorites. Purchases from CDNOW are entered automatically into the "own it" list. Although "own it" ratings are initially treated as an indication of positive likes, customers can go back and distinguish between "own it and like it" and "own it but dislike it." When customers request recommendations the system will predict 6 albums the customer might like based on what is already owned. A feedback option is available by customers providing an "own it," "move to wish list" or "not for me" comment for any of the albums in this prediction list. The albums recommended change based on the feedback [8].

This type of recommendation is a content based recommendation in which user profiling is done and on the basis of the content of the profile, recommendations are further suggested. In the current scenario the user profiling is done on the basis of "own it" history which is further filtered as mentioned above.

EBay

Feedback Profile: The Feedback Profile feature at eBay.com™ (www.ebay.com) allows both buyers and sellers to contribute to feedback profiles of other customers with whom they have done business. The feedback consists of a satisfaction rating (satisfied/neutral/dissatisfied) as well as a specific comment about the other customer. Feedback is used

to provide a recommender system for purchasers, who are able to view the profile of sellers. This profile consists of a table of the number of each rating in the past 7 days, past month, and past 6 months, as well as an overall summary (e.g., 867 positives from 776 unique customers). Upon further request, customers can browse the individual ratings and comments for the sellers [8].

This time of recommendation is primarily manual and content based but it involves a concept which is beyond recommendations and that is sentiment analysis and opinion mining. Opinion mining, which is also called sentiment analysis, involves building a system to collect and categorize opinions about a product. In this case it is mining all the reviews and giving a summary in the form of positive or negative or a neutral review.

Challenges to Recommender Systems

Data Sparsity. In practice, many commercial recommender systems are used to evaluate very large product sets. The user-item matrix used for collaborative filtering will thus be extremely sparse and the performances of the predictions or recommendations of the *CF* systems are challenged. The data sparsity challenge appears in several situations, specifically, the *cold start* problem occurs when a new user or item has just entered the system, it is difficult to find similar ones because there is not enough information (in some literature, the *cold start* problem is also called the *new user problem* or *new item problem*. New items cannot be recommended until some users' rate it, and new users are unlikely given good recommendations because of the lack of their rating or purchase history [2].

As illustrated above, taking the example of amazon.com and cdnow.com even active users purchase only 1% of the total products therefore leading to sparsity problem (for e.g. 1% of 2 million books is 20,000)

Scalability. When numbers of existing users and items grow tremendously, traditional CF algorithms will suffer serious scalability problems, with computational resources going beyond practical or acceptable levels [15].

This problem is very general but obvious problem for practical application because of increasing amount of data over the internet, it may be the number of items or the number of users. Synonymy. Synonymy refers to the tendency of a number of the same or very similar items to have different names or entries. Most recommender systems are unable to discover this latent association and thus treat these products differently. For example, the seemingly different items "children movie" and "children film" are actual the same item, but memory-based CF systems would find no match between them to compute similarity [2].

Shilling Attacks. In cases where anyone can provide recommendations, people may give tons of positive recommendations for their own materials and negative recommendations for their competitors [2].Other Challenges: Changing data: The systems are usually biased towards the old and have difficulty showing the recommendations against temporally new data.Changing user preferences: In some domains, for e.g. Entertainment domain, the users' preferences usually change over time, which leads to the difficulty of developing a general-purpose recommender [5].

Content-based filtering (CBF) and collaborative filtering may be manually combined by the end-user specifying particular features, essentially constraining recommendations to have certain content features. More often they are automatically combined, sometimes called a hybrid approach. There are many ways to combine them, and no consensus exists among researchers. However, such systems generally use the content analysis to identify items that meet the immediate need of the user, and use CF to try and capture features like quality that are hard to automatically analyze.[12]

CONCLUSION

Recommender systems are an extremely potent tool utilized to assist the selection process easier for users. Not surprisingly, these systems, while used mainly in the e-commerce shopping world, can also be applied in other fields like academics as well. This paper presented some of the algorithms used to build recommender systems. There is no a silver bullet to deal with all contents' categories and users' behaviors efficiently. Thus, how to develop a recommender system, which can take the advantages of various kinds of recommendation approaches and then efficiently coordinate them to adaptively meet the user's preference according to the contents' characteristics and users' behaviors will be the future concern [4]. In conclusion, recommender systems are powerful systems and are a relatively recent technology and they will only keep improving in the future [1]

REFERENCES

[1] Dhoha Almazro, Ghadeer Shahatah, Lamia Albdulkarim, Mona Kherees, Romy Martinez, William Nzoukou, " A Survey Paper on Recommender Systems", Submitted on 28 Jun 2010, ACM classes: H.3.3, Cite as: arXiv:1006.5278v4 [cs.IR]

[2] Xiaoyuan Su and Taghi M. Khoshgoftaar," A Survey of Collaborative Filtering Techniques," Advances in Artificial Intelligence, Volume 2009, Hindawi Publishing Corporation, August 2009

[3] Magnus Mortensen," Design and Evaluation of a Recommender System", Master's Thesis in Computer Science Faculty of Science Department of Computer Science, University of Troms, Feb. 2007

[4] Huan-Yu Lin, Jun-Ming Su, Yi-Li Liu, Jin-Long Li, Shian-Shyong Tseng, Shien-Chang Tang," OSCAR: an Online SCalable Adaptive Recommender for Improving the Recommendation Effectiveness of Entertainment Video Webshop, Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference, pp. 69-77

[5] Asela Gunawardana, Guy Shani, "A Survey of Accuracy Evaluation Metrics of Recommendation Tasks", Journal of Machine Learning Research - JMLR , vol. 10, pp. 2935-2962, 2009

[6] K. Goldberg, T. Roeder, D. Gupta, and C. Perkins, "Eigentaste: a constant time collaborative filtering algorithm," Information Retrieval, vol. 4, no. 2, pp. 133–151, 2001.

[7] B. N. Miller, J. A. Konstan, and J. Riedl, "PocketLens: toward a personal recommender system," ACM Transactions on Information Systems, vol. 22, no. 3, pp. 437–476, 2004. [8] J. Ben Schafer, Joseph Konstan, John Riedl, "Recommender Systems in E-Commerce," Proceedings of the 1st ACM conference on Electronic commerce, pp 158-156, 1999

[9] Deshpande, M., and Karypis, G. Item-based top recommendation algorithms. ACM Trans. Inf. Syst. 22, 1 (2004), 143–177.

[10] Ghazanfar, M. A., and Prugel-Bennett, A. A scalable, accurate hybrid recommender system. International Workshop on Knowledge Discovery and Data Mining (2010), 94–98

[11] G. R., Sarwar, B., Karypis, G., Konstan, J., and Riedl, J. Analysis of recommendation algorithms for e-commerce. ACM Press, pp. 158–167.

[12] J. Ben Schafer1, Dan Frankowski2, Jon Herlocker3, and Shilad Sen2," Collaborative Filtering Recommender Systems".

[13] J. Mostafa, W. Lam," Automatic classification using supervised learning in a medical document filtering application," Information Processing & Management, Volume 36, Issue 3, pp. 415–444, 1 May 2000.

[14] Lu Zhiqiang, Shao Werimin, Zhenhua, Y.," Measuring Semantic Similarity between Words Using Wikipedia," Web Information Systems and Mining, International Conference, pp. 251-255, 7 November 2009

[15] Urmila Shinde, Rajashree Shedge,"Comparative Analysis of Collaborative Filtering Technique," IOSR Journal of Computer Engineering, Volume 10, Issue 1, pp 77-82, Mar. - Apr. 2013

Hierarchical Routing Protocols in Wireless Sensor Network: A Survey

Tahira Mazumder,
Ajay Kumar Garg Engineering College, Ghaziabad, India.
tahiramazumder@yahoo.co.in

Sushruta Mishra,
Gandhi Engineering College, Bhubaneswar, India.
mishra.sushruta@gmail.com

-

Abstract: **- Considering the limitations in WSNs, such as low computing capacity, small memory, power supply limitations and price, appropriate routing path needs to be selected for transmission of data to the base station. Wireless Sensor Networks (WSNs) are also subject to various kinds of attacks such as replaying of messages, battery exhausting, and nodes compromising. Care is to be taken to ensure that data exchange is done using minimal resources and less communication overheads. To transmit data, the intermediate sensor nodes communicated together and then transmit towards the base station by selecting appropriate routing path decided by the routing protocol governing the network. The goal is to ensure that the base station receives correct and fresh data. This paper studies some important hierarchical routing techniques for WSNs and finally analyzes and compares these techniques.**

Keywords: WSNs, hierarchical routing techniques,

INTRODUCTION

Wireless sensor networks (WSN) consist of a large collection of sensor nodes with each node equipped with sensors, processors and radio transceiver. Large number of sensor nodes can be deployed in a variety of situations capable of performing both military and civilian tasks owing to their low cost. A communication path between the relay nodes is established which further helps in forwarding the data from sensor nodes to the base station by Routing. Routing is one of the biggest challenges faced by wireless sensor network and it becomes more complicated and complex in WSN owing to its dynamic nature, limited battery life, computational overhead, no conventional addressing scheme, self-organization and limited transmission range of sensor nodes [1], [2]and[3].
The time overheads and the amount of data successfully received by Base station from sensors nodes deployed in the network region determine how good the routing protocol is. Number of routing protocols has been proposed for wireless sensor network. Mainly these are three types of routing protocols
1) Flat routing protocols
2) Hierarchical routing protocols
3) Location based routing protocols
This paper discusses some of Hierarchical routing protocols and its characteristics.

DESIGN PARAMETRES DECIDING ROUTING PROTOCOLS:

Wireless sensor networks are expected to fulfill the following requirements because of reduced computing, radio and battery resources of sensors [4] and [5]:
Energy Efficiency: Routing protocols should prolong network lifetime while maintaining a good grade of connectivity to allow the communication between nodes. It is important to note that the battery replacement in the sensors is infeasible since most of the sensors are randomly placed.
Authenticity: The communicating node should have a method of verifying the authenticity of the node with which it is communicating through the key establishment techniques.
Confidentiality: An adversary may try to access the network if it manages to obtain the secret keys to obtain the data. Confidentiality refers to the ability to protect the disclosure of data from unauthorised access. Key establishment techniques should provide confidentiality and in case of a node being compromised, it tries to keep the data from being further known.
Scalability: Key establishment techniques should provide high-security features not only for small networks but also for network of large size. Key

establishment techniques if scalable can support variations in the size of the network.

Integrity: Access to the keys should be available only to the nodes within the network and only the authenticated base station should be allowed to change keys. This would stop unintended nodes from obtaining knowledge about the secret keys or from trying to change it.

Freshness: Freshness implies that receiver receives the recent and fresh data and ensures that no adversary can replay the old data. This requirement is especially important when the WSN nodes use shared keys for message communication, where a potential adversary can launch a replay attack using the old key as the new key is being refreshed and propagated to all the nodes in the WSN [6]. To achieve the freshness the mechanism like nonce or time stamp should add to each data packet.

HIERARCHICAL ROUTING PROTOCOLS

A. Low energy adaptive clustering hierarchy (LEACH)[7]

It is one of the very first hierarchical routing protocol. Since nodes in a network cease to be of any use once its battery dies, the need for such a protocol arose. Here, the sensor nodes will be organizing themselves into local clusters with one of them taking the role of the cluster head (CH).The energy load on the nodes is evenly distributed by randomly rotating the cluster head role. The cluster head collects data from its cluster nodes and then aggregates these collected data which is then sent to the base station. The working of LEACH protocol is based on two rounds, with each round consisting of two phases, the Set up Phase and the Steady Phase.

In the Set up Phase, clusters are formed with some nodes electing themselves as a cluster-head independently from other nodes. These nodes elect themselves on behalf Suggested percentage P and its previous record as cluster-head. Nodes which were not cluster-head in previous 1/p rounds generate a number between 0 to 1 and if it is less then threshold T(n) then nodes become cluster-head. Threshold value is set through this formula.

$$T(n) = \begin{cases} p/1-p*(r \bmod 1/p) & \text{if } n \in G \\ 0 & \text{otherwise} \end{cases}$$

r is the current round; *p*, the desired percentage for becoming CH; and *G* is the collection of nodes not elected as a CH in the last 1/ *p* rounds. The decision takes into account when a node last served as the Cluster Head.

Once the clusters have been created, the Steady phase begins. In its allotted TDMA time slot, nodes communicate to cluster-head or else it turns off its radio thus using minimal energy. The CH aggregates all the received data and transmits to base station. LEACH protocol is very useful for the applications, where constant monitoring is required. TL-LEACH[8], where TL stands for Two-Level is the extension of the LEACH which utilizes two level of clustering where primary CH communicate with secondary CH in order to send the data, for better throughput. Clusters are formed on the basis of minimum distance of nodes to their corresponding CH.

***B** Threshold Sensitive Energy Efficient Sensor Network Protocol (TEEN)[10]*

It's a hierarchical clustering protocol based on threshold values and it is targeted at reactive network. It is mainly designed for time critical applications which are responsive to a sudden change that occurs in the network (eg: temperature). The sensors within a cluster report their sensed data to their CH. The CH sends aggregated data to higher level CH until the data reaches the sink[9].

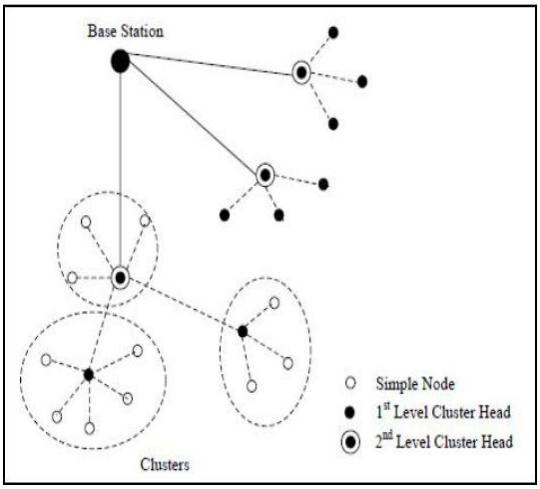


Fig: Hierarchical Clustering in TEEN

In TEEN, the first step involves the formation of clusters. At every cluster change time, in addition to the attributes, the cluster-head broadcasts to its members, broadcasts two threshold values to the nodes in its respective cluster. They are hard and soft thresholds. A Hard Threshold (HT) is a value for the sensed attribute beyond/at which a node switches on its transmitter and reports to its respective cluster head. A Soft Threshold (ST) is a change made in the value of the attribute which induce the node to switch on its transmitter and report data only when the value is beyond HT or the small change in the value is greater than ST. The nodes next transmits data in the current cluster period, only when the current value of the sensed attribute is greater than the hard threshold and the current value of the sensed attribute differs from *SV*, an internal variable that stores the sensed attribute by an amount equal to or greater than the soft threshold. TEEN is

useful for applications where the users can control a trade-off between energy efficiency, data accuracy, and response time dynamically. Also, since message transmission consumes more energy than data sensing, so the energy consumption in this scheme is less than the proactive networks. However, TEEN is not suitable for sensing applications where periodic reports are needed since the user may not get any data at all if the thresholds are not reached.

Adaptive Periodic Threshold-sensitive Energy Efficient Sensor Network Protocol- APTEEN[11]

This protocol was developed by extending the existing TEEN to overcome its drawbacks. Similar to TEEN, APTEEN reacts to the changes in the network and also in architecture but supports capturing periodic data collections (LEACH) and reacting to time-critical events (TEEN). It supports (i) historical query, to analyze past data values, (ii) one-time query, to take a snapshot view of the network; and (iii) persistent queries, to monitor an event for a period of time. It offers a flexibility of allowing the user to set the time interval (TC) and the threshold values for the attributes and the energy consumption can be controlled by the count time and the threshold values. The hybrid network can emulate a proactive network or a reactive network, by suitably setting the count time and the threshold values.

C. Energy Efficient Clustering Scheme (EECS)[12]

EECS extends TL-LEACH by dynamic sizing of clusters based on cluster distance from the base station. CH election is based on the residual energy of the node.

D. Hybrid Energy-Efficient Distributed Clustering- HEED [13]

(HEED) is a multi-hop clustering approach that uses residual energy as the primary parameter and node degree or density (a function of intra-cluster communication cost) as secondary parameter as a metric for cluster selection to achieve power balancing. The primary parameter selects an initial set of CHs and the secondary cluster used to break the ties. When clusters are chosen, a node that produces the lowest intra-cluster communication cost will communicate with the cluster head. This intra-cluster communication cost is measured using the Average Minimum Reachability Power (AMRP) measurement [13]. The AMRP is the average of all minimum power levels required for each node within a cluster range R to communicate effectively with the cluster head i. The AMRP of a node i then become a measure of the expected intra-cluster communication energy if this node is elevated to cluster head. Utilizing AMRP as a second parameter in cluster head selection is more efficient then a node selecting the nearest cluster head [13].

E. Power-Efficient Gathering in Sensor Information Systems – PEGASIS [14]

It is a chain based protocol and guarantees an improvement over LEACH protocol. Chains are formed in two steps, Chain construction and Gathering data. In Chain Construction step, sensor nodes form chains so that each node transmits and receives from a neighbor and only one node is selected from that chain to transmit to the base station. Greedy Algorithm works in the chain construction step starting from the node farthest to the sink. The nearest node to this node is put as the next node in the chain. This procedure continues until all the nodes are included in the chain. A node cannot appear more than once in the chain. When a sensor fails or dies due to low battery power, the chain is constructed using the same greedy approach by bypassing the failed sensor.

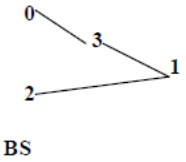


Fig: *Chain construction using the greedy algorithm.*

The above figure shows node 0 connecting to node 3, node 3 connecting to node 1, and node 1 connecting to node 2 in that order.

For gathering data in each round, each node receives data from one neighbor, fuses with its own data, and transmits to the other neighbor on the chain. Nodes take turns transmitting to the BS, and node number *i* mod N (N represents the number of nodes) is used to transmit to the BS in round *i*.

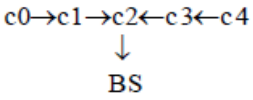


Fig: Chain forming and data gathering in PEGASIS

In Figure 3, node c2 is the leader, and it will pass the token along the chain to node c0. Node c0 will pass its data towards node c2. After node c2 receives data from node c1, it will pass the token to node c4, and node c4 will pass its data towards node c2.

ANALYSIS

LEACH reduces the energy dissipation by reducing the number of transmission to sink using Cluster head and increase the life time of all nodes through randomized rotation being as cluster-head and allowing non-cluster-head nodes to keep sleeping except specific time duration. LEACH routing protocol makes wireless sensor network scalable

and robust. But no particular attention has been given in LEACH to the time criticality of the target application in sensor networks. TEEN protocol aims at energy conservative by making them reactive to changes but the main drawback of it is that the nodes will never get to communicate if the threshold values are not reached. While LEACH works best for Proactive network, TEEN and TEEN is best suited for Reactive network. APTEEN intends to combine proactive and reactive networks by creating a Hybrid network with that and sends data periodically, as well as responds to sudden changes in attribute values. The main drawback of APTEEN is the additional complexity required to implement the threshold functions and the count time. However, this is a reasonable trade-off and provides additional flexibility and versatility. LEACH which transmits data at all times while TEEN and APTEEN does it on the basis of threshold values. PEGASIS eliminates the overhead caused by dynamic cluster formation in LEACH and via data aggregation and hence increases the lifetime of the network twice as much the lifetime of the network under the LEACH protocol. PEGASUS also reduces the amount of energy spent per round because transmit are much less compared to transmitting to a cluster-head in LEACH. PEGASIS still introduce significant overhead because nodes require dynamic topology adjustment to decide where to next route its data. PEGASIS outperforms LEACH by limiting the number of transmissions and dynamic transmission overheads. HEED aims at extending network lifetime, minimizing the energy consumed for selecting cluster head and minimizing the control overhead. The methods in HEED are suitable for prolonging the network lifetime rather than for the entire needs of WSN. HEED cannot guarantee optimal head selection in terms of energy since it uses the secondary parameter to resolve conflicts.

CONCLUSION

Many researchers have proposed many different types of routing protocols for Wireless Sensor Networks (WSNs) which is a very critical issue from the energy efficiency, scalability and data correctness point of view. This paper presents an overview of some of the important protocols proposed in various papers. The choice of choosing a particular routing protocol for the WSN should be based the requirements of that particular application. There are immense research opportunities in this field wireless sensor network. Further study on the security aspects of key management in WSNs will make the wireless sensor networks to be of immense utility in various aspects of life.

REFERENCES

[1] Heinzelman W. B., Chandrakasan A. P., Balakrishnan H., ”An applicationspecific protocol architecture for wireless microsensor networks,” IEEE Trans on Wireless Communications, Vol. 1, No. 4, 2002, pp. 660-670, doi: 10.1109/TWC.2002.804190.

[2] X. H. Wu, S. Wang, ”Performance comparison of LEACH and LEACHC protocols by NS2,” Proceedings of 9th International Symposium on Distributed Computing and Applications to Business, Engineering and Science. Hong Kong, China, pp. 254-258, 2010

[3] P.T.V.Bhuvaneswari and V.Vaidehi ”Enhancement techniques incorporated in LEACH- a survey”Department of Electronics Engineering, Madras Institute Technology, Anna University Chennai, India, 2009.

[4] Yang Xiao, Venkata Krishna Rayi, Bo Sun, Xiaojiang Du, Fei Hu, and Michael Galloway “A Survey of Key Management Schemes in Wireless Sensor Networks”

[5] Navdeep Kaur, Deepika Sharma and Prabhdeep Singh, “Classification of Hierarchical Routing Protocols inWireless Sensor Network: A Survey”, International Journal of P2P Network Trends and Technology- Volume3Issue1- 2013

[6] J. Sen. A survey on wireless sensor network security. International Journal of Communication Networks and Information Security (IJCNIS), 1(2):59–82, August 2009.

[7] V. Loscri, G. Morabito, and S. Marano.A two-levels hierarchy for low-energy adaptative clustering hierarchy (tl-leach). In *Proc. VTC2005*, pages 1809–1813, Dallas (USA), September 2005.

[8] V. Loscri, G. Morabito, and S. Marano, “A Two-Level Hierarchy for Low-Energy Adaptive Clustering Hierarchy”, DEIS Department, University of Calabria.

[9] Khushboo Pawar, Y.Kelkar, A Survey of Hierarchical Routing Protocols in Wireless Sensor Network”, International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 5, May 2012

[10] A. Manjeshwar and D. P. Agrawal, “ TEEN: A Protocol for Enhanced Efficiency in Wireless Sensor Network”, 1st international Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile" Computing, 2001, p.189.

[11] Arati Manjeshwar and Dharma P. Agrawal **“**APTEEN: A Hybrid Protocol for Efficient Routing and Comprehensive Information Retrieval in Wireless Sensor Networks” Proceedings of the International Parallel and Distributed Processing Symposium (IPDPS.02) 2002 IEEE.

[12] M.Ye,C.Li,G.Chen and J.Wu,EECS, “An Energy Efficient Clustering Scheme in Wireless Sensor Networks”, National

Laboratory of Novel Software Technology, Nanjing University, China.
[13] O. Younis and S. Fahmy, “HEED: A Hybrid Energy-Efficient Distributed Clustering Approach for Ad Hoc Sensor Networks”, IEEE Transactions on Mobile Computing, vol. 3, no. 4, Oct-Dec 2004.
[14] S. Lindsey and C. S. Raghavendra. Pegasis: Power-efficient gathering in sensor information systems. In IEEE Aerospace Conference Proceedings, pages 1125–1130, 2002

Video Analytics Using Hadoop & Mapreduce

Satyam Agrawal, Saurabh Tripathi, Shivam Agrawal, Ankur Tripathi
Ajay Kumar Garg Engineering College.
satyam0499@gmail.com

***Abstract*-Today the installation of cctv cameras on road and the video uploaded on social networking sites are growing day by day and the video generated from these activities are doubled in every single year, so there is an difficulty arises to handle huge amount of data.so we develop an efficient and effective way to manage and analyze video data which can be helped in solve bank robbery, traffic analysis and other business aspects. We use BigData and Hadoop technology because BigData and Hadoop reduces manpower, cost and time. Any traditional approach is not able to handle this large amount of data.**

Keywords-BigData, Hadoop, CCTV

INTRODUCTION

Today there is large amount of data is generated from various sources. These sources may be in form of various sensor, CCTV cameras, aircraft, Stock Exchange Sectors, social networking sites.At present the data which is present is approximately 2.75 Zettabytes and there is an estimation that data Will rise to 8 Zettabytes in 2015.This data may be in various forms such as Images, Text, Audio and video. In which the size of video data grows at unpredictable Scale. As the technology grows the quality of video Is also enhancing that's why the size of video which is at Past in Kilobytes now in MB and GB's.

The video data is generated by different sources Like social networking sites, youtube , CCTV cameras, movies and from commercial websites. The traditional technologies which is used to analyse this video data is not efficient in terms of money, time and effort. So we use BIGDATA AND HADOOP technology, which overcomes the disadvantages of past technology by reducing manpower ,cost and time. Due to the distributed architecture of hadoop Framework the data is divided among various nodes so processing speed is quite high.

Parallel & Distributed Processing on Hadoop

There are two main components in Hadoop Framework the first component is HADOOP DISTRIBUTED FILE SYSTEM(HDFS) which is act as a storage of data and the other component is MAPREDUCE which is used for the analysis of data. Both HDFS and mapreduce follows the master and slave architecture in which many slaves are monitored by a single master. There are two subcomponent of HDFS one is namenode which act as a master node and other is datanode which act as a slavenode. In mapreduce Jobtracker act as masternode and taskTracker act as a slave node.**NameNode**: In HDFS cluster there is a single namenode which controls all the datanode present in the cluster. Namenode contains all the metadata which tells which data is stored at which datanode. When a client want to store the data in cluster the client ask to the namenode and namenode tells the client about free datanodes.

(A) **DataNode**: In cluster there are number of nodes which act as a datanode. These datanodes are the actual storage of data.The data is replicated at 3 Different datanodes to ensure the safety of data.

(B) **JobTracker:** In HDFS cluster there is a single Jobtracker which controls all the tasktracker present in the cluster. The Jobtacker assigns the job to the task tracker.And it also perform Job scheduling and Resource allocation.

(C) **TaskTracker:**Tasktracker is act as a slave daemon accepts the task which is assigne by Jobtracker. TaskTracker sends a heartbeat to the jobtracker in every 3 seconds which implies that particular datanode is alive.

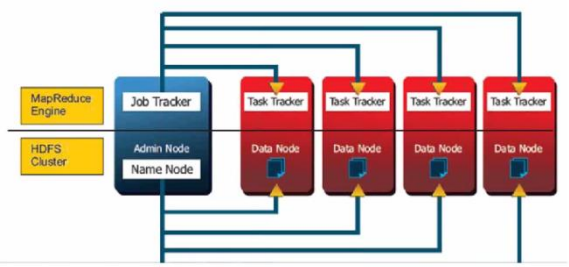


Figure-HDFS and mapreduce components

OPERATIONS PERFORMED DURING VIDEO ANALYTICS USING HADOOP:

There are various steps for the analysis of data which is captured by the CCTV cameras and websites.

(1) **Deploying data Into HDFS cluster:** Our first step is to collect the data from various sources like CCTV and Social networking sites and put this data in our hadoop cluster. The data which is captured by CCTV cameras is sent to our HADOOP processing center by using networking protocol and the data which is on the webserver is transferred by using flume . Flume is a distributed service used for collecting and moving large amounts of log data. It has a flexible architecture which is based on streaming of data.

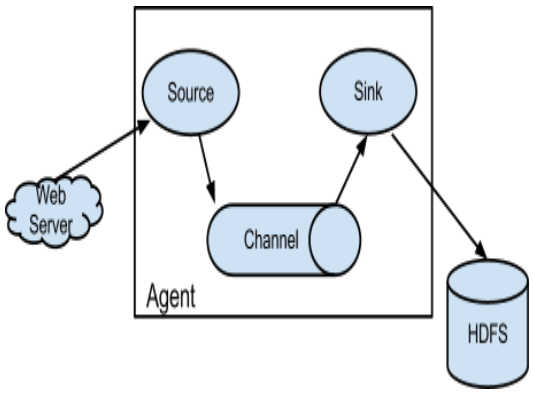


Figure- flume architecture

(2) **Video Transcoding**: JCodec is an pure java implementation of video codecs and formats. It is open source.In digital transcoding we convert the video data into Frames by the help of JCodec ,we can also use Xuggler and other related tools. Now theses images are collected and make a large files because there are lots of frame is available after conversion.These are the code which is used for the conversion of video into frame-

```
int frameNo = 785;
BufferedImage frame1 = FrameGrab.getFrame(new File("sk.mp4"), frameNo);
ImageIO.write(frame1, "png", new File("abc.png"));
```

(3) **Analysis Of Frame by HIPI Framework** –

There are 2 ways to analyze the frame the first way is to convert the image into byteStream and then by the help of sequence file we can analyse the image.But this way requires a lot of effort a and time. The second way to analyse the frame is by using HIPI framework. HIPI is an Framework for Image Processing which was created for data analyst and enable them with an efficient tool by which they can do image processing in an efficient way .This Framework contains a lots of API related to the image processing or frame processing .

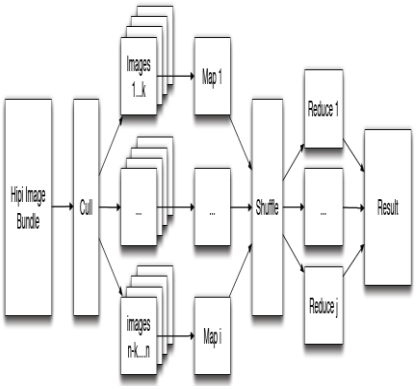


Figure-Hipi architecture

(4) **Store images in a HIPI Image Bundle**: After transcoding the video the images are available these image should be combined into a single large file so that it can easily managed.By the help of addImage method we can add every image into the HIPI imageBundle.So HIPI ImageBundle can be considered as a bunch of Images.

Each mapper will generate a HIPI Image Bundle, and the Reducer will merge all bundles into a single large bundle. By storing images in this way now you are able to work on HIPI framework for our logical part that is MapReduce tasks that you want to perform on image Bundle .

Suppose if you want to calculate the average color value at each pixel then it can be perform in an easy way.

```
Configuration conf123 = new Configuration();

HipiImageBundle hib = new HipiImageBundle(new Path("/path/to/file12.hib"), conf123);


hib.open(AbstractImageBundle.FILE_MODE_WRITE, true);
```

(5)**Analysis Of Images By using HIPI api:**

HipiImageBundle contains a large set of images , before analysis we are dividing the images in a block size of 64MB among various datanodes .Now we analyze the image which is stored on datanode by writing the mapreduce code .

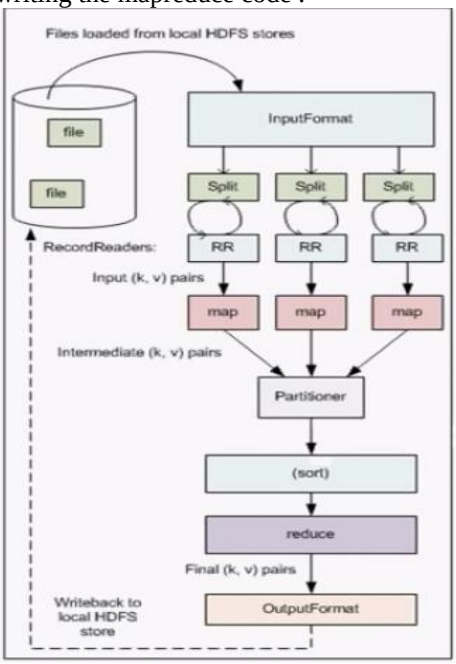


Figure: Simplified view of the MapReduce process for image processing we use the Eclipse Framework ,and add all the external jar's of Hadoop and Hipi .So that it can support all the classes which is required for the analysis of image. We have an image of traffic in which vehicle are run on the road.Then with the help of Mapper we extract the vehicle number, color .And now in the mapper we compare this vehicle number from the valid data which is already stored ,so that we can analyze that the vehicle which is in the image is valid vehicle or a suspicious one.So now all the operation of image processing is complete.

APPLICATIONS

1. CCTV camera video footage analysis helps in women security across the various parts of the country.
2. Video analysis helps in solving the bank robbery.
3. It also helps in traffic analysis so that we provide the necessary solutions to decrease traffic on roads.
4. Video analysis helps in minimizing the road accidents by alarming an signal in nearby hospitals and police stations**.**

CONCLUSION

We have describe how we could ingest video in Hadoop cluster and perform parallel transcoding to create an set of JPEG images by the help of JCodec. And then we combined all the images into a bundle which is known as HIPI ImageBundle .Then we analyze the image stored in the datanode by the help of mapreduce programing. Since We analyze all the frames of the video which driven out some relevant results.By this analysis the extracted information can be used to solve the bank robbery cases, reduce violence against women, traffic on roads and the business forgery.

References

[1] HANCOCK, BADDELEY, AND SMITH,1992.The main components of images. Network: computation in neural systems.

[2] Parallel Image Processing With MapReduce & Performance analysis in fully distributed mode, M.Yamamoto , Kyushu University , K. Kaneko , Kyushu University 2013.

[3] K. Yasushi, & K. Kenichi, Detection of various feature points for computer vision. The Journal of Institute of Electronics, Information & Communication Engineers.