IJCSIS Vol. 10 No. 6, June 2012
ISSN 1947-5500

International Journal of Computer Science & Information Security

Editorial
Message from Managing Editor

*The **International Journal of Computer Science and Information Security** (IJCSIS) is a well-established and notable venue for publishing high quality research papers as recognised by various universities and international professional bodies. IJCSIS is a refereed open access international journal for publishing scientific papers in all areas of computer science research. IJCSIS publishes original research works and reviewed articles in all areas of computer science including emerging topics like cloud computing, software development etc. The journal promotes insight and understanding of the state of the art and trends in computing technology and applications.*

IJCSIS solicits authors/researchers/scholars to contribute to the journal by submitting articles that illustrate research results, projects, surveying works and industrial experiences. IJCSIS helps academia promptly publish academic work to sustain or further one's career.

For complete details about IJCSIS archives publications, abstracting/indexing, editorial board and other important information, please refer to IJCSIS homepage. IJCSIS appreciates all the insights and advice from authors/readers and reviewers. Indexed by the following International Agencies and institutions: Google Scholar, Bielefeld Academic Search Engine (BASE), CiteSeerX, SCIRUS, Cornell's University Library EI, Scopus, DBLP, DOI, ProQuest. Average acceptance for the period January-June 2012 is 25-30%.

We look forward to receive your valuable papers. The topics covered by this journal are diverse. (See monthly Call for Papers). If you have further questions please do not hesitate to contact us at ijcsiseditor@gmail.com. Our team is committed to provide a quick and supportive service throughout the publication process.

A complete list of journals can be found at:

http://sites.google.com/site/ijcsis/

IJCSIS Vol. 10, No. 6, June 2012 Edition

ISSN 1947-5500 © IJCSIS, USA.

Journal Indexed by (among others):

IJCSIS EDITORIAL BOARD

JCSIS

ISSN (online): 1947-5500

Please consider to contribute to and/or forward to the appropriate groups the following opportunity to submit and publish original scientific results.

CALL FOR PAPERS International Journal of Computer Science (IJCSIS)
August-December 2012 Issues

The topics suggested by this issue can be discussed in term of concepts, surveys, state of the art, research, standards, implementations, running experiments, applications, and industrial case studies. Authors are invited to submit complete unpublished papers, which are not under review in any other conference or journal in the following, but not limited to, topic areas.
See authors guide for manuscript preparation and submission guidelines.

Indexed by Google Scholar, DBLP, CiteSeerX, Directory for Open Access Journal (DOAJ), Bielefeld Academic Search Engine (BASE), SCIRUS, Cornell University Library, ScientificCommons, EBSCO, ProQuest and more.

Deadline: see web site
Notification: see web site
Revision: see web site
Publication: see web site

Context-aware systems
Networking technologies
Security in network, systems, and applications
Evolutionary computation
Industrial systems
Evolutionary computation
Autonomic and autonomous systems
Bio-technologies
Knowledge data systems
Mobile and distance education
Intelligent techniques, logics and systems
Knowledge processing
Information technologies
Internet and web technologies
Digital information processing
Cognitive science and knowledge
Agent-based systems
Mobility and multimedia systems
Systems performance
Networking and telecommunications
Software development and deployment
Knowledge virtualization
Systems and networks on the chip
Knowledge for global defense
Information Systems [IS]
IPv6 Today - Technology and deployment
Modeling
Software Engineering
Optimization
Complexity
Natural Language Processing
Speech Synthesis
Data Mining

For more topics, please see web site https://sites.google.com/site/ijcsis/

For more information, please visit the journal website (https://sites.google.com/site/ijcsis/)

TABLE OF CONTENTS

[2]*Ajayi Crowther University, Oyo, Oyo State, Nigeria*
[4]*Mathematics & Statistics Department, Rufus Giwa Polytechnic, Owo, Ondo State, Nigeria*

16. Paper 31081151: Data Mining System For Quality Prediction Of Petrol Using Artificial Neural Network (pp. 90-95)

Omowumi O. Adeyemo, Adenike O. Osofisan, Ebunoluwa P. Fashina, Kayode Otubu
Department of Computer Science, University of Ibadan, Ibadan, Nigeria

Comparison of Data Mining Techniques used to Predict Cancer Survivability

Charles Edeki, Ph.D
Mathematics and Computer Science Department
Mercy College
Dobbs Ferry, NY, USA
cedeki@mercymavericks.edu

Shardul Pandya, Ph.D
School of Business and Technology, Faculty of Information technology
Capella University
Minneapolis, MN, USA
Shardul.Pandya@capella.edu

***Abstract*— Huge efforts are being made by computer scientists and statisticians to design and implement algorithms and techniques for efficient storage, management, processing, and analysis of biological databases. The data mining and statistical learning techniques are commonly used to discover consistent and useful patterns in a biological dataset. These techniques are used in a computational biology and bioinformatics fields. Computational biology and bioinformatics seeks to solve biological problems by combining aspects of biology, computer science, mathematics, and other disciplines [1]. The main focus of this study was to expand understanding of how biologists, medical practitioners and scientists would benefit from data mining and statistical learning techniques in prediction of breast cancer survivability and prognosis using R statistical computing tool and Weka machine learning tool (freely available open source software applications). Six data mining and statistical learning techniques were applied to breast cancer datasets for survival analysis. The results were mixed as to which algorithm is the most optimal model, and it appeared that the performance of each algorithm depends on the size, high dimensionality of data representation and cleanliness of the dataset.**

Keywords- Data Mining, WEKA, R tool, Computational Biology, Bioinformatics

I. INTRODUCTION

The advancement of medicine now relies upon the collection, management, storage, and analysis of large biological datasets. Data mining, statistical and machine learning techniques are the process by which new knowledge is extracted from a dataset. According to [2], the definition of machine learning is as follows: "A computer program is said to learn from experience E with respect to some class of tasks T and performance measure P, if its performance at tasks in T, as measure by P, improves with experience E" (p. 2). Data mining, statistical and machine learning are based on inductive inference, a process of observing a phenomenon, then building a model for that phenomenon and making predictions using the model.

In this study, the results of a comprehensive comparative study of the following data mining, statistical and machine learning algorithms was examined:, Support Vector Machines (SVM);, RandomForest;, AdaBoost, Bagging;, Boosting;, Decision Trees and Artificial Neural Networks (ANN) classifiers algorithms. The main focus of this research was to study the effective classification learning techniques for prediction of breast cancer survivability. In other words, can one algorithm or techniques be more effective at predicting survivability over others.

There are two main aspects in prediction of cancer survivability: accuracy (how true is the algorithm's prediction), and efficiency (how fast can the algorithm execute the prediction task). Data reduction technique was applied to the dataset and obtained a reduced representation of the breast cancer dataset. The resulting data set was much smaller in volume, yet closely maintained the originality of the data [3]. The R PCA function was used to reduce the large dataset (the patients in this case) to smaller components of objects related according to their expression patterns with tumor size.

Classification algorithms are the most common data mining and machine learning algorithms, often used for data analysis in both industry and academia. Classification is a supervised learning algorithm used to map a dataset into predefined groups or classes. The biological datasets from the National Cancer Institute (NCI) biological database system was used to find the prediction rate of each algorithm and comparative

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

studies of the algorithms were performed in order to find the optimal classification model.

R and Weka software were used to analyze the breast cancer dataset. R is open source statistical analysis software and Weka is open source machine learning application software that can be used to normalize and analyze datasets.

II. METHODS

The exponential growth of the amount of biological data available raises two problems: on one hand, efficient information storage and management, and on the other hand, the extraction of useful information from these data. The second problem is one of the main challenges in computational biology, which requires the development of an effective computational analysis tool and is the problem that was presented in this study.

For many studies in medicine, researchers are interested in assessing the time it takes for an event to happen. Very often, the event is an outcome, such as diagnosis or death, but the outcome may also be other measurable parameters, such as onset of disease or relapse of disease. There is a term that describes the period leading to the event, called survival time. Furthermore, survival analysis is the term used to describe the investigation into the patterns of these events that occur within one or more cohorts in a study [4]. In dealing with the analysis of survival data, researchers are interested in the length of time it takes a patient to reach an event rather than simply the fact that the event has or has not occurred.

There are at least two ways to motivate why particular data mining and statistical learning techniques were suitable for a particular learning task [5]. One way was through comparative studies and the other was through benchmarking [5]. This research study was based on comparative study of data mining and statistical learning techniques. Each of the data mining and statistical learning techniques is briefly discussed below.

Support Vector Machine (SVM) was mainly developed by Vladimir Vapnik and is based on the structural risk minimization principle from statistical learning theory. SVM algorithm uses a nonlinear mapping to transform original training data into higher dimensions. Then SVM searches for the linear optimal separating hyperplane within the new dimension. The hyperplane is the decision boundary separating the datasets of one class from another. The SVM finds this decision boundary using training sets or support vectors, and margins defined by the support vectors. SVM is very accurate due to its ability to model complex nonlinear decision boundaries and is, less prone to overfitting problem, but according to [3], SVM is very slow when compared with other classification algorithms [3] and [6].

The decision tree algorithm is the most popular algorithm in data mining classification technique because it is easy to understand how it makes predictions. There are many decision tree algorithms for constructing a decision tree, such as ID3, C4.5, SLIQ, Scalable Parallelizable Induction of Decision Tree (SPRINT), etc. There are two phases in generating or creating a decision tree, namely the tree-growing phase and tree-pruning phase. In the tree-growing phase the algorithm starts with the whole data set at the root node. The data set is partitioned according to a splitting criterion into subsets. This procedure is repeated recursively for each subset until each subset contains only members belonging to the same class or is sufficiently small. In the tree-pruning phase, the decision tree is reduced in order to improve time complexity and prevent overfitting [7].

AdaBoost is one of the most powerful learning ideas introduced in the past twenty years. It was originally designed for classification problems, but has been extended to regression as well [9]. AdaBoost is a popular ensemble method and has been shown to significantly enhance the prediction accuracy of the base learner [4]. It is a learning algorithm used to generate multiple classifiers and to utilize them to build the best classifier [10]. The process of boosting is to combine the outputs of many weak classifiers to produce a powerful classifier. The predictions from the weak classifiers are then combined through a weighted majority vote to produce the final prediction [9]. The advantage of this algorithm is that it requires less input parameters and needs little prior knowledge about the weak learner [4].

The study of artificial neural networks (ANN) was inspired by attempts at mimicking the brain functionality [11]. Neural networks represent an alternative computational paradigm, which has received much attention in the past few decades [12]. Neural networks are capable of predicting new classes based on past examples after executing a process of learning. There are two phases in the processes of training the artificial neural network: learning and recalling. Networks are trained by inputting a training dataset with the target data. Weights are adjusted until the outputs reach the desired training outputs. The goal is to minimize the error, which is the difference between the target output and desired output. After learning, the testing dataset would be applied to the artificial neural network to estimate the desired output and determine the performance of learning.

The general approach that was used for predictive model building in this research is as follows:

1. Create training and testing datasets.
2. Apply a data mining/statistical learning technique to the training set.
3. Generate the predictive model.
4. Evaluate model using testing dataset.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

5. Repeat step# 2 with other techniques.
6. Compare performance between techniques.

The breast cancer dataset consists of five categories of patient data, as shown in Table 1, that exist for more than 62,000 breast cancer patients diagnosed in the United States between 1990 and 1997. Thus, all files contain variable data for the same group of patients. The dataset originated from The Surveillance, Epidemiology, and End Results (SEER) Program of the NCI. Most of the data, including pathology, diagnosis, and treatment, are real and excellent biomedical dataset. The demographic data, however, was partially artificial due to patient's privacy, as the original dataset from SEER is completely anonymous. This identifier acts like a hospital record number of a patient but is purely fictitious, as the original data is anonymous. Variables for the complete patient dataset are shown in Table 1.

There are a number of methods that can be used to transform data variables into forms that are usable by data mining algorithms. The Weka data-mining tool was used for the preparation of the breast cancer datasets for mining.

The PCA data reduction method (prcomp( ) function) in R statistical program was used to reduce the dataset. PCA is a statistical method routinely used to analyze interrelationships within a large set of data, revealing common underlying factors or components. PCA examines the correlations between the original data values and condenses the information contained within objects into smaller group of components with minimal loss of information.

According to [4], stratified 10-fold cross-validation is a common validation method used to minimize bias and variance associated with random sampling of the training and test datasets. Also, it is a common method for data selection in machine learning related to medical and biological research. The stratified 10-fold cross-validation process was used in this study in evaluating and validating the predictive model. The process consists of four steps as follow [4]:

1. Divide the dataset into a set of subclasses.
2. Assign a new sequence number to each set of subclasses.
3. Randomly partition the subclass into 10 subsets or folds.
4. Combine each fold of each subclass into a single fold.

The Weka data mining tools support automatic splitting of a data set into training and test sets using either a straight percentage splits or through k-fold cross validation.

TABLE 1. PATIENT DATSET VARIABLES

Table Name	Attribute Name	Attribute Description
Demographic data	patientid	unique patient identifier (artificial)
	dateofbirth	patient date of birth (artificial)
	maritalstatus	marital status at diagnosis
	race	patient ethnicity
	ageatdiagnosis	age at diagnosis
	alivestatus	patient alive or dead
	survivaltime	survival time from date of diagnosis
Diagnosis data	patientid	
	yearofdiagnosis	year of diagnosis
	histology	histologic type of tumor
	primarysite	site of primary tumor
	numberofprimaries	number of primary tumor
Pathology data	patientid	
	Grade	tumor grade
	Nodesexam	number of lymph nodes examined
	Nodespos	number of positive lymph nodes
	Extent	extent of disease
	Nodalstatus	status of lymph node involvement
	Size	size of tumor
	Pgr	progesterone receptor status
	Er	estrogen receptor status
Staging	patientid	
	Stage	stage of tumor
Treatment	patientid	
	Surgery	surgery regime received
	Radiotherapy	radiotherapy received

III. RESULT

This section discusses analysis of the breast cancer dataset by various methods.

Analysis was begun by performing logistic regression on the complete 10-year survival dataset. The summary( ) function was used and length on the alivestatus factor to determine the number of rows for each outcome, as well as the total number of patients as shown in Table 2.

TABLE 2. TOTAL NUMBER OF PATIENTS

Total Number of Rows in the Dataset		
0	Number of live patients	11,714
1	Number of dead patients	3,480
	Total number of patients	15,194

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

The number of patients alive after 10 years (row 0) is more than three times the number of patients that have died (row 1). To create a logistic regression model, glm( ) function is called, which provides a model that is an equation to predict whether a patient will survive 10 years. To evaluate the predictive ability of the model, we used the predict( ) function to predict the probability of outcome for all cases in the dataset. The classification result of the logistic regression was 12,080 (11,301 + 779) correct predictions (true positive and true negative), and 3,114 (2,697 + 417) incorrect predictions, resulting in the overall accuracy of 79.5% (12,080/15,194). The precision was 80.7% (11,301/13,998). The recall was 96.4% (11,301/(11,301+417)).

Logistics Regression with Holdout: We repeated the logistic regression approach using the holdout method that contained lesser dataset to evaluate the model; the result was 1,482 (816 + 666) correct predictions (true positive and true negative), and 604 (392 +212) incorrect predictions, resulting in the overall accuracy of 71% (1,482/2,086). The precision was 67.5% (816/(816+392)). The recall was 79.4% (816/(816+212)).

Decision Tree Algorithm: The Weka's J48 decision tree learner, based on C4.5 decision tree algorithm was used with default parameter setting to build a decision tree model for a 10-year survival dataset. The function was called J48 and is already implemented in RWeka. The precision for the model is 79.9% (2,485/(2,485+631)). The decision tree model was evaluated using the 10-fold cross-validation.

The multilayer perceptron learner algorithm in Weka with default parameter settings was modified such that it could serve as a Neural Network. The hidden layers parameter was set to one hidden layer with five nodes to build the artificial neural network model for a 10-year survival dataset. The function is called multilayerPerceptron and is already implemented in RWeka. The model was evaluated using 10-fold cross-validation and the original train.full_1 dataset was used to build the model. The result was 72.94% accuracy in classification. The correct prediction was 4926/(4926+1827), which was 72.94% and incorrect prediction was 1827/(4926+1827), which was 27.1%. The kappa statistics was 0.523.

The next modeling approach was a support vector machine (SVM). The SVM algorithm implemented in Weka is called SMO (sequential minimal optimization). A significant factor in the SVM model-building process is parameter adjustment. The SVM model was generated using RWeka's built-in function, SMO( ). Ten-fold cross validation of the SVM model was performed and the model was evaluated using the 200-instance test set.

The SVM model accuracy result on the full dataset was 68.4%, the correct prediction was 4620/(4620+2133), and incorrect prediction was 2133/(4620+2133), which was 31.6%. The kappa statistics was 0.3683 and the ROC area was 0.684.

We applied boosting to the breast cancer dataset using J48 decision tree as our model-building algorithm. To implement AdaBoost.M1, we called the AdaBoostM1( ) function and set the classifier algorithm parameter (W) to "J48" using Weka_control().

We evaluated the model by performing 10-fold cross-validation; the boosted model is then evaluated on the small test set. The boosting model accuracy result on the full dataset was 69.5%, the correct prediction was 4694/(4694+2059) and incorrect prediction was 2059/(4694+2059), which was 30.5%. The kappa statistics was 0.3902 and the ROC area was 0.759. The boosting model accuracy result on the 200_test data was 73%. We applied bagging to the breast cancer dataset using the J48 decision tree. The bagging( ) function in Weka was called and set the classifier algorithm parameter (W) to "J48". The model was evaluated by performing 10-fold cross-validation, the bagged model was evaluated on the small test set (200 instances).

The bagging model accuracy result on the full dataset was 68.84%, the correct prediction was 4649/(4649+2104), which was 68.84% and incorrect prediction was 2104/(4649+2104), which was 31.16%.

The RandomForest model was built using Weka's RandomForest ( ) function, which is based on the same concept as the original Random Forest algorithm developed by Breiman (Breiman, 2001). Like boosting and bagging, the Random Forest model was created using the Weka's RandomForest( ) classifier and evaluated the model by performing 10-fold cross-validation. Using Weka_control() function, the RandomForest( ) function created 1,000 trees by setting the parameter I to 1000.

The Random Forest model accuracy result on the full dataset was 75%, the correct prediction was 5064/(5064+1689), which was 74.99% and incorrect prediction was 1689/(5064+1689), which was 20.01%.

The summary of the prediction results of the data mining and statistical learning algorithms are shown in Table 3. The SVM classifier is the only algorithm that did not improve when applied to the independent dataset with 200 records. The rest of the algorithms showed slight improvement when applied to the independent dataset.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

TABLE3. PREDICTION RESULTS OF THE ALGORITHMS

Type	Overall Accuracy – Full Dataset	Overall Accuracy – 200 Independent dataset	Precision – full dataset	Precision – 200 Independent dataset
Logistics Regression	71%	72.5%	67.5%	68.3%
Decision Tree – J48	70.17%	71.5%	71.7%	74.2%
ANN MultilayerPerceptron( ) function	72.94%	73.04%	74%	74.7%
Support Vector Machine (SVM) using Weka's Sequential Minimal Optimization (SMO)	68.414%	66.5%	69.7%	69.4%
Boosting- AdaBoostM1	69.5%	73%	70.2%	71.7%
Bagging - Weka's Bagging( ) function	68.84%	72%	67.3%	71.6%
Random Forest - Weka's RandomForest function	75%	76.6%	72%	73.1%

IV. DISCUSSION

The prediction of cancer survivability has been a major issue in medicine and biology. In this study, we have explored six different statistical and machine learning methods for generating predictive models for datasets with either binary or continuous response variables. It is critical that one does not apply classification or regression methods to datasets without having confidence that the methods are indeed suitable for data.

For the binary outcome survival status dataset, we generated six models from diverse statistical learning and data mining techniques. This was useful because it gave us a choice of models and indicated which model is superior by assessing the accuracy and precision. From the accuracy perspective, the best model is RandomForest (75.0%). We did, however, express concern about cost of predicting patients to survive 10 years but who actually die (False–Negative). If this is more important than overall accuracy or precision, our best model is produced by bagging (26.5% error) and the worst is the decision tree (33.3% error). The second best error rate for false-positive is Random Forest (30% error). Clearly there is much to think about even after we have generated the models, from this study, we can say the result of each model depends on the quality of the biological dataset, the size of the dataset and the representation of the dataset.

Results of the classifiers applied to the full breast cancer dataset were mixed. Logistic regression outperformed decision tree, SVM, AdaBoost, Bagging and naïve Bayes algorithms based on accuracy. However, the artificial neural network showed slight improvement over logistic regression, while the decision tree resulted in slightly higher classification accuracy over AdaBoost, Bagging and naive Bayes' models in terms of accuracy. The outcome of this study indicated that data mining and statistical learning are not necessarily a panacea to understanding the prediction and diagnostics of breast cancer problem. It is hoped that this study advances the understanding of the appropriateness and effectiveness of selecting appropriate data mining, machine learning and statistical learning methodologies in prediction of breast cancer survivability. Results indicate that in terms of accuracy and precision, Random Forest and Artificial Neural Network techniques are the good models to use for prediction of breast cancer survivability. Improving the prediction's accuracy and precision rates is possible by actions that include changing the size of the variables, reducing the feature or selecting most reliable features using PCA, singular value decomposition (SVD), RELIEF or any robust feature selection algorithm. The modification of data preprocessing techniques, adjusting runtime parameters, and generating ensemble methods with different parameters may improve the precision and accuracy rates.

V. CONCLUSION

Medical institutions looking to undertake a data mining approach to solve biological problems could be well-served by including statistical learning and data mining processes in their analytical and intervention efforts. Computer scientists, medical researchers and statisticians need to look at their own biological data availability for variables that might potentially link to prediction of cancer survivability. The selection of variables in this study was based on computational biology and bioinformatics literatures, breast cancer dataset available and domain knowledge of the researcher.

Data preparation (data quality) could be the difference between a successful machine learning project and a failure and takes between 60 – 80% of the whole data mining or machine learning effort or process (Witten & Frank, 2005).

The ability of a medical practitioner to effectively pinpoint how long cancer patients survived during treatment, may lead to better evaluation of the treatment and design of personal medicine or drugs to breast cancer patients. This study provides a detailed account of a data mining process applied to the prediction of breast cancer survivability. The data mining process followed for this study began with the inclusion of a large set of factors that was reduced manually through standard statistical analysis.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Findings indicate that none of the data mining and statistical learning algorithms applied to the breast cancer dataset outperformed the others in such a way that it could be declared the optimal algorithm. Additionally, none of the algorithm performed poorly as to be eliminated from future prediction model in breast cancer survivability tasks.

ACKNOWLEDGMENT

We would like to extend our appreciation and thanks to Dr. Eugene Fink at Carnegie Mellon University and Dr. John Rusnak at Capella University for their advice and recommendations in this study. The data used in this study is freely available at National Cancer Institute website; the Weka and R were free software applications that were available to download online.

REFERENCES

[1] J. Adams, S. Matheson, and R. Pruim, BLASTED: Integrating biology and computation, Journal of Computing Sciences, vol. 24, pp. 47 54, 2008.

[2] T. Mitchell, Machine Learning, San Francisco, CA: McGraw Hill 1997.

[3] J. Han, and M. Kamber, Data Mining: Concepts and Techniques, San Francisco, CA: Morgan Kaufman, 2008.

[4] J. Thongkam, G. Xu, Y. Zhang, and F. Huang, "Breast cancer survivability via AdaBooost Algorithms", Australian workshop on health data and knowledge management, Wollongong, NSW, Australia, 2007.

[5] T. Joachims, "A Statistical learning model of text classification for support vector machines", SIGIR, New Orleans, LA, 2001.

[6] V. N. Vapnik, Statistical Learning Theory, Chichesrter, GB: Wiley, 1998.

[7] C. Kleissner, Data mining for the enterprise. "1060-3425/98 IEEE". Retrieved from the Institute of Electrical and Electronics Engineers (IEEE) Digital Library.

[8] K .Sattler, and O. Dunemann, "SQL database primitives for decision tree classifiers", Proceedings of the 2001 CIKM Conference. Atlanta, Georgia, 2001.

[9] T. Hastie, R., Tibshirani, and J. Friedman, The Elements of Statistical Learning: Data Mining, Inference and Prediction. New York, NY: Springer, 2001.

[10] R. E. Schapire, and Y. Singer, "Improved boosting algorithms using confidence-rated predictions", Journal of Machine learning, vol. 37, pp. 297-336, 1999.

[11] P. Tan, M. Steinbach, and V. Kumar, Introduction to Data Mining. Boston, MA: Addison Wesley, 2006.

[12] J. Hertz, A. Krogh, and R. Palmer, Introduction to the heory of Neural Computation. New York, NY: Addison-Wesley.

[13]. J. H. Witten, and E. Frank, Data Mining: Practical Machine Learning Tools and Techniques. San Francisco, CA: Morgan Kaufman.

AUTHORS PROFILE

Charles Edeki, Ph.D.

Faculty Member

Mercy College, Mathematics and Computer Science Department,

555 Broadway, Dobbs Ferry, NY 10522

cedeki@mercymavericks.edu

Phone: 917-627-0024

Shardul Pandya, Ph.D.

Information Technology, Information Management Professor,

Dissertation Supervisor/Mentor

Research Methods Faculty

School of Business and Technology,

Faculty of Information Technology,

Capella University,

225 South Sixth Street,

Minneapolis, Minnesota – US

Shardul.Pandya@Capella.edu

Phone: 804-337-3445

Fax: 804-835-6447

Advanced Security-Based Data Sharing Model for the Cloud Service Providers

Mohamed Meky
Center of Security Studies
University of Maryland University College
Adelphi, Maryland, USA
mmeky@faculty.umuc.edu

Amjad Ali
Center of Security Studies
University of Maryland University College
Adelphi, Maryland, USA
amjad.ali@umuc.edu

***Abstract*- The authors recently published a security model that provides data owner full control over data sharing in the cloud environment and prevents cloud providers from revealing data to unauthorized users. Security analysis has demonstrated that the published model meets cloud security requirements and is resilient to several security threats. However, in the subject published model, the cloud service provider was a passive party that did not have the authority to authenticate nor confirm users' access policies before forwarding encrypted data to authorized users. In this paper, the authors propose an enhanced model that introduces authentication and policy confirmation authorization to cloud service providers without compromising the full data owner control. The result is an advanced security-based data sharing model that may be applied to secure data sharing of highly sensitive information in the cloud environment.**

Keywords- cloud computing; cloud storage; data sharing model; data access control; data owner full control, cloud storage as a service; data encryption

I. INTRODUCTION

Cloud computing offers new service opportunities with more efficient resource utilization, on-demand scalability, and cost reduction for organizations. An enterprise could use on-demand cloud computing services to increase its storage capacity or add capabilities to their infrastructure or applications without the need to acquire new hardware licenses for new software and the necessary training [1]. Cloud computing services include three major models: Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS) [2]. Examples for SaaS, PaaS, and IaaS are Salesforce [3], Google App Engine [4], and Amazon S3 [5] respectively. However, adapting cloud computing services introduces several security threats to data, as data is no longer on the data owner's premise and cloud providers may have complete control on the computing infrastructure that underpins the services. Some of these security threats include unauthorized data access, compromised data integrity and confidentiality, and lack of full owner control over data. With the cloud computing industry still being defined, it is often unclear which party is responsible for security-related issues. In addition, the customer ignorance of security practices and service providers' refusal to release information is ranked among the top security risks in cloud computing [6]. As a result, it is vital to question cloud service providers about security-related concerns prior to migrating customer data. The increasing concerns about the data security threats in the cloud environment has prompted several research efforts such as [7-9] to establish data sharing models that mitigate the potential security risks while allowing data owners to continue enjoying the enormous benefits cloud computing offers. However, these research efforts are either applicable to specific data format or encryption technique. In addition, they don't provide full control for data owners to grant/deny access to data sharing to authorized users. The authors analyzed the previous research efforts and published a model that allows the data owners to have full control over granting or denying access to data sharing in the cloud environment. However, the cloud provider was a passive party in the published model and did not have the authority to authenticate nor confirm users' access policies before forwarding encrypted data to authorized users. This advanced security-based data sharing model for cloud providers will provide additional security layer to ensure security of highly sensitive information for military and intelligence organizations in the cloud environment by synchronizing security controls between data owners and cloud service providers. The remainder of this paper is organized as follow. Section II describes the details of the advanced security-based model. Section III explains the security analysis of the advanced security-based model, and finally, section IV concludes the paper.

II. THE ADVANCED SECURITY-BASED MODEL

The mechanism of the advanced security-based model is illustrated based on a scenario in Figure 1 and notations listed in Table 1. As shown in the advanced security-based model in Figure 1, a data owner receives a data access request message (m_1) from a user (step 1). Then, after successfully authenticating the user's identity, the data owner simultaneously issues an access ticket (step 2) to the user and a permit ticket (step 3) to the cloud service provider. The access ticket contains a control message (m_2) and an access certificate (m_3). The user forwards the access certificate, issued by the data owner, to the cloud provider (m_5) as shown in step 4. Then the cloud provider compares the permit ticket (m_4), issued by the data owner, and the

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

access certificate (m_5) submitted by the user. If there is a match, the cloud provider ensures that the access certificate is authentic and grants data access to the user. The user decrypts and authenticates the data retrieved from the cloud provider through control information (m_2).

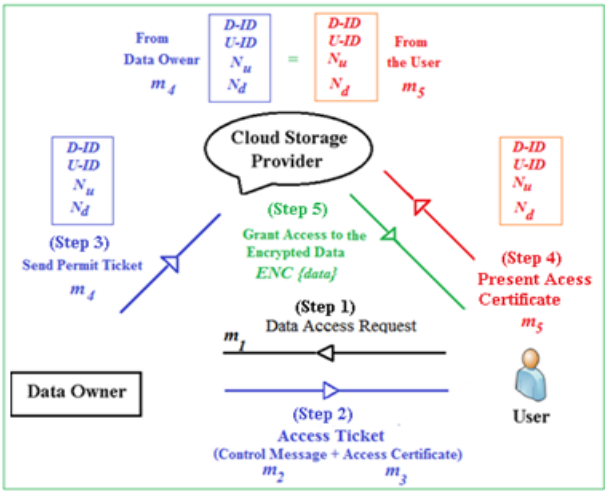


Figure 1. Advanced security-based data sharing model for cloud service providers

TABLE I. MODEL'S NOTATIONS

Notation	Description	Comments
O-ID	Data Owner ID	
C-ID	Cloud storage provider ID	
U-ID	User ID	
D-ID	Shared data ID	
SU	User secret anonymity	Published by data owner
SC	Cloud provider secret anonymity	Published by data owner
du	Secret encryption key for exchanging messages between data owner and the user	Published by data owner
dc	Secret encryption key for exchanging messages between data owner and the cloud provider	Published by data owner
XOR	Logical exclusive or operation	
ks	A one-time session key to be used with XOR operation when transferring message from the cloud provider to the user	Generated by data owner
h (.)	A one-way secure hash function such as SHA-1	
||	A concatenation operator	
$\{.\}_k$	Encryption operator using encryption key, *k*	
EN	Encryption algorithm used for encrypting the shared data	Chosen by the data owner based on data type
ENC{data}	Encrypted data	Sent by cloud provider
kd	Encryption key used for encrypting the shared data	Chosen by the data owner
h(data)	Hash value of the shared data	Calculated at the data owner

Unlike in the previously published model [10] where a cloud service provider has a passive role in authenticating data users, the proposed advanced security-based model introduces a new and enhanced capability for cloud provider to authenticate users and confirm their policies before forwarding them the encrypted data. This new capability is achieved by a permit ticket, sent by the data owner to the cloud service provider, and the access certificate, sent by user to cloud provider, as shown in Figure 2.

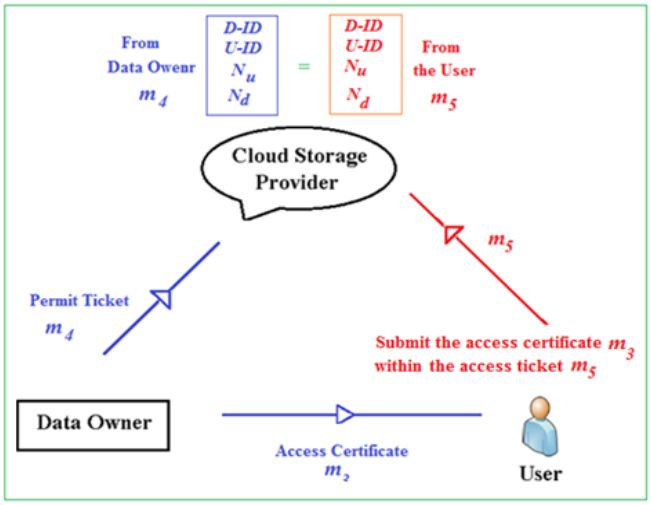


Figure 2. User's authentication and policy confirmation capability of the cloud provider

To execute the proposed advanced security-based model, data owner first needs to complete the following prerequisite tasks:

a) *Issue two secret anonymities, SC and SU, for the cloud service provider and the user.*
b) *Issue two secret symmetric encryption keys, dc and du, for the cloud service provider and the user.*
c) *Use a secure channel, such as Diffie-Hellman key agreement [11], to exchange SC and dc with the cloud provider, and submit SU and du to the user*

After completing the above prerequisite tasks, the proposed advanced security-based model follows the below six steps:

1. *A user requests data access from the data owner*

A user who would like to access data, defined by *D-ID*, generates a nonce, N_u, and prepares a message m_1= *{O-ID // D-ID // N_u}* to be sent to the data owner. The user then sends a data access request message = *{U-ID, {m_1 // h (m_1 // SU)}$_{du}$}* to the data owner as shown in Figure 3.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

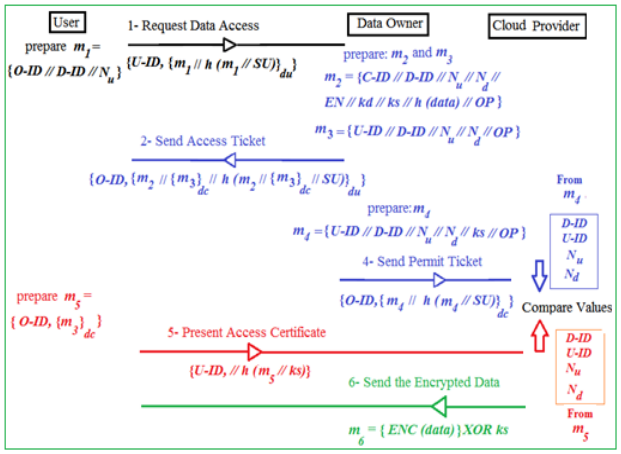


Figure 3. Exchange of messages among user, data owner, and cloud provider

2. *Data owner authenticates and sends access ticket to the user*

Upon receiving the data access request from the user, the data owner executes the following tasks:

a) Decrypt the received message, using the symmetric secret key, du, (that is relevant to *U-ID*) and obtain m_1 = *(O-ID, D-ID // N_u)* and h (m_1 // SU).
b) Verify the format of *O-ID, D-ID* from the decrypted message m_1. If there is no match, the data owner terminates the connection. Otherwise, the data owner continues.
c) Compute *h (m_1 // SU)* and check whether it equals the received h (m_1 // SU). If there is a match, the data owner determines the authenticity of the user.

After authenticating the user, the data owner generates a nonce, N_d, a one-time session key, *ks*, and prepares the access ticket to be sent to the user. The access ticket, *{O-ID, {m_2 // {m_3}$_{dc}$ // h (m_2 // {m_3}$_{dc}$ // SU)}$_{du}$}*, includes the control message, m_2 = *{C-ID // D-ID // N_u // // N_d // EN // kd // h (data) // ks // OP}*, and the access certificate, m_3 = *{U-ID // D-ID // N_u // N_d //OP}*. The optional field, *OP*, could be used to extend the capability of the advanced security-based model. For example, the optional field could have the time limits when the data should be accessed or special access policy that could be related to Mandatory Access Control **(**MAC) or Role Based Access Control (RBAC)**.** It is important to note that the access ticket is encrypted by the secret key, *du*, known only to the user. While the access certificate is encrypted by the secret key, *dc*, known only to the cloud provider.

3. *Data owner sends a permit ticket to the cloud provider*

In addition to sending the access ticket to the user, the data owner prepares a message m_4 = *{U-ID // D-ID // N_u // N_d // ks // OP}* and sends a permit ticket *{O-ID, {m_4// h (m_4 // SC)$_{dc}$}}* to the cloud provider. Upon receiving the permit ticket, the cloud provider executes the following steps:

a) Decrypt the received message, using the symmetric secret key, dc, (that is relevant to O-ID) and obtain m_4 = {U-ID, D-ID // N_u // N_d // ks // OP}, and h (m_4 // SC).
b) Verify the format of *D-ID* from the decrypted message m_4. If there is no match, the cloud provider terminates the connection. Otherwise, the cloud provider continues.
c) Compute *h (m_4 // SC)* and checks whether it equals the received *h (m_4 // SC))*. If there is a match, the cloud provider ensures the authenticity of the data owner.
d) Keep *D-ID, U-ID, N_u, N_d,* and ks for processing the access certificate in step 4.

4. *The user processes the access ticket and presents access certificate to the cloud provider*

Upon receiving the access ticket, *{O-ID, {m_2// {m_3}$_{dc}$ // h (m_2 // {m_3}$_{dc}$ // SU)}$_{du}$}*, the user executes the following steps:

a) Decrypt the received message, using the symmetric secret key, du, and obtain obtain m_2 = *{C-ID // D-ID // N_u // // N_d // EN, kd // h (data) // ks // OP}*, {m_3}$_{dc}$, and *h (m_2 // {m_3}$_{dc}$ // SU)*
b) Compare the values of *D-ID* and N_u, obtained from m_2 to those values sent in message m_1. If there is a match, the user continues.
c) Compute *h (m_2 // {m_3}$_{dc}$ // SU)* and checks whether it equals the received *h (m_2 // {m_3}$_{dc}$ // SU)*. If there is a match, the user ensures the authenticity of the data owner.
d) Keep *C-ID, ks,* and N_d for processing cloud provide message, m_5, in step 5.
e) Extract the encrypted access certificate, {m_3}$_{dc}$, from the received access ticket, prepare a message m_5 = *{O-ID,* {m_3}$_{dc}$}and present the access certificate, *{U-ID, m_5 // h (m_5 // ks)}*, to the cloud provider to obtain the specific data, defined by *D-ID* in message m_1 and m_3.

5. *Cloud provider sends the encrypted data to the user*

Upon receiving the message, *{U-ID, {m_5// h (m_5 // ks)}* from a user, the cloud provider retrieves the one-session key, *ks*, received from the data owner in message m_4, and executes the following steps:

a) Compute *h (m_5 // ks)* and compares it with the received h (m_5 // ks). If there is a match, the user continues.
b) Extract {m_3}$_{dc}$ from m_5 and then decrypt {m_3}$_{dc}$, using the symmetric secret key, dc, that is relevant

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

to data owner, O-ID and obtain m_3 = *{U-ID // D-ID // N_u // N_d //OP}*

c) Compare the values of *U-ID*, *D-ID*, N_u , N_d , *OP*, received from user in m_3, to those values obtained from message m_4 received from the data owner. If there is a match, the cloud provider authenticates the user and continues.

d) Send the required data by preparing the message m_6 = *{ENC (data)} XOR ks* to the user.

e) Send a message = *{C-ID, m_6 // h (m_6 // ks)}* to the user defined by *U-ID*.

6. User verifies the received data from the cloud provider

Upon receiving a message {*C-ID, m_6 // h (m_6 // ks)}* from the cloud provider, the user retrieves the one session key, *ks*, received from the data owner in m_2, and executes the following steps:

a) Compute *h (m_6 // ks)* and compare it with the received *h (m_6 // ks)*. If there is a match, the user continues.

b) Compute m_6 *XOR ks* and obtain the encrypted data, *ENC {data}*.

c) Decrypt the received encrypted data, *ENC {data}*, with the encoding key, *kd*, received from the data owner in m_2.

d) Compute *h (data)* and compare it with *h (data)* obtained from the data owner in message m_2. If there is a match, the user ensures the integrity and confidentiality of the received data.

III. SECURITY ANALYSIS OF THE ADVANCED SECURITY-BASED MODEL

This section provides security analysis of the proposed advanced security-based data sharing model. The analysis demonstrates how the advanced security-based model achieves the goals of securing data storage and sharing and enhancing resiliency against cyber attacks in the cloud environment.

A. Achieving data storage and sharing security goals

The advanced security-based model achieves the security of data storage and sharing in the cloud environments as follows:

1. Since the data is stored in encrypted form on the cloud and the data owner keeps the encryption information (algorithm and key), the cloud storage provider does not have the capability of compromising the integrity and confidentiality of the data stored in the cloud infrastructure.
2. The data owner is the only authority that authenticates the user and issues the data encryption information (algorithm and key) to authorized users. Therefore, cloud providers would not be able to grant data access to unauthorized users.
3. Authentication is achieved by using a hash code, containing a secret anonymity (*SU* or *SC)* and encryption by a secret encryption key (*du* or *dc*). For example, as shown in Figure 4, the data owner appends a secret user's anonymity, *SU*, to the exchanged message, m_2, before computing its hash code, *h* (m_2 // *SU*). The data owner then encrypts the exchanged message, {m_2 // *h* (m_2 // *SU*)} by the secret symmetric key (*du*) and sends it to the user.

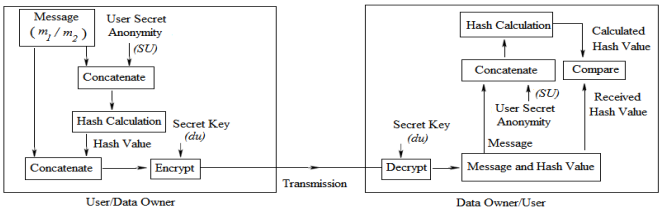


Figure 4. Securing transmission between the data owner and the user

B. Enhancing Resilience Against Cyber-Attacks

The advanced security-based model offers resiliency against various types of cyber-attacks as follows:

1) Resilience against Unauthorized data access attack

This advanced security-based model makes it extremely difficult for unauthorized user to access data since an unauthorized user must pass through the following advanced security layers and authentication steps:

1. Data owner authentication: The attacker must have the knowledge of user anonymity, *US*, and the encryption key, *du*, to request data access and pass the authentication process controlled by the data owner. The attacker would not be able to guess both parameters needed to pass the authentication process nor hack the data access ticket from the owner required to be delivered to the cloud providers to access data.
2. Cloud provider authentication: The attacker must have the knowledge of the nonce, N_u and N_d, sent from the data owner to the cloud provider in m_4 (m_4 = {*U-ID //D-ID* // N_u // N_d // *ks* // *OP}*), the cloud provider encryption key, *dc*, and the one-time session key, *ks*, to create an access certificate *(U-ID*, m_5 // *h* (m_5 // *ks*)), (m_5 = {*O-ID*, {{*U-ID // D-ID* // N_u // N_d //*OP*}}$_{dc}$}), and submit it to the cloud provider in order to gain access to the encrypted data. The attacker will not be able to guess the above parameters needed to pass the authentication process nor hack the data access certificate from the user required to be delivered to the cloud providers to access data. This additional authentication step in

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

the advanced security based model provides an additional security layer to the cloud service providers by allowing them to authenticate users' identities before forwarding them the encrypted data. The introduction of this additional security layer ensures heightened security needed for highly sensitive military and intelligence related information in the cloud environment.

3. Data encryption: If somehow the attacker is able to successfully pass the previous two steps, he/she would not be able to decrypt the data received from the cloud provide since the encryption information (key and algorithm) is not known to unauthorized user and the cloud provider.

2) Resilience against sharing attack

To acquire data during sharing, an attacker must have the decryption key and algorithm. Under the proposed advanced security based model, the decryption key and algorithm remain in the data owner's domain. Therefore, cloud storage providers and unauthorized users would not be able to decrypt the data.

3) Resilience against user's identify guessing attack

This advanced security-based model uses hash code and encryption concepts for the exchanged messages between the data owner and a user. For example, as shown in Figure 4, an authorized user appends a secret user's anonymity to the exchanged message (m_1) before computing its hash code, and then encrypts the exchanged message by the secret symmetric key, *du*. Both secrets (*SU*, and *du*) are known only to the authorized user. Since the hash code provides authentication and the encryption provides confidentiality to the exchanged message between data owner and a user, an attacker may not guess the user's anonymity from the exchanged messages and therefore would not be able to imitate the user's identity to create a new data access request.

4) Resilience against data owner's identify guessing attack

Similarly, data owner uses hash code and encryption concepts for the exchanged messages to authorized users. Therefore, an adversary cannot guess the user's anonymity from the exchanged messages and cannot imitate a data owner and send fake data access to authorized users

5) Resilience against Cloud Provider's Identify Guessing Attack

Since data owner uses hash code and encryption concepts for the exchanged messages to the cloud provider, an adversary cannot guess the cloud provider's anonymity from the exchanged messages.

6) Resilience against Impersonation Attack

An impersonation attack involves an adversary that attempts to impersonate a data owner, a user, or a cloud provider. Under this advanced security based model, an adversary may not be able to impersonate a data owner, a user, or a cloud provider as follows: an adversary may not be able to imitate a data owner to grant data access to a user without knowing user secrets (*SU, du*), cloud provider secrets (*SC, dc*), and data encryption information (encryption algorithm, data encryption key).Without knowing the user secrets *(Su, du)*, an adversary would not be able to imitate a user to decrypt the message m_2 to gain unauthorized access to data. Since the cloud provider doesn't know the data encryption algorithm, *EN*, the data encryption key, *k*d, and the message encryption key, *ks*, (issued by the data owner to the authorized user), an adversary would not be able to imitate a cloud provider to allow access to unauthorized users.

7) Resilience against Replay Attack

A replay attack is a method in which an adversary attempts to replay messages obtained during past communications. An attacker may replay the used message ($m_{1)}$ to the data owner requesting data access and then receiving the message ($m_{2)}$ from data owner. However, under this advanced security based model, the attacker will not be able to derive correct data information (data ID, data encryption algorithm, and data encryption key) from m_2 since the attacker cannot decrypt m_2 without knowing the user secrets(*SU, du)*. In addition, the attacker will not be able to decrypt message (m_5), received from the cloud service provider, since the attacker cannot retrieve the one time encryption key, *ks*, issued by data owner in message, m_2. An attacker may replay the used access message, (m_5 = {*O-ID,* $\{m_3\}_{dc}$} = {*O-ID,* $\{\{$*U-ID // D-ID //* N_u *//* N_d *//OP*$\}\}_{dc}$}*)*, to the cloud provider to gain access to the encrypted data. Since the cloud provider will recognize that message nonce (N_u and $N_{d)}$ has been expired, the cloud provider will ignore the received access message and will not provide data access to the attacker.

IV. CONCLUSION

This paper has introduced an advanced security-based data sharing model that offers authentication and policy confirmation capabilities to cloud service provider while maintaining data owner full control capability, security requirements achievement, and resiliency to several cyber security threats in the cloud environment. The proposed advanced model can be used to secure data sharing of highly sensitive information stored by military and intelligence organizations in the cloud environment. The proposed advanced security-based model offers flexibility for each application to use its own unique data format and encryption technique for facilitating secure data sharing in the cloud environment.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

REFERENCES

[1] M. Luo, L. Zhang, and F. Lei, "An Insuanrance Model for Guranteeing Service Assurance, Integrity and QoS," IEEE International Conference on Web Services, pp. 584-591, 2010

[2] T. Sridhar, "Cloud computing – a primer, Part 1: models and technologies," The Internet Protocol Journal, vol. 12 (3), pp. 2–19, September 2009.

[3] Salesforce Inc., 2011. Retrieved from Salesforce Inc.: http://www.salesforce.com/.

[4] Google Inc., "Google app engine," 2011, retrieved in March 2011 from http://appengine.google.com

[5] Amazon Inc., "Simple storage service," 2011, retrieved in March 2011 from http://aws.amazon.com/s3.

[6] K. Fogarty, "*Cloud computing's top security risk: how one company got burned*," 2010, retrieved from http://www.cio.com/article/599473/Cloud_Computing_s_Top_Security_Risk_How.

[7] K. Hamlen, M. Kantarcioglu, L. Khan, and B. Thuraisingham, "Security issues for cloud computing," International Journal of Information Security and Privacy , vol. 4 (2), pp. 39-51, 2010.

[8] G. Zhao, C. Rong, J. Li, F. Zhang, and Y. Tang, "Trusted data sharing over untrusted cloud storage providers," 2nd IEEE international conference on cloud computing technology and science, pp- 97-103, 2010

[9] W. Wan and Z. Li, "Secure and efficient access to outsourced data," 16th ACM conference on computer and communication security, 2009.

[10] M. Meky and A. Ali, "A Novel and Secure Data Sharing Model with Full Owner Control in the Cloud Environment," International Journal of Computer Science and Information Security, vol. 9 (6), pp.12-17, 2011.

[11] W. Diffie and M. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory , vol. 22 (6), pp- 644-654, 1976.

AUTHORS PROFILE

Mohamed Meky is an Adjunct Professor of Cybersecurity at the Center for Security Studies, University of Maryland University College (UMUC). He has more than fifteen years of experience in industrial, research, and teaching. He has published several articles in IT field and cybersecurity. His current research interest is in the cybersecurity.

Amjad Ali is the Director of the Center for Security Studies and a Professor of Cybersecurity at University of Maryland University College. He played a significant role in the design and launch of UMUC's cybersecurity programs. He teaches graduate level courses in the area of cybersecurity. He has served as a panelist and a presenter in major conferences and seminars on the topics of cybersecurity and innovation management. In addition, he has published several papers in the area of cybersecurity.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Secure and context-aware routing in mobile ad-hoc networks

r.haboub and m.ouzzif
RITM laboratory, Computer science and Networks team
ESTC - ENSEM - UH2 Casablanca, Morocco
rachidhaboub@hotmail.com and ouzzif@gmail.com

Abstract - The increasing availability of wireless handheld devices and recent advances in Mobile Ad-hoc networks (MANET) open new scenarios in which users can benefit from anywhere and at anytime for impromptu collaboration. However, nodes energy constraints, low channel bandwidth, node mobility, channel variability and packet loss are some of the limitations of MANETs. Instead of handling packet loss, in this work, we propose an approach to reduce packet loss by avoiding the conditions in which packet losses are likely, using a context-aware routing approach, which selects the optimal path from source node to the destination node. The proposed approach was tested and the results show an interesting reduction of packet loss.

Keywords - *MANETs, context aware routing, packet loss.*

I. INTRODUCTION

The demand of smart phones, laptops and PDAs has grown exponentially each year since their introduction. These mobile devices can be used to form a MANET. A MANET consists of arbitrary deployed communicational devices such as cell phones, personal digital assistants (PDAs), laptops, etc; it is a wireless multi-hop network, where all nodes maintain network connectivity cooperatively. The mobile nodes are capable of connecting and communicating with each other using limited bandwidth radio links. These types of networks are useful in any situation where temporary network connectivity is required and in areas where there is no infrastructure, such as disaster relief, where existing infrastructure is damaged, or in military applications where a tactical network is necessary.

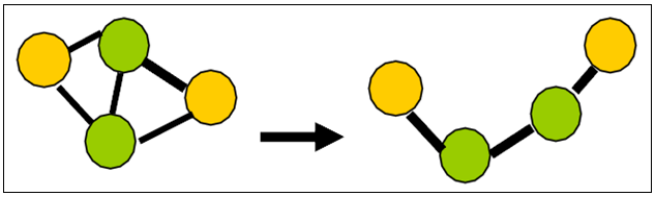


Figure 1. MANETS can change the topology

In the battlefield, typically in a foreign land, one may not rely on the existing infrastructure. In these situations, establishing infrastructure is not practical in terms of expenditure and time consumed. Hence, providing the needed connectivity and network services becomes a real challenge. In a wireless ad hoc network where pairs of mobiles communicate by exchanging a variable number of data packets along routes set up by a routing algorithm, reliability may be defined as the ability to provide high delivery rate, that is, to deliver most of the data packets in spite of faults breaking the routes or buffer overflows caused by overloaded nodes. Given the intrinsic nature of wireless ad hoc networks, reliability is a major issue.

Links failures may occur due to interferences on the wireless medium, or, most probably, to nodes mobility, when pairs of nodes move out of the reciprocal transmission range or are shadowed by obstacles. MANETs do not only provide dynamic infrastructure networks but also allow the flexibility of wireless devices mobility. MANETs differ significantly from existing networks. First, the topology of the nodes in the network is dynamic. Second, these networks are self-configuring in nature and do not require any centralized control or administration. Such networks do not assume all the nodes to be in direct transmission range of each other. Hence these networks require specialized routing protocols that provide self-starting behavior.

However energy constrained nodes, low channel bandwidth, node mobility, high channel error rates, and channel variability are some of the limitations of MANETs. Under these conditions, existing wired network protocols would fail or perform poorly. Thus, MANETs require specialized routing protocols. Operating power is one of the most important resources required by wireless devices [20]. For practical use, wireless devices can only store electricity in relatively small quantities. This makes it necessary to consider conservation measures that reduce consumption of electricity by the equipment. In a related issue, current technology employed by batteries is not sufficient to power wireless devices for long periods.

Thus, energy conservation is one of the few strategies that can really make a difference in the context of mobile device usage. Given the scarcity of power as an operational resource on mobile systems, it is important to notice that there is still no satisfactory solution that provides long-term service and/or low

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

power consumption. In this work we propose an approach which tries to find the optimal path from source node to destination. This paper is organized as follow: the next section shows MANETs applications, section three discusses some routing protocols, section four describes the problematic, section five gives some related works, section six present the proposed approach, the simulation is presented in section seven and the last section conclude this work and gives some perspectives.

II. MANETs APPLICATIONS

MANETs are specifically designed for particular applications [14]. This section discusses potential applications which motivate deploying this kind of networks. MANETs can be used in collaborative networks. A typical application of a collaborative MANET can be considered as a conference room with participant's wishing to communicate with each other without the mediation of global Internet connectivity. In such scenario, a collaborative network can be set up among the participants' devices. Each participant can thus communicate with any other participant in the network without requiring any centralized routing infrastructure. These networks are thus collaborative in nature and are useful in cases where business network infrastructure is often missing or in scenarios where reduction in the cost of using infrastructure links is important.

Figure 2. MANETS applications

MANETs can be used in distributed control systems. MANETs allow distributed control with remote plants, sensors and actuators linked together through wireless communication. These networks help in coordinating unmanned mobile units and lead to a reduction in maintenance and reconfiguration costs. MANETs are used to co-ordinate the control of multiple vehicles in an automated highway system, coordination of unmanned airborne vehicles, and exploration of new geographical areas, rescue, medical applications, mobile systems in a conference and remote control of manufacturing units.

III. ROUTING PROTOCOLS

A protocol is a set of rules that must be followed by partners during a communication process. Without a protocol, messages sent on a network have no meaning, therefore, connection between nodes cannot be established and as result, no information is transferred. Protocols are a required part of the logical structure of a computer network.

There are two main categories of routing protocol (Fig. 3): proactive [10] and reactive [15]. Proactive protocols maintain fresh lists of destinations and their routes by periodically distributing routing tables throughout the network. Reactive protocols find a route on demand (only when needed) by flooding the network with Route Request packets. Studies show, that proactive protocols perform poorly when the mobility increase because of excessive routing overhead [1, 2].

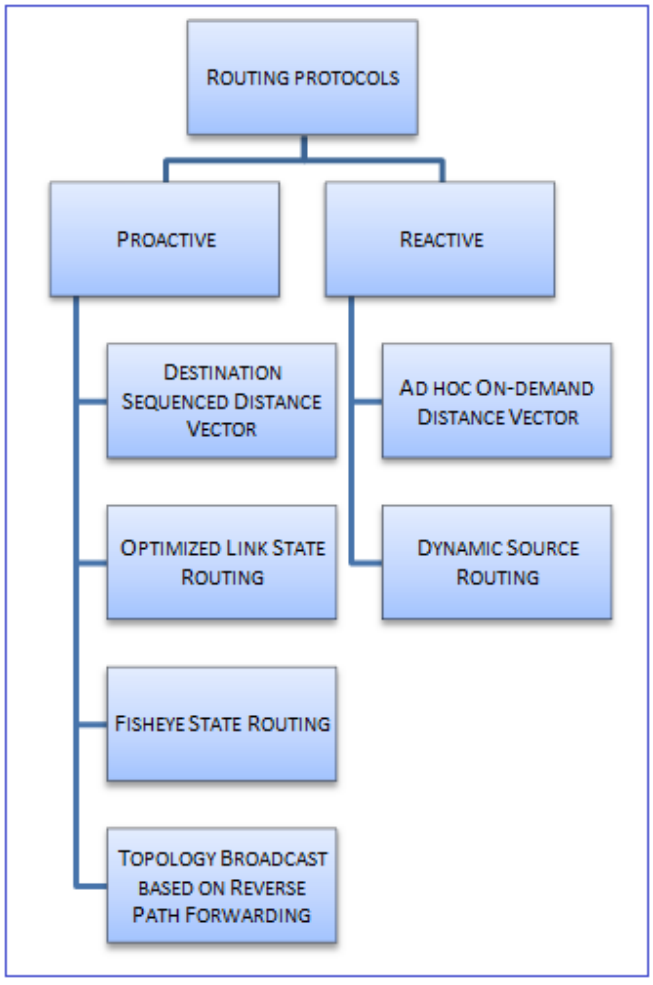


Figure 3. Routing protocols classification

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

IV. PROBLEM STATEMENT

Despite of long history of MANETs, there are still a quite number of problems that are open for the research community. Routing is one of the most important open issues in MANETs research. When nodes want to communicate with each other, they must initially discover a suitable route to be used for the communication. The high mobility, low bandwidth, and limited computing capability characteristics of mobile hosts make the design of routing protocols very challenging. The protocols must be able to keep up with the rapid unpredictable changes in network topology with as minimal control message exchanges as possible and in the most efficient and reliable way. An essential problem concerning ad hoc wireless networks is to design routing protocols allowing for communication between mobile hosts. The dynamic nature of ad hoc networks makes this problem especially challenging.

In any network communication there is a need for a suitable routing mechanism to deliver packets from source to destination nodes. The concept of routing can be described as the process of path finding. In case of mobile ad hoc networks (MANETs) the main problem in routing mechanism, is how to send a packet from one node to another when no direct link exist between source and destination nodes. The routing protocol must also be aware of MANETs limitations. Using for example node's energy in a non-efficient way, may lead to some nodes death, which lead to breaking links and packets loss.

V. RELATED WORKS

Different approaches have been proposed in the research community to improve the reliability of packet-delivery in different application scenarios. Forward Error Correction (FEC) approaches [3,4] and multipath transmission approaches [8] are proposed to improve the reliability of packet-transmission by adding redundant information into transmitted data. With the redundant information, some bit errors can be eliminated without retransmission. Data-fusion mechanisms [16] can change the structure of data packets to distribute transmission errors across multiple packets.

Geographical routing protocols [7] use nodes location information to determine link status and avoid links between distant nodes. On-demand routing protocols [5] check the status of links by exchanging a small control message before the transmission of any data packet. These approaches reduce the probability of transmitting a data packet through a link that has already failed. Most proposed on-demand routing protocols (for example, Dynamic Source Routing (DSR) [6] and Ad hoc On-demand Distance Vector (AODV) [5, 12]) however, use single route for each session.

SPAN [18] selects a number of coordinators to keep an ad hoc network connected. These coordinators are responsible for forwarding and buffering packets while others sleep. Thus it saves power without significantly diminishing the capacity or connectivity of the network. However it introduces large delays and is not applicable for time critical applications. Some routing algorithms given by [20, 21] can optimize the energy use with a global perspective. But these algorithms cause expensive overheads for gathering, exchanging and storing the state information of a node. Power control techniques have direct impact on routing strategies for MANETS.

Therefore, much of the work on power control has been concentrated on the development of new protocols that can minimize the used power. For example, Jung and Vaidya [21] provide a new protocol for power control, based on information available through lower level network layers. Another example of this approach is given in Narayanaswamy et al. [22]. A simple strategy for minimizing the power consumption in a network consists of trying to reach the state of minimum power in which the network is still connected. Despite the apparent optimality of this technique, Park and Sivakumar [23] have shown that this is not necessarily an optimum power strategy for power control minimization. Still another approach for power control is presented by Kawadia and Kumar [24]. Two protocols are proposed, in which the main technique used is clustering of mobile units according to some of its features.

VI. APPROACH

If the motion parameters of two neighboring nodes like speed, direction, radio propagation range are known (using for example a Global Positioning System (GPS)), the duration of time these two nodes will remain connected can be determined. Assume two nodes i and j within the transmission range of each other. Let (xi, yi) be the coordinates of node i and (xj, yj) be the coordinates of node j. Let Vi and Vj be the speeds, ɵi ($0 \leq$ ɵi) and ɵj (ɵj $\leq 2\Pi$) be the directions of motion for nodes i and j, respectively. The amount of time two mobile hosts will stay connected, is predicted by the formula given by equation:

$$\text{Link time life} = \frac{-(ab + cd) + \sqrt{(a^2 + c^2)r^2 - (ad - bc)^2}}{a^2 + c^2}$$

$$a = V(r)\text{Cos}\Theta - V(s)\text{Cos}\Theta$$

$$b = X(r) - X(s)$$

$$c = V(r)\text{Sin}\Theta - V(s)\text{Sin}\Theta = V\big(Y(r)\big) - V\big(Y(s)\big)$$

$$d = Y(r) - Y(s)$$

r is the transmission range of a wireless node with an Omni-directional antenna, which is 250 m. V(s) and V(r) are the velocities of the sender and receiver respectively. Θ is the direction of motion of nodes. (Xs,Ys) and (Xr,Yr) are the coordinates of the sender and receiver respectively. Parameter "a" is the relative velocity of the receiver node with respect to the sender node along Y axis. "b" is the parameter used to determine the distance of the receiver node from the sender node along X axis. The third parameter used to determine LET is "c", which is the relative velocity of receiver node with

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

respect to the sender node along Y axis. “d” is the distance of the receiver node from the sender node along Y axis.

Consider a MANET consisting of four nodes illustrated in Fig. 4, figures a, b and c represent the network topologies for a non mobility aware protocol at times t, t+1 and t+2, respectively. Figures d, e and f narrate the expected network topologies for the MARP (Mobility Aware Routing Protocol) approach at times t, t+1and t+2, respectively. Node 0 and Node 3 are assumed to be sender and receiver nodes respectively. A non-mobility aware protocol would use route 0-1-2. If node 1 is moving away out of the transmission range of node 3, the link 1-3 breaks. This event initiates route maintenance activity which results in heavy control traffic generated by node 0 and node 3 in an attempt to revive the broken link but in vain.

It forms route 0-2-3 to retain the network data transmission. Apart from high control traffic generated, the active transmission of data through these links during a link disconnection results in loss of data packets. Both the excess control overhead generated to revive the broken links and the data packet loss could have been avoided if a more reliable route 5-4-3-1 was formed instead of 5-4-2-1. This can be achieved with the implementation of the MARP routing algorithm in the underlying routing protocol. With MARP, the fast moving node, node 2, is eliminated from route discovery process by node 1 and the routing protocol forms the route through node 3 instead.

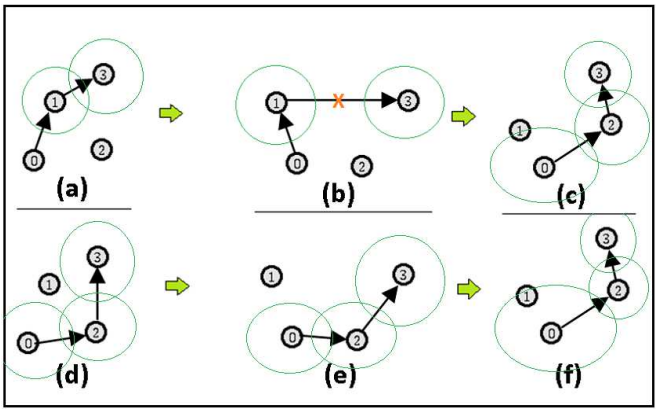


Figure 4. Mobility awareness

When a node wants to send data, it starts sending "RREQ" packets to find a path to the destination node. Our contribution is to delete the "RREQ" messages when it reaches a node with low energy, in this way, this node will not play the role of a router (which means that this node will not consume additional energy by acting as a router), but it can continue to play its oversight role, in the case of a military network of wireless sensors for example.

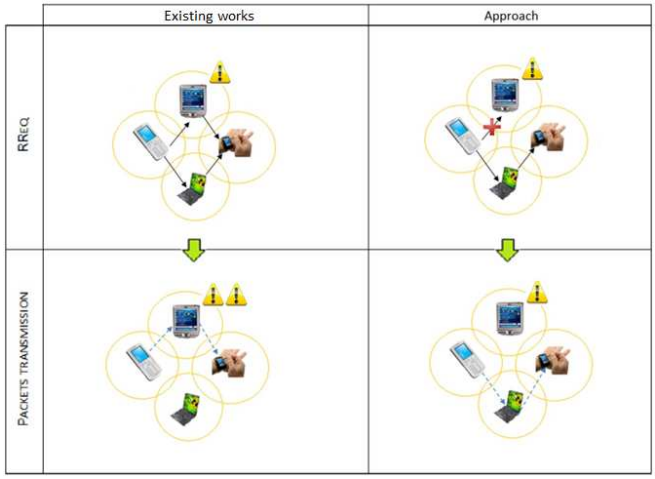


Figure 5. Energy awareness

```
//Getting the receiver coordinates.
Xr, Yr, Zr

//Getting the receiver velocities.
V(Xr), V(Yr), V(Zr)

//Getting the sender coordinates.
Xs, Ys, Zs

//Getting the sender velocities.
V(Xs), V(Ys), V(Zs)

//Calculating the link expiration time.
double a = V(Xr)-V(Xs);
double b = Xr-Xs;
double c = V(Yr)-V(Ys);
double d = Yr-Ys;

// The average transmission range of a wireless node with an 20
Omni-directional antenna is 250 m.
double r = 250;

double P = (((a*a)+(c*c))*(r*r))-(((a*d)-(b*c))*((a*d)-(b*c)));
float Q;

if (P>=0) {Q = sqrt(P);          }
else      { Q = sqrt(-(P));      }

if (((a*a)+(c*c)) == 0.0) {// LET will have an infinite value.}
else { LET = (-1*((a*b)+(c*d))+Q)/((a*a)+(c*c));}


//If LET or the node’s energy is too low, drop the RReq packets.
```

Figure 6. Context awareness algorithm

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

VII. SIMULATION

We use the NS-2 simulator [9]. Figure 7 gives a simplified View of NS-2. NS-2 takes as an input a TCL file (in which we implement the scenario). NS2 consists of two key languages: C++ and Object-oriented Tool Command Language (OTcl). While the C++ defines the internal mechanism of the simulation objects, the OTcl sets up simulation by assembling and configuring the objects as well as scheduling discrete events.

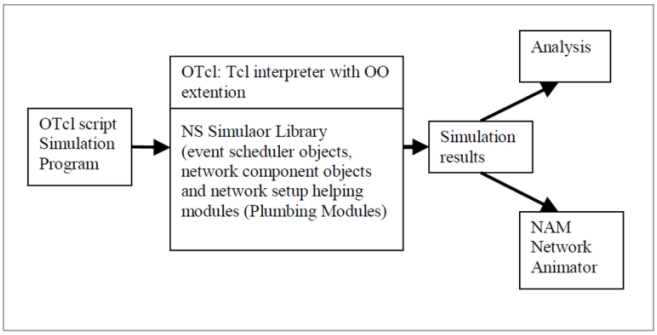


Figure 7. Simplified view of NS2

NS2 is an object oriented, discrete event driven network simulator. It is written in C++ and OTcl (Object-oriented Tool command language) script language with Object-oriented extensions developed at MIT (Massachusetts Institute of Technology). In order to reduce the processing time, the basic network component objects are written using C++. Each object has a matching OTcl object through an OTcl linkage. The procedure of using NS2 [24] to simulate the network and analyze the simulation result is as follows. Firstly, the user has to program with OTcl script language to initiate an event scheduler, set up the network topology using the network objects and tell traffic sources when to start and stop transmitting packets through the event scheduler. OTcl script is executed by NS2.

The simulation results from running this script in NS2 include one or more text based output files and an input to a graphical simulation display tool called Network Animator (NAM). Text based files record the activities taking place in the network. It can be analyzed by other tools such as Gwak and Guplot to calculate and draw the results such as delay and jitter in form of figures. NAM is an animation tool for viewing network simulation traces and real world packet traces. It has a graphical interface which can present information such as number of packets drops at each link. After simulation, NS2 outputs a trace file, which can be interpreted by many tools, such as NAM and Xgraph. We create a simulation scenario using NS-2 Scenario Generator [11].

Fig. 8 shows the NS-2 trace file format. The first field is event, it gives many possible symbols ('r', 'd', etc.). These symbols may correspond for example to received and dropped packets. The second field gives the time at which the event occurs. The third field gives the source node at which the event occurs. The fourth field gives the destination node at which the event occurs. The fifth field shows information about the packet type, whether it's a UDP or a TCP packet. The sixth field gives the packet size. The seventh field gives information about some flags. The Fid field is the flow Id, it can be used for specifying the color of flow in NAM display. The ninth field is the source address. The tenth field is the destination address. The eleventh field is the network layer protocol's packet sequence number, and the last field shows the unique id of a packet.

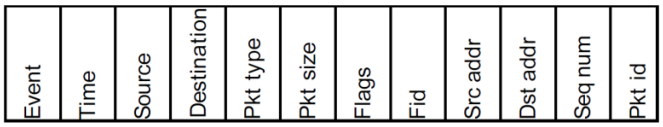


Figure 8. NS-2 Trace File format

We use the Java-Trace-Analyzer to interpret the trace file generated by the simulation. Our approach was simulated using our secure protocol [26]. Figure 9 shows that the proposed approach reduce packet loss.

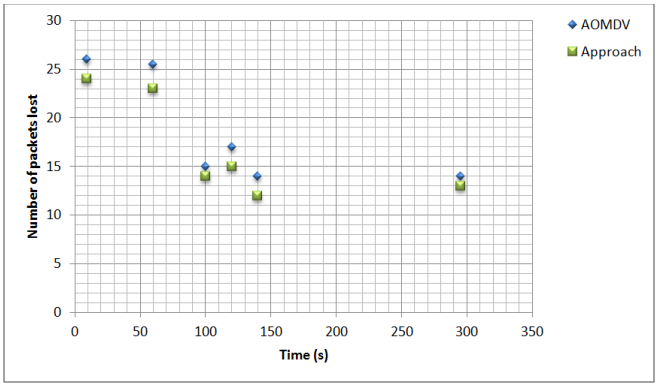


Figure 9. Packet loss versus time

VIII. CONCLUSION AND FUTURE WORKS

In this work we propose an approach to reduce packet loss in MANETs by avoiding conditions in which packet losses are likely, by using a context-aware routing technique, which selects the suitable routing path from source node to destination, according to nodes states. For future work we plan to use more experimentation metrics (such as nodes power, mobility, transmission delay, network vicinity, etc.). We also plan to consider more criteria like connectivity, and so on.

REFERENCES

[1] J. Broch, D.A. Maltz, D.B. Johnson, Y.-C. Hu, and J. Jetcheva, .A "Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols". Proceedings of ACM/IEEE MOBICOM'98, Dallas, TX, Oct. 1998, pp. 85-97.

[2] P. Johansson, T. Larsson, N. Hedman, B. Mielczarek, and M. Degermark, "Scenario-based Performance Analysis of Routing Protocols for Mobile Ad-hoc Networks". Proceedings of ACM/IEEE MOBICOM'99, Seattle, WA, Aug. 1999, pp. 195-206.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

[3] J. Gemmell, L. Rizzo, M. Handley, J. Crowcroft, M. Luby and L. Vicisano, “Forward error correction (FEC) building block”. Internet experimental RFC 3452.

[4] L. Vicisano and M. Luby. “Compact forward error correction (FEC) schemes”, Internet experimental RFC 3695.

[5] Georgy Sklyarenko, “AODV Routing Protocol”, Takustr. 9, D-14195 Berlin, Germany.

[6] Rakesh Poonia, Amit Kumar Sanghi and Dr. Dharm Singh, “DSR Routing Protocol in Wireless Ad-hoc Networks: Drop Analysis”, International Journal of Computer Applications (0975 – 8887), Volume 14– No.7, February 2011.

[7] Jorge Ariza , “Geographic Routing Protocol vs. Table Driven Protocols”, Seminar Routing Algorithmen.

[8] Stephen Mueller, Rose P. Tsang, and Dipak Ghosal, “Multipath Routing in Mobile Ad Hoc Networks: Issues and Challenges”.

[9] Kevin Fall, Kannan Varadhan, “The NS manual”, May 9, 2010.

[10] Guoyou H., “Destination-Sequenced Distance Vector (DSDV) protocol”. Technical report, Helsinki University of Technology, Finland.

[11] Jia Huang, Hamid Shahnasser, "A preprocessor Tcl script generator for NS-2 communication network simulation", San Francisco State University, USA, pp. 184-187, 5 May 2011.

[12] M.Devi and Dr.V.Rhymend Uthariaraj, "Routing with AODV Protocol for Mobile ADHOC Network", International Journal of Technology And Engineering System, Jan – March 2011- Vol2. No1.

[13] Huda Al Amri, Mehran Abolhasan, Tadeusz Wysocki. "Scalability of MANET Routing Protocols for Heterogeneous and Homogenous Networks". International Conference on Signal Processing and Communication Systems. Dec 2007.

[14] I. Chlamtac, M. Conti and J. J.-N. Liu. “Mobile ad hoc networking: imperatives and challenges”. Ad Hoc Networks, Vol.(1), pages 13–64, 2003.

[15] Changling Liu and Jörg Kaiser, “A Survey of Mobile Ad Hoc network Routing Protocols”, 2008.

[16] F. Ye, G. Zhong, S. Lu and L. Zhang, “A robust data delivery protocol for large scale sensor networks”. in Proceedings of IPSN'03, pages 658.673, Palo Alto, CA, USA, April 22-23, 2003.

[17] D.E. Comer, “Internetworking with TCP/IP”, Vol. 1: “Principles, Protocols, and Architecture” (PrenticeHall, Englewood Cliffs, NJ, 1991).

[18] B. Chen, K. Jamieson, H. Balakrishnan, R. Morris, “SPAN,an energy efficient coordination algorithm for topology maintenance in ad hoc wireless networks”, Wireless Networks, Kluwer Academic Publishers 2002.

[19] Chang J. H. and Tassiulas L. “Energy Conserving Routing in Wireless Ad hoc Networks”, Proceedings of IEEE INFOCOM’00, pp. 22-31, 2000.

[20] M. Min and A. Chinchuluun. Optimization in wireless networks. In Handbook of Optimization in Telecommunications, pages 891–915. Kluwer, Dordrecht, 2006.

[21] E. Jung and N. H. Vaidya. A power control mac protocol for ad hoc networks. In ACM MOBICOM 2002, Atlanta, USA, 2002. ACM.

[22] S. Narayanaswamy, V. Kawadia, R. Sreenivas, and P. Kumar. Power control in ad-hoc networks: Theory, architecture, algorithm and implementation of the compow protocol. In European Wireless Conference – Next Generation Wireless Networks: Technologies, Protocols, Services and Applications, pages 156–162, Florence, Italy, 2002. EW2005.

[23] S.-J. Park and R. Sivakumar. Load sensitive transmission power control in wireless ad-hoc networks. In IEEE Global Communications Conference (GLOBECOM’02), Taipei, Taiwan, 2002. IEEE.

[24] V. Kawadia and P. Kumar. Power control and clustering in ad hoc networks. In IEEE INFOCOM’03, San Francisco, CA, 2003. IEEE.

[25] Mathematical Aspects of Network Routing Optimization, Springer, USA, August 30, 2011.

[26] Rachid Haboub and Mohammed Ouzzif, SECURE AND RELIABLE ROUTING IN MOBILE AD-HOC NETWORKS, International Journal of Computer Science & Engineering Survey (IJCSES) Vol.3, No.1, February 2012.

AUTHORS

Rachid Haboub is a full time Ph.D student. He received the Master degree in computer science in 2009. His research spans wireless communication.

Dr. Mohammed Ouzzif is a professor in the computer science department of the higher school of technology of Casablanca - Hassan II university of Morocco.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Non-Linear Attitude Simulator of LEO Spacecraft and Large Angle Attitude Maneuvers

31051243

Azza El-S. Ibrahim
Electronics Research Institute:
Computers & Systems dept.
Giza, Egypt
e-mail: azza@eri.sci.eg

Ahamed M. Tobal
Electronics Research Institute:
Computers & Systems dept.
Giza, Egypt
e-mail: atobal@eri.sci.eg

Mohammad A. Sultan
Cairo University, Faculty of
Engineering: Electronics &
Communications dept.
Giza, Egypt
e-mail: msultan@cu.edu.eg

***Abstract*—the Attitude control problem of a rigid spacecraft with highly nonlinear characteristics has attracted a great interest for its important applications. The main challenge of designing the non-linear attitude control is the controller parameters determination. Most of the early published works use trial and error method for these parameters computation, but it is not accurate and takes a lot of time to get the appropriate parameters. Therefore, this paper presents a novel mathematical way for sliding mode control parameters calculation at every initial attitude state, taking into consideration the actuator saturation constraints. The developed attitude control ensures shortest angular path maneuvers. The objectives are accomplished by building the microsatellite simulator using MATLAB/Simulink software. In addition, the chattering problem of the SMC technique is solved using the saturation function. A system stability based on Lyapunov's direct method is presented. Numerical simulations are performed to show that rotational maneuver is accomplished in spite of the presence of disturbance torques, and control saturation nonlinearity. The results are compared with the conventional PD control technique.**

Keywords-MATLAB/Simulink; sliding mode control; satellite attitude control

I. INTRODUCTION

Attitude determination and control system (ADCS) is one of the most crucial subsystems of the spacecraft. Main function of ADCS is to stabilize the spacecraft, and steer it to a particular direction correctly despite the internal and external disturbance torques acting over spacecraft. Satellite hardware structure and Simplified block diagram of ADCS is shown in Fig. 1.

Attitude control is an important task for the satellite optical payload and for remote sensing applications which, guarantees pointing towards the ground area of the desired image. In general, the spacecraft motion is governed by the so-called kinematic and dynamic equations. Actually, mathematical descriptions are highly nonlinear and thus, the conventional linear control techniques are not suitable for the controller design, especially when large-angle spacecraft maneuvers are required [11]. There are several methods trying to solve this problem, where some research linearized the nonlinear attitude equations then applied different linear controls [7]. Doruk utilized integrator back - stepping method which, provides a

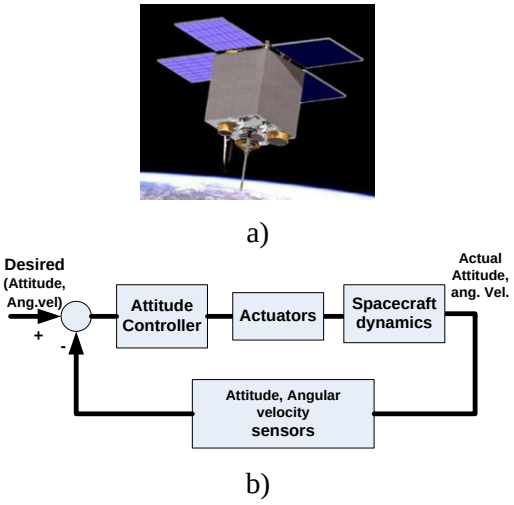


Figure1. a) Satellite hardware structure, b) Attitude control system block diagram

recursive stabilization methodology [5]. Nadir-pointing control is achieved by a full-state feedback Linear Quadratic Regulator which drives the attitude quaternion and their respective rates of change into the desired reference [14].

Sliding Mode Control (SMC) which is a particular type of control, known as variable structure control (VSC), is a powerful and robust control technique, and it has been extensively studied in the last three decades for many classes of linear and non-linear systems [1, 2, 3, 11]. For example, SMC has been applied for mobile robot and welding processes [16], it combined with fuzzy to control robot manipulators [17], also used for linear time varying systems [18]. Recently, some investigators [4, 8, 9 and 13] have applied the sliding-mode to the spacecraft attitude maneuvers.

This paper presents a control system design method for the three-axis-rotational maneuver of a rigid spacecraft. The design of attitude controller was based on variable structure control (VSC) theory leading to a discontinuous control law. Most of the works done in this area did not target how the controller parameters can be chosen. Other works advise to

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

compute them by trial and error method. A novel mathematical way is introduced here to deal with the controller parameters adjustment of attitude tracking problems depending on the actuator saturation limits and on the reaching time. Furthermore, the chattering in control signal is avoided using a boundary layer approach. The thickness of the layers is not constant but they are related to the feedback gains such that the slope of the linear control inside the layer is constants.

The paper is organized as following: In Section II satellite kinematics and dynamics are defined and modeled in state space form. The explanation of the different models used in simulation is mentioned in section III. Section IV discuses the design of SMC control which acts as the attitude controller for the satellite. Control parameters selection methodology is described in section V. Section VI shows the stability analysis of the controller. Section VII shows the way of dealing with the chattering problem. Numerical simulations and comparative study have been performed and presented in the last section.

II. SATALLITE MATHEMATICAL MODEL

The equations of motion of satellite attitude dynamics can be divided into two sets: kinematic equations of motion and dynamic equations of motion.

A. Dynamic Equation of Motion

The dynamic equations of a rigid spacecraft actuated by reaction wheels can be defined in (1) [5, 6].

$$I\dot{\omega}_b^i = T_{dist} - \omega_b^i \times \left(I\omega_b^i + h_w\right) - \dot{h_w} \quad (1)$$

In (1), the angular acceleration of the satellite referenced to the inertial coordinate system is influenced by the disturbance torque T_{dist}, and the control torques exerted by a combinations of reaction wheels $\dot{h_w}$. The satellite moment of inertia, I was estimated by the mass and the shape of the body. The derivation steps of the satellite model starts with the definition of the relative angular momentum of the reaction wheel rotors, $h_w = I_s\,\omega_s$, I_s is the mass moment of inertia of the reaction wheels and ω_s is the angular velocity of the reaction wheel rotors with respect to the body reference frame [6]. For nadir-pointing satellite, the inertial referenced satellite body angular velocities are converted to the orbit frame by the fact that $\omega_{ob}^b = \omega_{ib}^b - R_o^b\omega_{io}^o$ therefore the dynamic differential equations become as in (2) and (3).

$$\dot{\omega}_{ob}^b = J^{-1}\left[-S\left(\omega_{ob}^b - \omega_o c_2\right)\left(I(\omega_{ob}^b - \omega_o c_2) + AI_s\omega_s\right)\right] + J^{-1}\tau_e - J^{-1}A\tau_a - S\left(\omega_{ob}^b\right)\omega_o c_2 \quad (2)$$

$$\dot{\omega}_s = -A^T J^{-1}\left[-S\left(\omega_{ob}^b - \omega_o c_2\right)\left(I(\omega_{ob}^b - \omega_o c_2) + AI_s\omega_s\right)\right] - A^T J^{-1}\tau_e + [A^T J^{-1}A + I_s^{-1}]\tau_a \quad (3)$$

Where, ω_{io}^o is the orbital angular velocity vector and assumed to be constant in circular orbits and equal to $\omega_{io}^o = [0 \quad -\omega_o \quad 0]^T, \omega_o = \sqrt{\frac{\mu_e}{a^3}}$ *where* μ_e is the gravitational parameters, a is the orbit semi-major axis, $R_o^b = [c_1 \quad c_2 \quad c_3]$ is the rotation matrix from orbit frame to body frame and J = [I - $AI_s A^T$] is the inertia-like matrix and A is the reaction wheel orientation matrix. The three reaction wheels are mounted along the body principle axes so A is the identity matrix. τ_e is the total disturbance torques action on the satellite from variety of sources, τ_a is the control torque generated by the reaction wheels.

B. Kienamatic Equatios of Motion

The attitude is assumed to be represented by the quaternion, defined as $q \equiv [q_v \;\; q_4]^T$. The kinematic equation through unit quaternion representation is given in (4):

$$\dot{q} = \frac{1}{2}\,\Xi\,(\mathrm{q})\omega_{ob}^b \quad (4)$$

Where, $\Xi\,(\mathrm{q}) = \begin{bmatrix} q_4 I_{3\times3} + [q_v \times] \\ -q_v^T q_v \end{bmatrix}$, $I_{3\times3}$ is a 3x3 identity matrix and $[q_v \times] = \begin{bmatrix} 0 & -q_3 & q_2 \\ q_3 & 0 & -q_1 \\ -q_2 & q_1 & 0 \end{bmatrix}$ is a skew symmetric matrix

C. System Errors

The error between the desired attitude and current attitude is calculated in quaternion form. Let $q_{e=}[q_{ve} \quad q_{4e}]^T$ denotes the relative attitude error from a desired reference frame to the body-fixed reference frame of the spacecraft, then one may have: $q_e = q \otimes q_d^{-1}$ where, q_d^{-1} is the inverse of the desired quaternion, q is the spacecraft current quaternion and $\otimes$ is the operator for quaternion multiplication. For any given two groups of quaternion, the relative attitude error can be defined by (5) obtained by:

$$\begin{bmatrix} \dot{q}_{ve} \\ \dot{q}_{4e} \end{bmatrix} = \frac{1}{2}\begin{bmatrix} q_{4e}\,I + [q_{ve} \times] \\ -q_{ve}^T \end{bmatrix}\omega_e(t) \quad (5)$$

Where,$\omega_e = \omega - \omega_d$, ω_d is the desired angular velocity of the body and assumed to be zero so $\omega_e = \omega$ and q_{ve} is the attitude quaternion error direction vector.

III. SIMULATION MODULES

This section describes the simulation process. The simulator is built using simulink toolbox of Matlab version 7.5.0.342 (R2007b).

The overall system simulator includes many subsystems or modules. The main modules with their inputs and outputs are shown in Fig. 2

Block (1). "System constant parameters": all satellite physical parameters are gathered in a simulink block so any satellite configuration can be easily used.

Block (2). "Euler to q": the attitude is represented in quaternion form to avoid singularity and complex computation in trigonometric functions in rotation matrix between satellite body frame and orbit frame. Because of the quaternion representation is not physically clear so building a transformation block to transfer from "Euler angles to quaternion" and from "quaternion to Euler" is necessary [10].

Block (3). "qe-calculation": quaternion error calculation module is built using (5).

Block (4). "SMC Controller": the sliding mode control is designed and constructed later in the next section.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

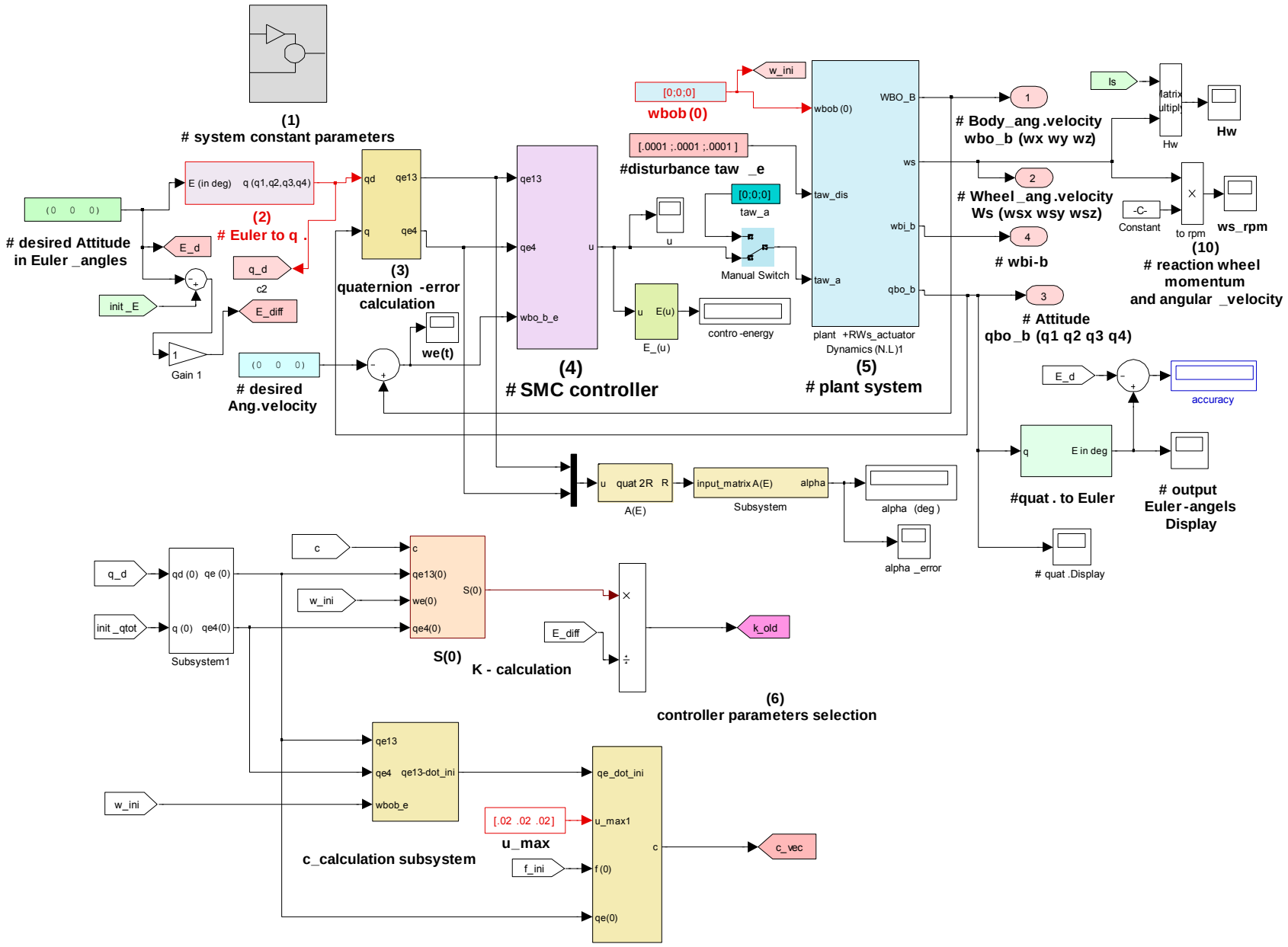


Figure 2. Overall system simulator

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Block (5). "Plant System": the kinematic and dynamic equations are constructed in vector form. These coupled equations must be solved simultaneously

Numerical integration method is used to obtain the time evolution of body attitude and angular velocity referred to the orbit frame. For ensuring that the construction of this module is done correctly, a special case for getting analytic solutions is used in Wertz [6]. The idea assumes that the external torques equal to zero and for axial symmetric body case, equation (1) can be solved then the three component of the body angular velocity can be obtained analytically and compared with the output of the simulator. The kinematic equations become first order differential equations which, can be solved separately and the output is checked.

IV. Sliding Mode Attitude Control Design

Sliding mode control has been widely applied [13, 17, 18] The conventional SMC design approach consists of two steps. First, a sliding manifold is designed such that the system trajectory along the manifold acquires certain desired properties, then a discontinuous control is designed such that the system trajectories reach the manifold in finite time. Therefore the objective is to develop an attitude control law such that $q \to q_d$ and $\omega \to 0$ as $t \to \infty$ under the assumptions of bounded external disturbance, $|T_{dist}(t)| < d_{max}$ and the unit-quaternion q and the angular velocity ω are available in the feedback control design.

A. Sliding Surface Design

A linear sliding surface in vector form is defined in (6) [1].

$$s = \omega + \mathrm{c}\ \mathrm{sgn}(\mathrm{q_{e4}})\ \mathrm{q_{ev}} \tag{6}$$

Where $s(t) = [s_1\ s_2\ s_3]^T \in \mathbb{R}^{3\times 1}$ and c is a strictly positive real constant vector determining the slope of the sliding surfaces. Vadali and Crassidis in [13] added the term $\mathrm{sgn}(\mathrm{q_{e4}})$ so that the spacecraft maneuver follows the shortest path and requires the least amount of control torque.

B. Control Law Design

Based on the selected sliding surface proposed in the above equation, a variable structure attitude controller for the complete system is presented.

Le $f = J^{-1}\left[-S\left(\omega_{ob}^b - \omega_o c_2\right)\left(I(\omega_{ob}^b - \omega_o c_2) + AI_s\omega_s\right)\right] - S\left(\omega_{ob}^b\right)\omega_o c_2, \quad b = -J^{-1}A, \quad$ and $\quad d = J^{-1}\tau_e$

Equation (2) can be rewritten as:

$$\dot{\omega} = f + bu + d \tag{7}$$

Based on the SMC methodology [1, 2] the control signal $u(t)$ is defined in (8).

$$u(t) = u_{eq}(t) + u_d\,(t) \tag{8}$$

The first component of the proposed controller is $u_{eq} = [u_{eq1}\quad u_{eq2}\quad u_{eq3}]^T$which make sliding surface s(t) invariant and it is calculated by setting $\dot{s}$(t) to zero considering s(t) to be zero. Second component $u_d = [u_{d1}\quad u_{d2}\quad u_{d3}]^T$ is an extra control effort which forces the state trajectory to reach on sliding surface in finite time in spite of disturbances and model uncertainties in the system. After differentiating (6) with respect to time equate it by zero.

$$\dot{s} = \dot{\omega} + \mathrm{c}\ \mathrm{sgn}(\mathrm{q_{e4}})\ \dot{\mathrm{q}}_{\mathrm{ev}} = 0 \tag{9}$$

Substitute with Eq. (7) get:

$$bu_{eq} = -f - c\ \mathrm{sgn}(\mathrm{q_{e4}})\dot{q}_{ve} \tag{10}$$

Outside the sliding manifold the system trajectory must be moving towards it. The component u_d , is added to satisfy the reaching condition. For this purpose, the constant rate reaching law ($\dot{s} = -k\ sgn(s)$ is used to specify the dynamics of the switching function directly [2] the control law is obtained.

$$bu = -f - \boldsymbol{c}\ \mathrm{sgn}(\mathrm{q_{e4}})\dot{q}_{ve} - \boldsymbol{k}sgn(s) \tag{11}$$

Substitute the expressions of *b*, *f*, and $\dot{q}_{ve}$

$$u(t) = JA^{-1}\left[-S\left(\omega_{ob}^b - \omega_o c_2\right)\left(I(\omega_{ob}^b - \omega_o c_2) + I_s\omega_s\right)\right] + S\left(\omega_{ob}^b\right)\omega_o c_2 - \frac{1}{2}JA^{-1}\boldsymbol{c}\ \mathrm{sgn}(\mathrm{q_{e4}})(q_{4e}\,I + [\dot{q}_{ve}\times])\omega_e - J\,A^{-1}\boldsymbol{k}\ sgn(s) \tag{12}$$

The controller is simulated as in block (4) and connected in closed-loop with the nonlinear plant, its effectiveness is demonstrated through simulations results.

V. The Controller Parameters Selection Approach

In the previous works, the controller parameters (k, c) were selected by trial and error method that takes more effort and waste of time. This research presents a novel mathematical method to select these parameters.

A. A Self-Tuning Approach for Feedback Gain Vector k

The parameter *k* must be selected to be large enough to guarantee that the trajectories are reaching and remaining on the sliding surface in finite time. In other words, k must verify the following reaching condition [11].

$$\frac{1}{2}\frac{d}{dt}s^T s \le -\eta|s| \tag{13}$$

Where, η is a strictly positive real constant that determines the convergence velocity of the trajectory to the sliding surface. Differentiate (13), then substitute with the control signal in (11) it gives a general condition on the range of k values.

$$s^T\dot{s} \le -\eta|s|$$

$$s^T(\dot{\omega} + \mathrm{c}\ \mathrm{sgn}(\mathrm{q_{e4}})\ \dot{\mathrm{q}}_{\mathrm{ev}}) \le -\eta|s|$$

$$s^T(f + bu + d + \mathrm{c}\ \mathrm{sgn}(\mathrm{q_{e4}})\ \dot{\mathrm{q}}_{\mathrm{ev}}) \le -\eta|s|$$

$$s^T(f - f - c\ \mathrm{sgn}(\mathrm{q_{e4}})\dot{q}_{ve} - ksgn(s) + d + \mathrm{c}\ \mathrm{sgn}(\mathrm{q_{e4}})\ \dot{\mathrm{q}}_{\mathrm{ev}}) \le -\eta|s|$$

$$s^T\left(d - k\ sgn\,(s)\right) \le -\eta|s|$$

$$|s|\ d - k\,|s| \quad \le -\eta|s|$$

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

$$k \geq |d_{max}| + \eta \quad (14)$$

To compute the lower limit of k, η must be firstly determined. By integrating (13) between t= 0 and $t = tr$ the following equation can be obtained:

$$s(t = t_r) - s(t = 0) \leq -\eta(tr - 0) \quad (15)$$

Let t_r be the time required to hit the surface $s(t = t_r) = 0$ and assume the initial value of switching function, s(t=0) = s(0) > 0 hence

$$t_r \leq \frac{s(0)}{\eta} \qquad thus \qquad \eta \geq \frac{s(0)}{t_r} \quad (16)$$

If the system initial error is far from the sliding surface, the system takes longer time to reach the sliding surface and vice-versa. Then t_r is selected such that it is proportional to the difference between initial and required attitude angles (E_{diff}) in deg.

$$t_r = const.\, E_{diff} \quad (17)$$

According to the const.value the reaching phase time can be increased or decreased, let const. = 1. Therefore η can be determined from (16), then the lower limit of k for any initial orientation is computed in (18).

$$k = |d_{max}| + \frac{s(0)}{E_{diff}} \quad (18)$$

B. Selection of Sliding Surface Slope(c) Subject to Input Signal Constant

The system performance is sensitive to the sliding surface slope *c*. In (11) the larger values of ***c***, the larger control effort u(t) then the system will give a fast response, but the reaction wheels may enter their saturation regions. Now consider the situation when u_{max} is the maximum admissible value of the reaction wheel torque. It means that the following inequality must be hold.

$$|u(t)| \leq u_{max} \quad (19)$$

From analysis of the SMC, the maximum value of the control signal u(t), is occurred at the initial time such that the error is maximum. Substitute by the initial value of u(t=0) = u_{max} and the calculated value of k from Eq.(18). The parameter **c** can be obtained from (20)

$$\boldsymbol{c} = \frac{(u_{max} - J(f(0) + sgn(s)|d_{max}|))E_{diff} - Jsgn(s)\omega(0)}{Jsgn(q_{e4})\dot{q}_{ve}E_{diff} + Jsgn(s)q(0)} \quad (20)$$

VI. Controller Convergence analysis

To analyze the stability of the system, consider a positive definite Lyapunov function of the form

$$V(s) = \frac{1}{2}s^T s \quad (21)$$

Then $\dot{V} = s^T \dot{s}$

$$\dot{V} = s^T[d - ksign(s)] = d\,s - k|s| \quad (22)$$

According to the previous selection of k, the derivative of Lyapunov function is negative, which implies that the sliding surface ***s***=0 will be reached in some finite time. Once ***s***=0 is reached, the trajectory in error state-space that slides on the sliding manifold can be shown to be asymptotically stable using again Lyapunov's direct method. Another candidate Lyapunov function is proposed in (23).

$$V_2(q_{ve}) = \frac{1}{2}\, q_{ve}^T q_{ve} \quad (23)$$

$$\dot{q_{ve}} = -\frac{1}{2}\, c\, |q_{e4}|\, q_{ve} + \frac{1}{2}[q_{ve}\times](-c\, q_{ve}) \quad (24)$$

Substituting Eq. (24) into the derivative of the equation (23) leads to the following expression

$$\dot{V}_2 = -\frac{1}{2}\, c\, |q_{e4}|\, q_{ve}^T\, q_{ve} \quad (25)$$

This is clearly negative definite provided c > 0. This results show that attitude tracking error $q_{ve} \to 0_{3\times 1}$ as $t \to \infty$, and since the motion is on the sliding surface defined by $s(t) = 0_{3\times 1}$ It follows that $\omega(t) \to 0_{3\times 1}$ as $t \to \infty$.

VII. Chattering Avoidance

In SMC, the control signal may cause an undesirable chattering phenomenon due to the existence of the sign function. To alleviate such undesirable performance, the sign function can be simply replaced by the saturation function *sat*(*s*/ϵ) (as shown in (26) and Fig. 3),

$$sat(s_i, \epsilon_i) = \begin{Bmatrix} 1 & s_i > \epsilon_i \\ \frac{s}{\epsilon} & |s_i| \leq \epsilon_i \\ -1 & s_i < -\epsilon_i \end{Bmatrix} \; i = 1,2,3 \quad (26)$$

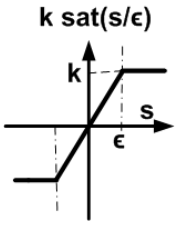


Figure 3: Saturation function

The system is now no longer forced to stay in the sliding mode but is constrained within the sliding layer$|s_i| \leq \epsilon_i$**.** The cost of such substitution is a reduction in the accuracy of the desired performance.

In this work, a constant rate of decay of *s* is selected to avoid chattering and ϵ is taken proportional to k.

VIII. Numerical Simulation Resultes

The effectiveness of the proposed control law is demonstrated by an example of a rest to rest maneuver. Consider a rigid spacecraft with the inertia matrix **I** = [14.28 0 0; 0 15.74 0; 0 0 12.5] kg-m ^{2}and the inertia matrix of reaction wheels is Is = [0.002 0 0; 0 0.002 0; 0 0 0.002] kg-m ^{2}. The initial attitude orientation of the unit-quaternion is q(0) = [0.1603, -0.1431, 0.06252, 0.9746]^T (which is equivalent to initial Euler angles E(0) = [20 -15 10] deg.) , the initial value of the angular velocity is ω(0) = [0, 0, 0]^T rad/s and the control authority is assumed to be u_{max}=[0.02 0.02 0.02]^T N.m, and the disturbances are bounded by $d_{max} = [0.0001\ 0.0001\ 0.0001]$

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

N.m. The SMC algorithm computes the suitable controller parameters required to steer the satellite from initial attitude condition to zero states in 100 sec with steady state error = [.0004592 .0005464 .0003582], k = [0.001401 0.001271 0.0016] , c = [0.1748 0.1332 0.256] and $\epsilon = 0.1k$.

A. Comparative Study

To validate the developed control law, the results are compared with a conventional PD feedback controller. A simulator of a quaternion based feedback controller is also built. The quaternion error and angular rate error vectors are fed to the quaternion feedback controller to generate the control torque vector.

$$u(t) = -k_p q_e - k_d \omega \qquad (27)$$

Where k_p and k_d are the PD controller gains. Notice that, PD controller has six unknown gains to be selected to meet the control system requirement.

Simulation studies have been performed to test both controllers. Figs. 4 and 5 clearly show the performance of the SMC and PD controller. From figures, the SMC controller follows the reference angles with little or no overshoot but the PD controller shows high over and under shoot which is not acceptable for satellite stable operation. In addition, the control effort in PD controller is not within the actuator saturation limit. Moreover, the selection of the controller gains vectors $(k_p,\ k_d)$ are difficult and tedious. The steady state error of SMC is lower than PD control (PD steady state errors are [.01439 .01146 .007685]). Finally, Fig. 6 shows the phase portraits of the error state-space in SMC & PD controllers.

IX. CONCLUSION

In this work the problem of tracking a desired spacecraft attitude in the presence of environmental disturbances and control input saturation has been justified and solved by means of a nonlinear controller. A simulator of attitude dynamics of a rigid satellite actuated via reaction wheels was built using MATLAB/Simulink software, and its detailed was described.

The developed control algorithm based on Sliding Mode Control has the following features: (i) Fast and accurate response in the presence of bounded disturbances; (ii) Explicit accounting for control input saturation; (iii) Computational simplicity and straightforward tuning.

The stability based on Lyapunov-like analysis and the properties of the quaternion representation of spacecraft dynamics was proofed; and the global stability of the overall system is guaranteed in the presence of bounded disturbances. Unlike the early published works, which use trial and error method for controller parameters determination, the developed control algorithm presented a novel mathematical way for sliding mode control parameters computing at every initial attitude state with promising accurate and very fast computation.

Moreover the developed control law reduces the undesirable chattering effect by taking the boundary layer thickness related to the feedback gain value; and save the controller energy by taking into account the shortest angular path maneuvers.

REFERENCES

[1] A Bastoszewicz and J. zuk, "sliding Mode Control-Basic Concepts and Current Trends," Inst. of autom. Control, Tech. Univ. of Lodz, Poland Industrial Electronics (ISIE), IEEE International Symposium on July 2010.

[2] J. Y. Hung, W. Gao, and J. *C.* Hung, "Variable Structure Control: **A** Survey," IEEE transactions on industrial electronics, vol. 40, no. 1, Febrauary 1993.

[3] A. Bartoszewicz, "Variable Structure Control – from Priciples to Applications." International Symposium on System Theory, Automation, Robotics, Computers, Informatics, Electronics and Instrumentation, Craiova, Romania, 18-20 October 2007.

[4] C. Li, Y. Wang, L. Xu, and Z. Zhang, "Spacecraft Attitude Stabilization Using Optimal Sliding Mode Control", National Natural Science Foundation of China 2010 IEEE.

[5] R. Doruk "Nonlinear Controller Design For a Reaction Wheel Actuated Observatory satellite", a thesis submitted to the graduate school of applied science of middle east technical university 2008.

[6] J. R. Wertz, Spacecraft Attitude Determination and Control. Academic Publishers, Dordrecht, Boston, London, 1991.

[7] M. J. Sidi, Spacecraft Dynamics and Control. Israel Aircraft Industries Ltd, Cambridge University Press 1997.

[8] Q. Hum, L. Xie, and Y. Wang, "Sliding Mode Attitude and Vibration Control of Flexible Spacecraft with Actuator Dynamics", 2007 IEEE International Conference on Control and Automation WeDl-2 Guangzhou, CHINA - May 30 to June 1, 2007

[9] C. Pukdeboon, A. S. I. Zinober, and M.-W. L. Thein "Quasi-Continuous Higher-Order Sliding Mode Controller Designs for Spacecraft Attitude Tracking Maneuvers", 2008 IEEE

[10] Y. Xia, Z. Zhu, M. Fu, and S. Wang, "Attitude Tracking of Rigid Spacecraft With Bounded Disturbances", IEEE Transactions On Industrial Electronics, Vol. 58, No. 2, pp. 647-659, February 2011

[11] J. Slotine and W. Li, Applied Nonlinear Control. Prentice Hall, New York, 1991.

[12] M. Jafarboland, N. Sadati, and H. Momeni, "Robust Tracking Control of Attitude Satellite with Using New SMC and EKF for Large Maneuvers", IEEEAC paper #1022, Version 5, Updated October 31, 2005

[13] J. L. Crassidis, S. R. Vadali, and F. L. Markley, "Optimal Tracking of Spacecraft Using Variable-Structure Control," *Proceedings of the Flight Mechanics/Estimation TheorySymposium*, NASA Conference, pp. 201-214 May 1999.

[14] O Hegrenæs, J.T. Gravdahl, and P. Tondel, "Attitude Control bY Means of Explicit Model Predictive Control, via Multi-Parametric Quadratic Programming.", American Control Conference, Dept. of Eng. Cybern., Norwegian Univ. of Sci. & Technol., Trondheim, Norway, pp 901-906, June 2005.

[15] J. Gießelmann, "Development of an Active Magnetic Attitude Determination and Control System for Picosatellites on highly inclined circular Low Earth Orbits," Master of Engineering RMIT University, June 2006.

[16] Z. Mrozek and S. Tarasiewicz, "Attempting sliding mode controller to mobile robot arc welding process.," paper presented on III Krajowa Konf. Metody i Systemy Komputerowe, pp 369-373, Nov.19-21. 2001.

[17] F. C. Sun, Z. Q. Sun, and G. Feng, "An Adaptive Fuzzy Controller Based on Sliding Mode for Robot Manipulators", IEEE Transactions On Systems, Man, And Cybernetics—Part B: Cybernetics, Vol. 29, No. 4, pp 661-667, August 1999.

[18] M. Reza, M. Hadi, A. J. Koshkouei, S. Effati, "Embedding-Based Sliding Mode Control for Linear Time Varying Systems", Applied Mathematics, pp 487-495, 2011.

AUTHORS PROFILE

Eng. Azza El-Sayed Ibrahim is a PhD student in Computers and Systems Department at the Electronics Research Institute, Cairo, Egypt. She received her Master degree from Faculty of Engineering, Cairo University. Research interest: fault detection and diagnosis in robotic systems, Neural Networks, and satellite attitude control. azza@eri.sci.eg

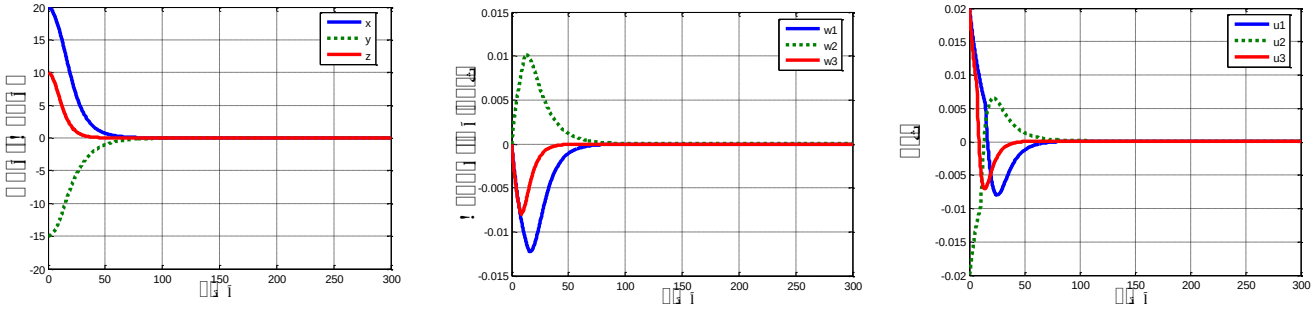


Figure 4. Attitude , body angular velocity and the control signal response in case of SMC Controller

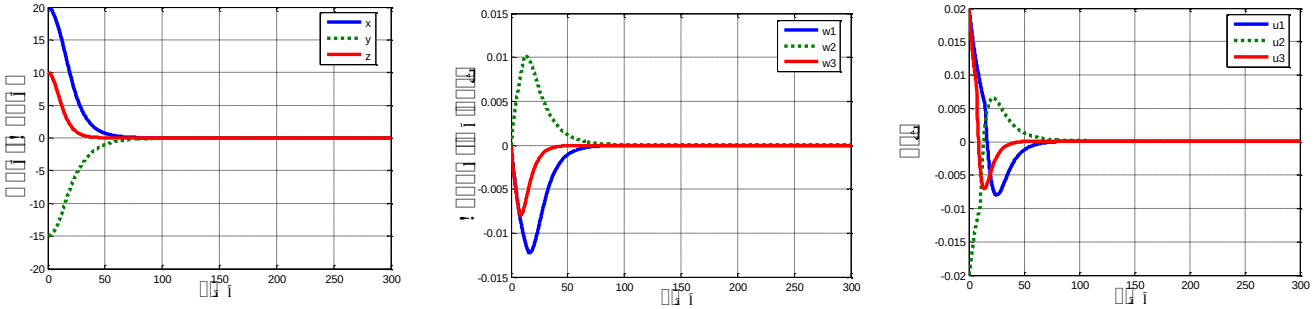


Figure5. Attitude , angular velocity and the control signal response in case of PD Controller

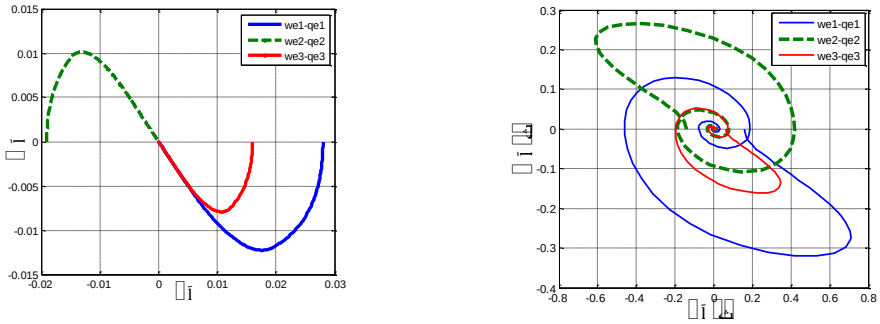


Figure. 6: a) Phase portraits ωe vs qe in SMC b) Phase portraits ωe vs qe in PD

Dr. A. Tobal is an Associate Prof. at the Electronics Research Institute, Cairo, Egypt. He received his B.Sc., M. Sc. And Ph. D. from Faculty of Engineering, Cairo University in 1990, 1994 and 1999 respectively. His fields of research include embedded systems implementation, digital signal processing, Biological Neural Network, pattern recognition and Artificial Intelligence. Dr. Ahmed actively participated in the design, implementation and commissioning of the first Egyptian remote sensing satellite "MisrSat 1" launched successfully in 17/04/2007. tobal51000@yahoo.com

Dr. Mohamed A. Sultan obtained his B.Sc. with honors in Electronics Engineering in 1979. He obtained his M.Sc. and Ph.D. in Control Engineering in 1982 and 1987 respectively. Since 1987 he was appointed as Assistant Professor, Associate Professor and Professor of Control Engineering in 1999 at the faculty of Engineering in Cairo University. His research interests include stochastic control, self- tuning and Predictive control. msultan@cu.edu.eg

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

The Evaluation of Performance in Flow Label and Non Flow Label Approach based on IPv6 technology

1st Nevila Xoxa Resulaj
Albanian Academy of Science,
Tirane, Albania
nresulaj@yahoo.com

2nd Nevila Baçi Kadzadej
University of Tirana, Faculty of Economic, Mathematics, Statistics and Applied Informatics Department,
Tirana, Albania
nevila.baci@unitir.edu.al

3rd Igli Tafa
Polytechnic University of Tirana Faculty of Information Technology,
Computer Engineering Department,
Tirana,Albania
itafaj@gmail.com

***Abstract* - In this paper, we want to evaluate the performance of two broadcasters with Flow label and Non flow label approach. Experimentally we have presented that the throughput utilization for each broadcaster with Flow Label approach which is implemented in MPLS Routing Technology is 89,95%. This result is better than Non Flow Label approach which is evaluated at 92,77%. The aim of this paper is to present that MPLS Routers performance is better than IP routers especially in Throughput Utilization, Low Level of Drop Packet Rate and time delay. The second technology is implemented in IP routing. Experimentally we have generated some video stream packets between 2 broadcasters with an arrange of router nodes. Experiments are performed by using ns-2 simulator.**

Keywords-MPLS technology, IP routing technology, Throughput, Flow-Label approach, ns-2 simulator

1. INTRODUCTION

As we know IPv6 is a recent technology of communication and it gives a lot of improvements compared to IPv4 [5], [2], [3]. These improvements based on features upgraded by the Internet Engineering Task Force (IETF), for example, the increase of the address space from 32 bits to 128 bits or the increase of some significant QoS conditions. By using the recent multimedia applications technologies [7], internet providers, companies, subscribers and the researchers will take some benefits. The Internet Protocol (IP) is considered to be a best effort service, so in the future, the TV broadcasters will use the IP address for communication. In other words, there will be a convergence of the broadcast network with the IP to form the Internet Protocol Television (multimedia with IP) under the recent development.

There are built some policies based on flow-labels to manage the routing of the packets (channels) to the nodes (subscribers) during the transmission with IP-multimedia approach.

For example, a broadcaster can tend to utilize the full bandwidth from the network manager, but meanwhile the network manager asks fairness in distributing packets to the remaining broadcasters [5], [6]. As it know throughput is one of the important feature of QoS Routing, because the management of throughput offers a better QoS performance. It is interesting to mention that IPv6 not only overcomes the shortcoming problems in the IPv4, but also it takes the benefits in Quality of service (QoS). QoS in IPv6 plays an important role in the Stream Model Approach between broadcasters [1], [4]. In [3] the packet's traffic on channel is organized without flow label technology. Flow label technology means that instead of router nodes (fig 1) based on IP routing we can use MPLS routers. MPLS technology has some advantages, but the most one is speed routing. Based on some executed tests we can present that bandwidth utilization is another good feature compared with IP routers technology.

The objective of this paper is to highlight our simulation results in terms of two attributes which are the Throughput and Time Computation Performance based on IPv6 technology with flow label packets technology in Multi-channel Stream Approach. Than we want to compare the results of our simulation with non-flow label packets technology in Multi-channel Stream Approach.

The rest of the paper is organized as follows: section 2 briefly discusses the comparison between MPLS and IP routing section 3 presents the experimental analysis and results, in section 4 are given some conclusions and future works and finally are presented the references.

2. COMPARISON BETWEEN MPLS ROUTING AND IP ROUTING.

1. IP routing uses hop-by-hop destination-only forwarding paradigm. When forwarding IP packets, each router in the path has to look up the packet's destination IP

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

address in the IP routing table and forward the packet to the next-hop router. [8]

2. MPLS uses a variety of protocols to establish Label Switched Paths (LSP) across the network. LSPs are almost like Frame Relay or Asynchronous Transfer Mode (ATM) permanent virtual circuit (PVC), with two major differences: they are unidirectional and they can merge (all LSPs toward the same egress router could merge somewhere in the network). One of the protocols [8]
3. MPLS is faster than IP routing because it is based on label
4. MPLS is in 2,5 OSI Layer and IP is in 2 OSI Layer.

3. EXPERIMENTAL ANALYSIS DESIGN AND RESULTS

In this section, we want to test the Throughput and Time Delay based on IPv6 technology with *non flow label packets technology* and *flow label packets* technology in Multi-channel Stream Approach. As we presented above we have used IPv6 technology because it offers more flexibility and QoS features than IPv4

3.1 Experimental Analysis

In the Multi - Stream Approach we have tested up to 10 nodes for 2 broadcasters as end-users. We have used ns2 simulator since it is considered to be powerful, efficient and flexible for simulation. The 10 nodes were tested sequentially starting from 1 node, 2 nodes, 3 nodes, … , 10 nodes, respectively. We have simulated for both broadcasters Video Stream Packets with 1.4 KB packet length, Rate Video Stream is 1.5 MB/sec and Bandwidth is 5 MB. Network topology is BUS. In NS2 simulator we configure RIP version 2 Routing Policy. We have choosen approximately characteristics with real environment [3].

The maximum Video Packet supported by Maximum Transmission Units (MTUs), which include the Maximum Segment Size (MSS) plus the 40-byte header, within TCP/IP traffic. We'd like video packets (which include a smaller header, apparently) to be around 1400 bytes to fit within acceptable limits and eliminate the possibility of broken packets.

Initially, the first broadcaster generate video stream packets to second one by httperf tool. In the first broadcaster we have installed client machine and in the second one we have installed server machine. In server machine we have built Apache Web Server. So the client is sending video packet request by using http protocol to the server machine. On the other hand second broadcaster can generate http video request to the first one. At this moment client machine is transform in server machine and vice versa. Thus at the same time one machine will utilized as client and server by installed Apache Web Server (Apache2 on CENTOS 5.5 OS)

For every experimental phase (by 2, 3 ,4 …10 nodes), we have calculated the throughput , then we have compared the throughput of the nodes into both broadcasters. Previously we have performed experiments with router nodes which are based on IP technology (non flow label technique). We have repeated this experiment with MPLS routers (flow label technique).

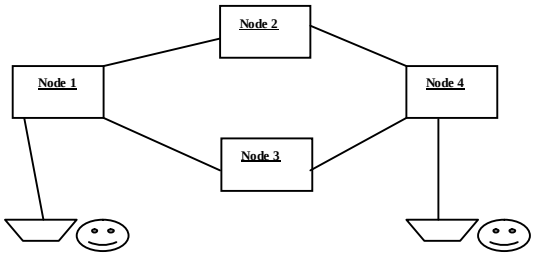


FIGURE 1. Two broadcasters and 4 nodes. The broadcasters generate video packet traffic between nodes

As it look from figure 1 two broadcaster generate video-stream packets at the same time. All these packets are routing on these nodes based on RIP v2 policy.

In [3] the throughput for a determined broadcaster and the number of nodes is calculated as in the following equation:

$$Throughput = \frac{Num(SBW) - Num(RBW)}{Num(SBW)} \times 100\% \quad (1)$$

Throughput: The amount of the non-lost received bandwidth.

Num. (SBW): The amount of the bandwidth provided by the network manager. Packets should be sent to all nodes of the determined broadcaster.

Num. (RBW): The amount of the bandwidth that is received from the determined broadcaster. This amount should get different value than SBW, because some packets have to lost during routing.

3.2 Simulation Results

In order to evaluate our method, the main attribute is the Throughput between the nodes and their broadcasters. We did compare the throughput behavior of each broadcaster with their nodes starting from 1 node and increasing the size to 10 nodes, based on IP routing protocol. The experiment presents that the total throughput for the 2 broadcasters with 10 nodes with IP routing technology is 92.77% . If we use the Non-Flow Label Technique which means that we can replace the IP routers with MPLS routers, with the same policy routing (RIP) with 2 broadcasters which generate the same packet traffic, the total throughput utilization for each broadcaster is decrease to 89,95%. This means that one broadcaster can use the same number of video stream packet generated with smaller utilization bandwidth. All router nodes in figure 1 are configured with IPv6 address. The total number of packets generated from each broadcaster is 1000. As it looks from table 1 and table 2, if the number of nodes is

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

increased the total throughput utilization for each broadcaster is decreased linearly. The number of dropped packets increased linearly if the number of nodes increased too (table 3,4). Each node can introduce drop packets (the reason are buffer, architecture of routers etc). In this paper we compared the percentage of dropped packets and time delay between 2 technologies, non-flow labels packet and flow labels packet as it shows in table 3-6.

TABLE 1. The throughput results for each broadcaster and a defined number of nodes without flow labels technology (IP)

Nr of Nodes	Throughput
1	94.401%
2	94.227%
3	94.055%
4	93.901%
5	93.607%
6	93.414%
7	93.243%
8	93.134%
9	92.998%
10	92.777%

TABLE 2: The throughput results between 2 broadcasters and number of nodes with flow labels technology (MPLS)

Nr of Nodes	Throughput
1	91.015 %
2	91.012 %
3	91.007 %
4	91.004 %
5	90.452 %
6	89.970 %
7	89.967 %
8	89.961 %
9	89.960 %
10	89.957 %

TABLE 3: The percentage of dropped packets between 2 broadcasters and nodes with non-flow label packet (IP)

Nr of Nodes	Drop Packets
1	1.025 %
2	1.142 %
3	1.272 %
4	1.444 %
5	1.652 %
6	1.876 %
7	2.067 %
8	2.261 %
9	2.480 %
10	2.631 %

TABLE 4: The percentage of dropped packets between 2 broadcasters and nodes with flow label packet (MPLS)

Nr of Nodes	Drop Packets
1	1.024 %
2	1.140 %
3	1.271 %
4	1.441 %
5	1.652 %
6	1.875 %
7	2.067 %
8	2.260 %
9	2.480 %
10	2.630 %

TABLE 5: Time delay in MS Approach with non-flow label packet (IP)

Nr of Nodes	Time delay
1	2,16 ms
2	3,44 ms
3	5,99 ms
4	8,32 ms
5	9,99 ms
6	11,39 ms
7	14,22 ms
8	17,86 ms
9	21,62 ms
10	26,55 ms

TABLE 6: Time delay in Multi-Stream Approach with -flow label packet (MPLS)

Nr of Nodes	Time delay
1	1,66 ms
2	2,56 ms
3	3,77 ms
4	6,20 ms
5	8,52 ms
6	9,98 ms
7	11,04 ms
8	12,56 ms
9	14,24 ms
10	14,89 ms

We have presented graphically, throughput utilization and time delay (figure 2 and figure 3) based on the flow-label technology. In figure 3 time delay increases linearly when the number of nodes increased too, because each router nodes introduce a slight delay. In figure 2 throughput utilization is decreased when the numbers of nodes is

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

increased. As we mentioned above the reason is increasing of data rate lost for each node. We have a sensitive reduction of throughput utilization, between node 4 and node 6. This was happen because in those nodes the ratio of drop packets is bigger than 3 nodes. After 6 nodes the drops of packet are stabilized.

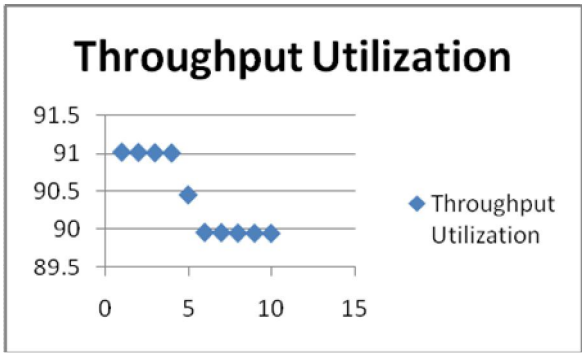


FIGURE 2. Throughput results between 2 Broadcasters.

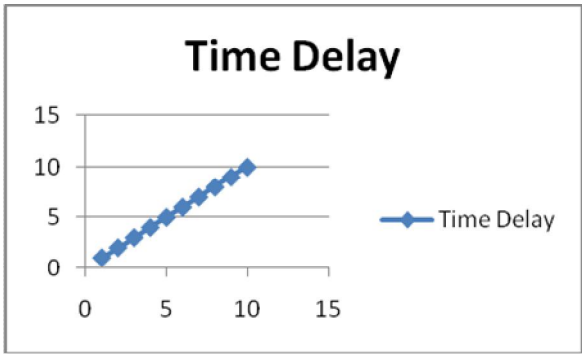


FIGURE 3. Time delay between 2 Broadcasters.

4.CONCLUSIONS AND DISCUSSIONS

1. As it look from table 3 and table 4 the drop packets rate are similarity for both methods (flow label and non-flow label). This is because both routers have the same buffers, so it doesn't affect the performance of drop packets routing.
2. If we compare table 5 and table 6 the difference of time is visible. This is because MPLS routers characterized from a fast routing technology. The reason is routing packet which are based on labels, not in IP. This is an important feature of the best throughput utilization in flow label technology, descripted in table 2 compared with non-flow label technology in table 1.

In the future we will increase the number of broadcasters and routers. Also we will generate the dynamic length of video stream packets in order to evaluate the throughput utilization performance and time delay in WAN

5.REFERENCES

[1] Almadi M.A, Idrus R, Ramadass S, Budiarto R, "A Proposed Model for Policy-Based Routing Rules in the IPv6 Offering QoS for IPTV Broadcasting," *International Journal of Computer Science and Network Security*, IJCSNS, VOL.8 No.3, March 2004, pp. 163-173, 2008.

[2] Cho K, Luckie M, Huffaker B, "Identifying IPv6 Network Problems in the Dual-Stack World" In *Proceedings of the Annual Conference of the Special Interest Group on Data Communication*, SIGCOMM'04, Portland, Oregon, USA, 30 August- 3 September 2004.

[3] Liang, J, Yu B, Yang Z, Nahrstedt K.. "A Framework for Future Internet-Based TV Broadcasting," In Proceedings of the International World Wide Web Conference, multimedia with IP Workshop, Edinburgh, Scotland, United Kingdom, 2006

[4] Pezaros DP and. Hutchison D. "Quality of Service Assurance for the next Generation Internet," In Proceedings of the 2nd Postgraduate Symposium in Networking, Telecommunications and Broadcasting (PGNet'01), Liverpool, UK, June 18-19, 2001.

[5] Pezaros D.P, Hutchison D, Gardner R.D, Garcia F.J and Sventek J.S, "Inline Measurements: A Native Measurement Technique for IPv6 Networks," In *Proceedings of the International Conference of the IEEE for Networking and Communication*, pp. 105-110, 2004.

[6] Silva J. S, Duarte S, Veiga N, and Boavida F,"MEDIA – An approach to an efficient integration of IPv6 and ATM multicast environments," [Online]. Available: http://cisuc.dei.uc.pt/dlfile.php?fn=171_pub_SaSilva.pdf&get=1&idp=171&ext= April 12, 2008.

[7] Zhiwei Y, Guizhong L, Rui S, Qing Zh, Xiaoming Ch, Lishui Ch. "School of Electronics and Information Engineering Xi'an Jiaotong University, Xi'an, China 710049, "A Simulation Mechanism for Video Delivery Researches, 2009

[8] http://searchtelecom.techtarget.com/answer/What-is-the-difference-between-MPLS-and-normal-IP

AUTHORS PROFILE

Nevila XOXA RESULAJ, studied Computer Science at the Faculty of Natural Sciences where she obtained her MSc. in 2001 and since March 2012 is a student of Ph.D. at this Faculty. She is ICT Administrator at Academy of Sciences of Albania, part-time pedagogue at Polytechnic University of Tirana for the course "Fundamentals of programming in C", part-time pedagogue at University of Tirana, Faculty of Economy for the course "Informatics" and part-time pedagogue at University of Tirana, Faculty of Natural Sciences, Department of Informatics for the course "Computer organization" and the course "Introduction to Informatics".

Nevila BACI KADZADEJ, is prof.assoc since September 2011, at University of Tirana, Faculty of Economy, Department of Mathematics - Statistics – Applied Informatics. Also she is Research associate at Centre for Research and Development Tirana. Since 2001 attached to this institute as statistic expert in implementation of conducting business surveys (manufacturing and construction sector) with EU methodology in Albania. She is member of some important projects in Albanian such as: Assessment of business constrains in manufacturing sector, Administrative constrains in construction sector, Assessment of micro enterprises activity in Albania, Strengthening institutional capacities of NPO in Shkodra region for improvement the social assistance scheme, etc.

Igli TAFA, is PhD Student at Polytechnic University of Tirana, Computer Engineering Department. Since 2003 he is assistant pedagogue at this Department. He has finished the Master Degree at 2007. Also he has participate in some projects such as: See Grid, FP7 etc.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

False Colour Composite Combination Based on the Determinant of Eigen Matrix

Maha Abdul-Rhman Hasso

Department of Computer Science, College of Computer Sciences and Math.,

University of Mosul / Mosul, Iraq

Maha_hasso@yahoo.com

***Abstract*— In remote sensing applications, a wise selection of the best colour composite images out of many possible combinations is necessary to ease the job of the interpreter and to overcome the data redundancy problem.**

This work includes a novel method for ranking the available three-band combinations according to the amount of information they contain. The method is based on measuring the determinant of the variance/covariance matrices of each possible combination. The consistency of the method is described and proven using the Eigen value matrix. However for ranking calculation the variance/covariance matrix is enough.

I. INTRODUCTION

In most of the remote sensing application colour composite image represent an important stage in the whole process of information extraction [1]. Due to the fact that most of the available sensors on board the current satellite portray the earth surface in more than three bands, the selection of the most important combination becomes a crucial matter in any application.

In the case of MSS sensor six different combinations of false colour composite can be made out of the four available bands. Whereas in the TM-sensor case thirty-five combinations can be made out of the seven bands of the sensor.

Given the fact that the spectral resolution of the future sensors in expected to be increased.

This number of combinations is expected to be increased for the next generation of the sensors which are expected to contain more than seven bands.

For image interpreter, dealing with that number of false colour composite images is a difficult task. Therefore, the selection of the most informative combination becomes a necessary step prior to any image analysis and interpretation. This work is involves the introduction of new method for ranking the available combination according to the amount of information (colours) that they may contain.

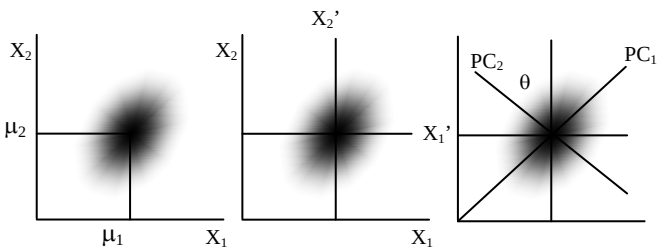
II. CONCEPTS OF COLOURS SPACE

Colours space is a three dimensional feature space whose axes are represented by the three primary colours RGB. In generating colour composite images, the gray levels of each image are projected on one of these axes. The resultant distribution shows the range of colours that can be generated.

The more space the distribution occupies the more range of colours that can be generated.

Multispectral images taken by satellite sensors show a substantial degree of correlation. This is partly due to the natural similarity between the spectral characteristics of the cover types and partly it is due to the limitation of the spatial and spectral resolution of the satellite sensors.

The length of each principal axes represent the square root of the data variance along that particular axis [1]. Thus, if the data distribution is rotated (linearly transformed) using principal component transformation, the resultant eigen value matrix will show the diagonal element as the variance of the output component and the off diagonal, which are zeros, as the covariance between the output component. Thus, the more close these diagonal element, are the more scattering of the data will be along the direction of the second & third principal component axes. Thus the volume of the distribution can be calculated simply by multiply the three diagonal axes. For example, an eigen value matrix with the diagonal elements of 8, 4 and 2 will produce a volume of 64 while if these eigen value are changed 7, 4, and 3 with their sum remaining the same, the resultant volume will be 84.



http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Figure (1), the separation axis between each two bands. X_1, X_2 *the bands,* μ *is the mean and PCs are the principle component axis*

III. Previous methods

Several strategies and methods exist for selecting the combinations that suits the application in hand. Some of them are based on the spectral characteristics of the existent cover types and others are based on some statistical measurements of the images.

In applications that motivate mapping or separation of specific cover type such as mineral exploration and vegetation mapping, the selection of the bands is made according to the spectral characteristics of the mineral indictors and vegetation [7]. For instance vegetation shows high reflectance at the near infrared band while iron oxide, which is a good indicator of the mineral prospected areas, shows an absorption feature at the same band. Thus, the inclusion of bands in the colour composite combination may be useful for discriminating these two cover types. However, in applications that motivate general mapping of the existence cover types the selection of the bands is made according to their position in the spectrum. For instance, one band from the visible region, one band from the near infrared region and one band from the middle or thermal infrared region are selected. This strategy is justified by the fact that naturally the spectral response of a particular cover type, more likely, shows more variation between two distinct bands than between two adjacent bands. Accordingly, for TM sensor bands 147 may be chosen.

In addition to these strategies several methods based on statistical properties of the available bands were introduced. One of these methods takes into account the degree of correlation between the possible pairs of the available bands and the best combination is chosen by selecting the bands that show least correlation [3-4]. However, this method does not take into account the variance of the available bands. That is, bands with high variance (more information) may be discarded.

The other method is based on the variance of the available bands. That is bands which show high variances are selected. This method again shows a limitation since it does not take into account the degree of correlation between bands. Thus there will be information redundancy. That is, bands with high variance that show high degree may be selected. According to Figure (1) this will result a colour composite image with law saturation, i.e. few colours, each with more different shades (narrow range of colours). Chavez (1983) introduced a method that takes into account both, the degree of correlation between the bands and the variance of the bands [2]. That was the calculation of The Optimum Index Factor (OIF) to select a three-band combination that displays the greatest details among a maximum of 20 bands by formulating the following equation:

$$OIF = \sum_{i=1}^{3} SD_i / \sum_{j=1}^{3} |CC_j|$$

Where *SDi* is the standard deviation of band *i* and $|CC_j|$ is the absolute value of the correlation coefficient between any two of the possible three pairs. According to Chavez et al., the highest values of OIF should be the three bands having the most information content. This measure favours the selection of those bands having high variances and low pair-wise correlation [5].

IV. Present method, The Determinant Based method

Referring to Figure (1), it is clear that the more the three axes of the ellipsoid are close to each other the more scattering of the distribution will be across its diagonal. Thus, more colours will be generated.

In most of the remote sensing study, the distribution of the data is assumed Gaussian or near Gaussian. Thus, the axes of the ellipsoid will represent the three principle axes of the distribution.

This proofs, that the more close the eigen value are the more space the distribution occupy and accordingly a better colourful image can be produced. The multiplication of the three diagonal element of the eigen value matrix is equivalent to the determinant of the variance/covariance matrix [6]. Since the shape of the distribution is invariant under rotation. That is, the determinant of the covariance matrix is positive, i.e.,

$$\mathrm{Det}(\mathrm{C_X}) = \prod_{\mathrm{i}=1}^{\mathrm{n}} \lambda_{\mathrm{i}} \geq 0$$

The eigenvectors of the covariance matrix transform the random vector into statistically uncorrelated random variables, i.e., into a random vector with a diagonal covariance matrix.

V. Application to TM images

The given method is applied to a multispectral images of TM-sensor, thermal bands is excluded. Twenty combinations can be making out of six remaining bands.

The Table (1) shows the ranking and combination of the applied OIF method and the proposed DET method.

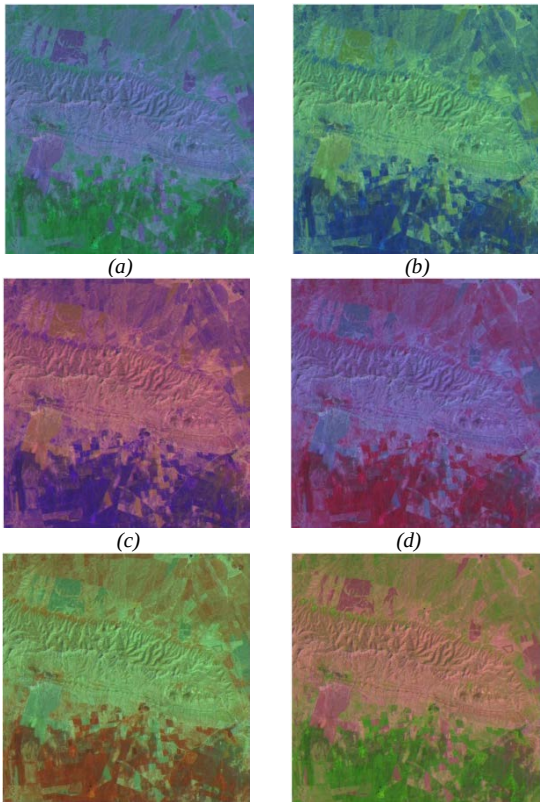
Table (1) shows the ranking of the twenty combination using the OIF method and determinate method.

Combine	OIF	Band i	Band j	Band k	DET	Band i	Band j	Band k
1	69.5493	3	4	5	19154201.94	3	4	5
2	67.4986	4	5	6	11163892.05	1	4	5

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

3	65.6903	3	4	6	10055252.29	3	4	6
4	63.1119	1	4	5	6983970.83	1	4	6
5	60.1420	1	4	6	5969593.84	2	4	5
6	57.0226	2	4	5	5006852.82	4	5	6
7	54.5363	1	3	4	4016074.97	1	3	5
8	53.0176	2	4	6	3877119.68	1	3	4
9	43.3697	2	3	4	3352550.15	2	4	6
10	42.3461	1	2	4	3332290.24	3	5	6
11	29.3038	3	5	6	2346223.25	1	3	6
12	27.9850	1	5	6	1983992.73	1	5	6
13	27.4343	1	3	5	1164365.92	1	2	5
14	25.9559	2	5	6	1126517.91	1	2	4
15	24.4786	2	3	5	1046195.57	2	5	6
16	23.9083	1	3	6	718679.35	1	2	6
17	23.8683	1	2	5	429827.41	2	3	5
18	20.9303	2	3	6	236031.38	2	3	4
19	20.4402	1	2	6	215006.70	2	3	6
20	18.2356	1	2	3	80846.22	1	2	3

From the table above it is clear that the best combination of false colour composite is bands 3,4,5 that gives the maximum OID and determinate. Figure (2) shows the false colour composite of TM-bands to RGB image with the reversed combinations of bands 3,4,5 on red, green and blue colours.



(a) *(b)* *(c)* *(d)* *(e)* *(f)*

Figure (2) Two False colour composite combination of bands 3,4,5 to RGB. a) bands 3,4,5 ; b) bands 3,5,4; c) bands 4,5,3 ; d) bands 4,3,5 ; e) bands 5,3,4 ; f) bands 5,4,3.

As shown in the figure (2), the best combination visually interpreting is when the band 5 is coloured as red, band 4 is green and band 3 is blue.

VI. Conclusion

Remotely sensed data colouring is important for easy vision and interpretation. The calculation of the eigen value matrix is not necessary since the multiplication of the three diagonal element of the eigen value matrix is equivalent to the determinant of the variance/covariance matrix. It is clear that in some cases the OID & DET gets the same combination but this combination is not the best. The best combination is the highest value of OID and DET(bands 3,4,5) which means that these bands has good amount of information with minimum of data redundancy.

References

[1] C. Ayday, E. Gümüşlüoğlu *" Detection And Interpretation Of Geological Linear Features On The Satellite Images By Using Gradient Filtering And Principal Component Analysis"*, The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences. Vol. XXXVII. Part B8. Beijing 2008

[2] Chavez, P.S., Jr., G.L. Berlin, and L.B. Sowers, *"Statistical Method For Selecting Landsat Mss Ratios"*, Journal of Applied Photographic Engineering, 8(1):23-30, 1982.

[3] Ehsani, A . H . & Quiel, F. *"Efficiency of Landsat ETM+ Thermal Band for Land Cover Classification of the Biosphere Reserve "Eastern Carpathians"* (Central Europe) Using SMAP and ML Algorithms", Int. J. Environ. Res., 4(4):741-750 , Autumn 2010

[4] Laurence A. Soderblom, Robert H. Brown, Jason M. Soderblom, Jason W. Barnes, Randolph L. Kirk,Christophe Sotin, Ralf Jaumann, David J. Mackinnon, Daniel W. Mackowski, Kevin H. Baines, Bonnie J. Buratti, Roger N. Clark, Philip D. Nicholson *"The geology of Hotei Regio, Titan: Correlation of Cassini VIMS and RADAR"*, iIcarus 204 (2009) pp., 610–618, Published by Elsevier Inc., 2009.

[5] M. Beauchemln and KO B. Fung *"On Statistical Band Selection for Image Visualization"*, Photogrammetric Engineering & Remote Sensing Vol. 67, No. 5, pp. 571-574. American Society for Photogrammetry and Remote Sensing, May 2001.

[6] Michael McCourt, *"A Stochastic Simulation for Approximating the log-Determinant of a Symmetric Positive Definite Matrix"* ,December 15, 2008, http://www.thefutureofmath.com/mathed/logdet.pdf

[7] Randall B. Smith, *"Introduction to Remote Sensing of Environment (RSE)"* , ©MicroImages, Inc., 4 January 2012.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Source Initiated Energy Efficient Scheme for Mobile Ad Hoc Networks

R.Bhuvaneswari
Anna University of Technology, Coimbatore
Coimbatore, India

Dr.M.Viswanathan
Senior Deputy Director, Fluid Control Research Institute (FCRI),
Palakkad, Kerala, India.

***Abstract* - In Mobile Ad Hoc Networks (MANETs), nodes are organized in a random manner without any centralized infrastructure. Due to node mobility and limited bandwidth, nodes consume more power unnecessarily. Mobile nodes collects the route information through overhearing and stores these information in route caches through Dynamic Source Routing (DSR) Protocol. When the route cache freshness is absent, it leads to the stale route information resulting in pollution caches. If the node overhears the packet to another node, node's energy consumption occurs unnecessarily. The main goal of this research work is to reduce the effect of overhearing and avoid the stale route problems while improving the energy efficiency using the Source Initiated Energy Efficient (SIEE) algorithm. Due to the lack of route cache update, the stale route entry and overhearing is originated among the network. For that, we developed five mechanisms to improve route cache performance in DSR. By simulation results the proposed algorithm achieves better performance than the existing methods.**

Keywords - MANET, DSR, Stale route entry, Cache freshness, overhearing, route cache update and energy efficiency.

I. INTRODUCTION

A. *Mobile Ad Hoc Networks (MANET)*

Mobile ad hoc network (MANET) is an infrastructure-less multi-hop network where each node communicates with other nodes directly or indirectly through intermediate nodes. Thus, all nodes in a MANET basically function as mobile routers participating in some routing protocol required for deciding and maintaining the routes. Since MANETs are infrastructure-less, self-organizing, rapidly deployable wireless networks, they are highly suitable for applications involving special outdoor events, communications in regions with no wireless infrastructure, emergencies and natural disasters, and military operations [1].

B. *Dynamic Source Routing (DSR) Protocol and the effects of overhearing*

Dynamic Source Routing protocol is a simple and efficient routing protocol designed especially for use in multi-hop wireless Ad Hoc networks of mobile nodes. DSR allows network to be completely self-organising and self-configuring, without the need for any existing infrastructure or administration [2]. DSR gathers the route information through overhearing. Overhearing improves the routing efficiency in DSR by eavesdropping other communications to gather route information but it spends a significant amount of energy. Overhearing [3] means a node picks up packets that are destined for other nodes. Wireless nodes will consume power unnecessarily due to overhearing transmissions of their neighboring nodes. Wireless nodes consume power unnecessarily due to overhearing the transmissions of their neighbors. This is often the case in a typical broadcast environment. For example, as the IEEE 802.11 wireless protocol defines, receivers remain on and monitor the common channel all the time. Thus the mobile nodes receive all packets that hit their receiver antenna. Such scheme results in significant power consumption because only a small number of the received packets are destined to the receiver or needed to be forwarded by the receiver.

C. Problem of Stale Route in Source Routing

When the link errors [4] (or RERR) are not propagated by route caches often contain stale route information for an extended period of time. Including this, the erased stale routes are possibly un-erased due to in-flight data packets carrying the stale routes. If a node has an invalid route in its route cache or receives a Route Reply that contains an invalid route, it would attempt to transmit a number of data packets without success while consuming energy. The design choices for route cache in Dynamic Source Routing protocol and concluded that there must be a mechanism,

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

such as cache timeout, that efficiently expels stale route information.

The main cause of the stale route problem is node mobility. It is unconditional overhearing that dramatically exaggerates the problem. This is because DSR generates more than one RREP packets for a route discovery to offeralternative routes in addition to the primary route to the source. While the primary route is checked for its validity during data communication between the source and the destination, alternative routes may remain in route cache unchecked even after they become stale. This is the case notonly for the nodes along the alternative routes, but also for all their neighbors because of unconditional overhearing.

II. PREVIOUS WORK

Hu C et.al [5] developed the 802.11 Power Saving Mode (PSM) applicable in multihop MANET with Dynamic Source Routing (DSR) protocol. The drawback in integrating the DSR protocol with 802.11 PSM comes from unnecessary or unintended overhearing and DSR depends on broadcast flood of control packets.

Lim S et.al [6] explored a mechanism called RandomCast mechanism. Here a node may decide not to overhear i.e. a unicast message and not to forward and a broadcast message when it receives an advertisement during an ATIM window, thereby reducing the energy cost without affecting the network performance. In addition to the energy consumption, overhearing brings in several undesirable consequences. It could aggravate the stale route problem, the main cause of which is node mobility.

Sree Ranga Raju [7] proposed a conservative approach to gather route information. It does not allow overhearing and eliminates existing route information using timeout. This necessitates more RREQ messages which in turn results in more control overheads in routing**.**

Laura marie feeney [8] analysed the energy consumption model for routing protocols in ad hoc networks. They have also shown that new insights are provided into costly protocol behaviours and suggests opportunities for improvement at the protocol and link layers.

Ramesh et.al [9] explored a new scheme called efficient energy management to achieve minimum energy consumption with the presence of overhearing. Here they have proposed five modules like networking module, packet division module, randomcast module and energy efficient balancing module in order to avoid redundant rebroadcasts and thus save additional energy.

Ashish K et.al [10] & Charles E Perkins et.al [11] proposed the on-demand routing protocols DSR and AODV, before sending a packet to the destination, discovers a route. Route maintenance is invoked when node detects link failure. In order to avoid route discovery for each packet, on-demand routing protocols utilizes cache routes previously learnt.

Ashish Shukla [12] proposed a cache timeout policy to predict route cache lifetime, and to expunge stale route cache entries, which are timed out. Many techniques have been proposed for route cache organization and its effect on the performance of on-demand routing protocols. But the concentration of cache timeout policy is very less.

It is used in route cache implementation to prevent stale route from being used. So, a technique for reducing the unintended overhearing of neighboring nodes is done with the help of RandomCast mechanism and for prevention of stale route problem, a cross-layer cache timeout policy is implemented. Time out policy derives cache timeouts of individual links that are present in route cache by utilizing Received Signal Strength Indicator (RSSI) information. So to fulfil the objective and to overcome the drawbacks, a message overhearing and forwarding mechanism called RandomCast [4] is chosen which makes a judicious balance between energy and network performance.

Sangeetha et.al [13] used the prediction mechanism and smart prediction mechanism which performs better than EOLSR protocol and reduce traffic load. In MANET state information such as residual energy level plays an important role in route selection. If latest information is not collected by nodes, then performance may degrade. They have also evaluated the effect of time at which state information was collected in ideal and realistic approach and concluded that although ideal approach is better than realistic but increase in frequency of packets improve the performance very little and also increase traffic overhead.

B. H. Liu [14] used hello messages to distribute transmission power, and uses the minimum power required to connect to a neighbor, while considering the costs of reception of a packet at the neighboring nodes.

Freeny [15] suggests that if ATIM window is fixed then energy saving can be affected. DPSM improves this performance by using the variable ATIM window. It allows the sender and receiver node to change their ATIM window dynamically. The ATIM window size increased when some packets are pending after the current window is expired. The data packets carry the current length of the ATIM window and the nodes overhear this modify their ATIM window length. DPSM allows the sender and receiver node to switch of their radio immediately after their transmission is over. The energy saving performance of DPSM is better as compare to IEEE 802.11 DCF in term of power saving however it is computationally more complex.

S.Singh and C.S.Raghavendra [16] projected energy efficiency technique which is achieved by using two separate channels, one for control and other for data.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

RTS/CTS signals are transmitted over the control channel while data are transmitted over data channel. Nodes with packet to transmit sends a RTS over the control channel, and waits for CTS, if no CTS they receives within a specific time then node enters to a backoff state. However, if CTS is received, then the node transmits the data packet over the data channel. The receiving node transmits a busy tone over the control channel for its neighbours indicating that its data channel is busy. The use of control channel allows nodes to determine when and how long to power off. The length of power off time is determined by different condition. After waking up, a node access the channel over the data channel and found multiple transmission going on. The node uses a probe protocol in this case to find how much time it will power off. Simulation results shows that good range of power saving is achieved.

In IEEE 802.11[17] standard protocols, it has two types of power managements. First type is known as power save (PS) mode for infrastructure based wireless network and the second type is known as IBSS Power Saving mode, which is for infrastructure-less networks. In the former method nodes in PS mode consume less power compare to active mode operation. The access point buffered the Media Authentication Code (MAC) service date unit (MSDU) and transmits them at designated time by the help of Traffic Indication Map (TIM) and delayed traffic indication map (DTIM). This type of power saving mechanism is not suitable for ad hoc network environment as there is no central coordinator like access point. On the other hand IBSS PS mode is applicable to fully connected single hop network where all the nodes are in the radio range to each other. Synchronized beacon interval is established by the node which initiates the IBSS and is maintained in a distributed fashion. All the nodes wake at the beginning of the beacon interval and wake till the end of the traffic window. The nodes participating in the traffic announcement remain awake till the end of beacon interval and the non-participator goes to sleep to conserve energy at the end of the traffic window. The amount of energy conserve by a node depends upon the time spent in the sleep state which can be affected by the state transition from sleep to active mode operation. The energy saving performance also depends upon the network size as well as on the length of the ATIM window and beacon interval duration.

Sofiane Boukli Hacene et.al [17] improved the promising DSR routing protocol for ad hoc networks. They have equipped DSR with expiration time technique for routes in route cache. This technique has been inspired from route management in the routing table of Ad Hoc on Demand Distance Vector (AODV) routing protocol, in order to avoid the use of stale route in routing. The performance of the proposed technique was evaluated and compared with DSR using detailed simulations. Several common performance metrics were considered. The proposed technique can overall generate lower communication overhead, fewer broken links and lower average end-to-end delay.

The paper is organized as follows. The Section 1 describes introduction about MANET, overview of DSR protocol and stale route problems in DSR. Section 2 deals with the previous work which is related to the energy consumption. Section 3 is devoted for the implementation of source initiated energy efficient algorithm. Section 4 describes the performance analysis and the last section concludes the work.

III.IMPLEMENTATION OF SOURCE INITIATED ENERGY EFFICIENT (SIEE) ALGORITHM

In our proposed technique, we have used four mechanisms in order to avoid stale route problems, achieve minimum energy consumption. Dynamic Source Routing aggressively uses route caching. Using source routing, it is possible to cache every overheard route without causing loops. If any forwarding node caches any source route in a packet, it forwards the packets for possible future use. The destination node replies to all requests. Thus the source node learns many exchange routes to the destination nodes that are cached. Swap routes are useful in case the primary route breaks. If any intermediate node on a route learns routes to the source and destination as well as other intermediate nodes on that route. A large amount of routing information is gathered and cached with just a single query reply cycle. So these cached routes may be used in replying to subsequent route queries. The reply from caches provides dual performance advantages. First, it reduces route discovery latency and without replies from caches the route query flood will reach all nodes in the network. Cached replies satisfy the query flood early, thus saving on routing overheads.

If without an effective mechanism, stale cache entries are removed. Then, route replies may carry stale routes. Attempted data transmissions using stale routes incur overheads and generate additional error packets and can potentially pollute other caches when a packet with a stale route is forwarded or snooped on. In the following, there are three problems are identified with the DSR protocol that are the root cause of the stale cache problem.

Case i:

If link breaks and route errors are not propagated to all caches that has an entry with the broken link. Instead, the RERR (Route error) is unicast only to the source whose data packet is accountable for identifying the link crack via a link layer feedback. We take only a limited number of caches are cleaned. The failure information is propagated by piggybacking it onto the subsequent route requests from the source. If the route requests may not be propagated network-wide, many caches may remain unclean.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Case ii:

Still now there is no mechanism is proposed to expire stale routes. If not fresh, stale cache entries will stay forever in the cache.

Case iii:

There is no way to determine the freshness of any route information. For an example, even after a stale cache entry is erased by a route error, a subsequent "in-flight" data packet carrying the same stale route can put that entry right back in. This problem is mixed by liberal use of snooping. Stale routes are chosen up by any other node overhearing any transmission. Thus, cache "pollution" can propagate fairly quickly.

Proposed Approaches:

A. Maximum Error Declaration: The proposed approach is based on the idea that bad news should be propagated "fast and wide". In case if we want to increase the speed and we need to the extent of error propagation, so the route errors are now transmitted as broadcast packets at the MAC (medium access control) layer. First, the node that determines the link breakage, broadcasts the route error packet containing the broken link information. Once receiving a route error, a node updates its route cache so that all source routes containing the broken link are shortened at the point of failure.

If node receiving a RERR (Route Error) propagates), it further only if there exists a cached route containing the broken link and that route was used before in the packets forwarded by the node. Note that using this scheme route errors reach all the sources in a tree fashion starting from the point of failure. In effect, route error information is efficiently disseminated to all the nodes that forwarded packets along the broken route and to the neighbors of such nodes that may have acquired the broken route through snooping.

B. Clock based Expiration of Route – If we recall that link breakage is detected only by a link layer feedback, when an attempted data transmission fails. Thus loss of a route will go undetected if there is no attempt to use this route. A more proactive clock-based approach will be able to fresh up such routes. A clock based approach is based on the hypothesis that routes are only valid for a specific amount of time (timeout period) from their last use. Each node in a cached route now has an associated timestamp of last use. This timestamp is updated each time the cached route or part thereof is "seen" in a unicast packet being forwarded by the

node. The main portions of cached routes unused in the past interval are pruned. The advantage of this approach depends critically on the proper selection of the timeout period A very small value for the timeout may cause many unnecessary route invalidations, while a very large value may defeat the purpose of this technique. Although well-chosen static values can be obtained for a given network, a single timeout for all the nodes may not be appropriate in all scenarios and for all network sizes. Therefore, a dynamic mechanism is desirable that allows each node to choose timeout values independently based on its observed route stability. The proposed technique heuristic approach for adaptive selection of timeouts locally at each node based on the average route lifetime and the time between links breaks seen by the node. When a cached route breaks due to link breakage or upon receipt of a route error, the lifetime of the broken route is computed as the time elapsed since it was last entered in the cache. Average route lifetime is obtained using the lifetimes of all broken routes in the past. Time of latest link breakage seen by a node is also maintained.

When route breaks occur uniformly in time, average route lifetime itself provides a good estimate. However when many route breaks occur in short bursts with a large separation in time, the average route lifetime does not accurately predict during the periods of no route breaks. The value of route life time is computed periodically and is used to expire stale entries from the cache. In the experiments, every half a second and route cache is computed then checked for stale entries.

C. Unconstructive Caches – In order to improve error handling in DSR, caching of negative information has already been recommended. In order to make use of this way, every node caches the broken links seen recently via the link layer feedback or route error packets. Within a interval of creating this entry if a node is to forward a packet with a source route containing the broken link, (i) the packet is fallen and (ii) a route error packet is produced. In addition, the negative cache is always checked for broken links before adding a new entry in the route cache. Essentially, route cache and negative cache are mutually exclusive with respect to the links present in them. This prevents the cache pollution problem.

D. Energy Consumption Model

All the discussions in this section and the following sections correspond to a mobile graph $U_M = U_1U_2\ldots U_T$ generated for an source-destination *(s-d)* session by sampling the network topology at instants of packet origination $ts_1, ts_2, \ldots, ts_T$. Let $Pk = v_0v_1\ldots vp$ be the static *s-d* path in $U_i = (R_i, O_i)$ at time *tsi*. Here, v_0 = *source* and v_l = *destination* and $(vp_{-1}, vp) \in O_i$ for $p = 1,2, \ldots, l$ are the hops of the *s-d* path. All the energy consumption calculations for the *s-d* path at time *tsi* are strictly based on the snapshot of the network topology U*i* at *tsi*. Thus the queuing delays and propagation delays are neglected while assuming infinite channels. The packets are being instantaneously transmitted from source *s* to destination *d*.

The energy consumed for a node to node traffic on the *source-destination* path *Pi* is modelled as the sum of the energy consumed along each hop. The energy consumption

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

is modelled per hop considering complete overhearing (non-destination nodes receive the entire data packet), a reduced overhearing case where the non-destination nodes discard the data packet after scanning its header and when there is no overhearing.

The over hearing costs are presented at the non-destination nodes for each of the three following cases:

$$Ptop\_Tx(v_{j-1}) = Transenergy(\frac{Sizeof\ \mathrm{Re}qToSend + Sizeoforiginaldata + PDR}{Bandwidth}) + \mathrm{Re}ceenergy * (\frac{SizeofCleartosend + Acksize + RERR}{Bandwidth}) \quad (1)$$

$$Ptop\_Rec(v_{j-1}) = Transenergy(\frac{SizeofClearToSend + ACKsize + RERR}{Bandwidth}) + \mathrm{Re}ceenergy * (\frac{Sizeof\ \mathrm{Re}qtosend + Datasize + PDR}{Bandwidth}) \quad (2)$$

i. Absolute overhearing

Here the nodes are operating in promiscuous mode. The non-destination nodes at the neighborhood of the sender v_{p-1} are stimulated for receiving the entire data packet. Including these nodes are charged for receiving the Request To Send (RTS) packet. Likewise, the non-destination nodes at the neighborhood of the receiver v_p are charged for receiving the Acknowledge (ACK) and Clear To Send (CTS) packets.

$$\forall\ l \in Nei\_Nodes(v_{p-1}, t_{si}), AOvhe(l, v_{p-1}, t_{si}) = \mathrm{Re}ceenergy * (\frac{Sizeof\ \mathrm{Re}qtosend + Datasize + PDR}{Bandwidth}) \quad (3)$$

$$\forall\ h \in Nei\_Nodes(v_p, t_{si}), AOvhe(h, v_{p-1}, v_p, t_{si}) = \mathrm{Re}ceenergy * (\frac{SizeofClearToSend + ACKsize + RERR}{Bandwidth}) \quad (4)$$

ii. Decreased overhearing

Instead of the receiving the entire data packet, a node could scan only the header of the data packet and discard the remaining of the packet. Thus, the non-destination nodes at the neighbourhood of the sender v_{p-1} are excited for only receiving the data packet header and the Request To Send packet. On the converse, the non-destination nodes at the neighborhood of the receiver *vj* are charged for receiving the ACK and CTS packets. This simple strategy can bring significant power savings when the data size is considerably larger than the size of the header preceding the actual data in the data packet.

$$\forall\ l \in Nei\_Nodes(v_{p-1}, t_{si}), AOvhe(l, v_{p-1}, t_{si}) = \mathrm{Re}ceenergy * (\frac{PSizeof\ \mathrm{Re}qtosend + Data\_Neigh\_size + PDrop}{Bandwidth}) \quad (5)$$

iii. Absence of Overhearing

If node enters the snooze or sleep state when there is an ongoing transmission in its neighborhood in which the node is neither a transmitter nor a receiver. If an intended receiver of the data packet is assumed to be notified by the sender through energy-efficient IEEE 802.11 ATIM frame mechanism [11]. Nodes are assumed to be identified their neighbors through the beacon frames exchanged as part of the power saving mechanism. The energy consumed for the transmission and reception of the ATIM and beacon frames is assumed negligible. Such an assumption may not be completely true because when the topology changes more frequently, power saving strategies require nodes to be awake at least half of the beacon interval. On the other hand, the maximum energy savings are evaluated that could be obtained when the cost of overhearing is totally discarded.

$$\forall\ l \in Nei\_Nodes(v_{p-1}, t_{si}), AOvhe(l, v_{p-1}, t_{si}) = 0 \quad (6)$$

$$\forall\ h \in Nei\_Nodes(v_p, t_{si}), AOvhe(h, v_{p-1}, v_p, t_{si}) = 0 \quad (7)$$

iv. Stale Route Avoidance in DSR

Nodes movements result stale route cache entries. Cache staleness is a big problem in link cache scheme where individual links are combined to find out best path between source and destination. A cache timeout policy is required to expire a route cache entry, when it is likely to become stale. DSR makes aggressive use of route cache to avoid route discovery. The performance of DSR heavily depends on efficient implementation of route cache. In this, a new cross-layer approach for predicting the route cache

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

lifetime is presented. This approach assigns timeouts of individual links in route cache by utilizing Received Signal Strength Indicator (RSSI) values received from wireless network interface card.

```
/* Source Initiated Energy Efficient Algorithm*/
{
if (LB =1)  RERR is transmitted and Route cache is updated
}

if (Tout = 1 ) Valid routes are determined

else if ( Negative caches )
{
 Cache Pollutions are determined  & cache freshness are initiated.
If( CO = 1 )
{
Nodes operating in promiscuous mode.
}
else ( RO = 1)
{
  Node scan only the header of the data
}
if( NO = 1) Maximum Energy Savings are determined.
}
{
Total Energy Consumption = ECO+ENO + ERO
else route cache is updated
}
```

IV. PERFORMANCE ANALYSIS

We use NS2 to simulate our proposed algorithm. In our simulation, 101 mobile nodes move in a 1000 meter x 1000 meter square region for 50 seconds simulation time. All nodes have the same transmission range of 100 meters. The simulated traffic is Constant Bit Rate (CBR). Our simulation settings and parameters are summarized in table 1

TABLE I. SIMULATION SETTINGS AND PARAMETERS

No. of Nodes	101
Area Size	1000 X 1000
Mac	802.11
Radio Range	100m
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	80 bytes
Mobility Model	Random Way Point

A. Performance Metrics

We evaluate mainly the performance according to the following metrics.

Control overhead: The control overhead is defined as the total number of routing control packets normalized by the total number of received data packets.

End-to-end delay: The end-to-end-delay is averaged over all surviving data packets from the sources to the destinations.

Packet Delivery Ratio: It is the ratio of the number .of packets received successfully and the total number of packets transmitted.

The simulation results are presented in the next part. We compare our proposed algorithm with DBEE – CLA [18] and RANDOMCAST in presence of overhearing environment.

Figure 3 shows the results of average end-to-end delay for varying the nodes from 20 to 100. From the results, we can see that SIEE scheme has slightly lower delay than the RANDOMCAST and DBEE-CLA scheme because of authentication routines.

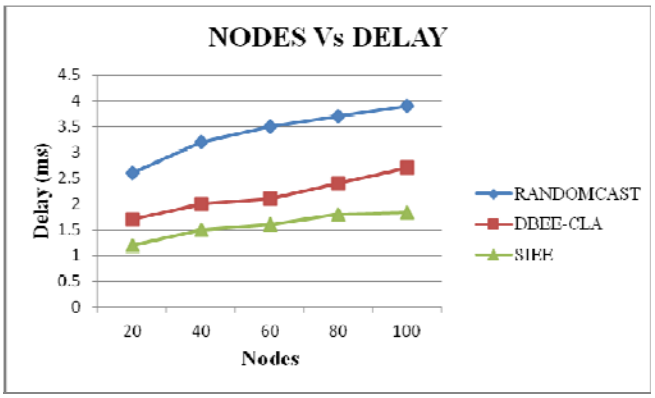


Fig. 3. Nodes Vs End to end Delay

Fig. 4, presents the energy consumption. The Comparison of energy consumption for SIEE, DBEE-CLA, RandomCast. It is clearly seen that energy consumed by SIEE is less compared to RandomCast and DBEE-CLA.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

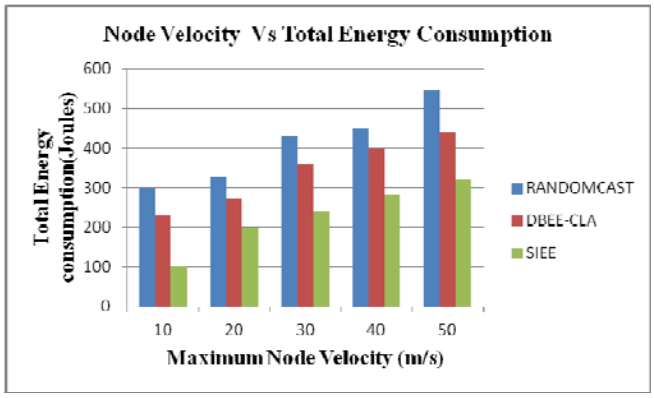


Fig. 4. No.of Nodes Vs Energy Consumption

Fig. 5, presents the comparison of overhead. It is clearly shown that the overhead of SIEE has low overhead than the RandomCast and DBEE-CLA.

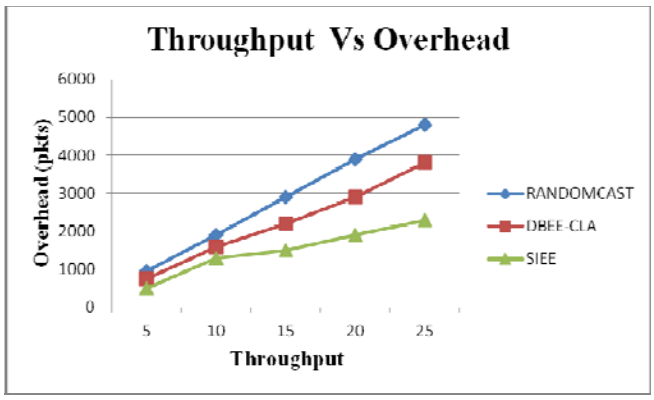


Fig. 5. Throughput Vs Overhead

Figure 6 shows the results of Mobility Vs Delay. From the results, we can see that SIEE scheme has slightly lower delay than the RANDOMCAST and DBEE-CLA scheme because of authentication routines.

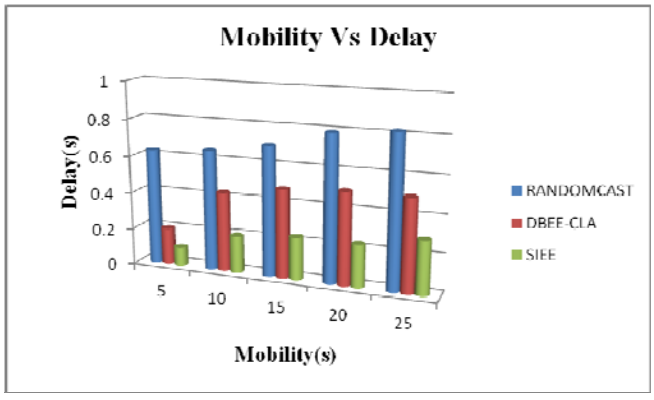


Fig. 6. Mobility Vs Delay

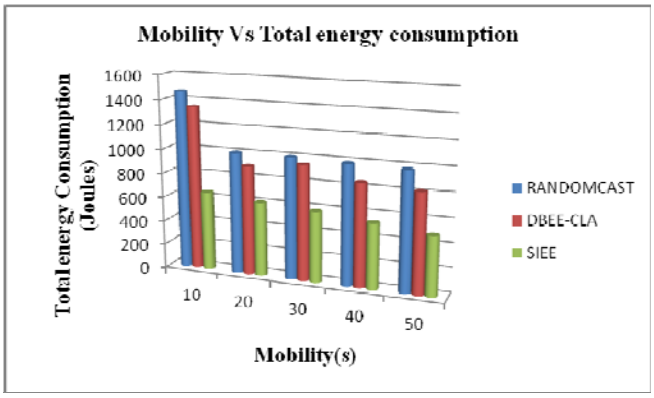


Fig.7.Mobility Vs Overhead

Fig. 7, presents the comparison of total energy consumption while varying the mobility from 10 to 50. It is clearly shown that the energy consumption of SIEE has low overhead than the RandomCast and DBEE-CLA.

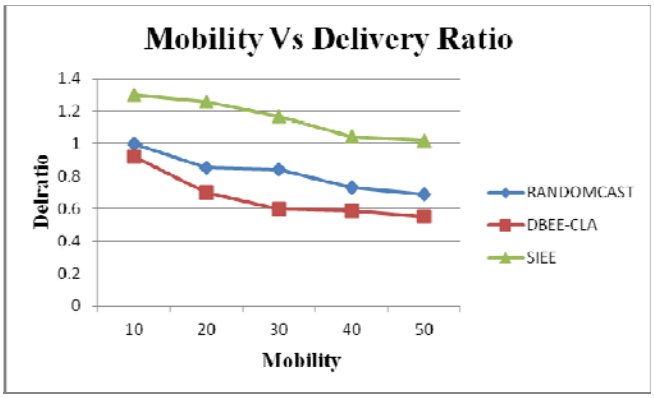


Fig.8. Mobility Vs Packet Delivery Ratio

Figure 8 show the results of average packet delivery ratio for the mobility 10, 20…50 for the 100 nodes scenario. Clearly our SIEE scheme achieves more delivery ratio than the Randomcast and DBEE-CLA scheme since it has both reliability and security features.

V. Conclusion

In MANET, mobile nodes are moving randomly without any centralized administration. Due to that, the node consumes more energy unnecessarily. In this paper, we have developed a source initiated energy efficient algorithm with energy consumption model which attains minimum energy consumption to the mobile nodes. In the first phase of the scheme, route cache update and stale route avoidance is achieved using SIEE algorithm. In second phase, minimum energy consumption is achieved using energy consumption model. It uses three factors called utility factor, energy factor, mobility factor to favor packet forwarding by maintaining minimum energy consumption for each node. We have demonstrated the energy estimation of each node. By simulation results we have shown that the SIEE achieves good packet delivery ratio while attaining low delay,

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

overhead, minimum energy consumption than the existing schemes Randomcast and DBEE-CLA while varying the number of nodes, node velocity and mobility.

REFERENCES

[1]. Perkins C. Ad Hoc Networking: Addison-Wesley: 2001; 1-28.

[2]. David B. Johnson, David A. Maltz and Yih-Chun Hu, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)," Internet Draft, draft- ietf-manet-dsr-09.txt,15April2004.

[3]. Fang Liu, Kai Xing, Xiuzhen Cheng, Shmuel Rotenstreich , "Energy-efficient MAC layer protocols in ad hoc networks" Resource Management in Wireless Networking, Kluwer Academic Publishers, 2004, pp.1-42.

[4]. Lim S, Yu C and Das C, "Rcast: A Randomized Communication Scheme for Improving Energy Efficiency in Mobile Ad Hoc Networks," Proc. 25th IEEE Int'l Conf. Distributed Computing Systems, pp. 123-132, 2005.

[5]. Ashish K. Shukla and Neeraj Tyagi, "A New Route Maintenance in Dynamic Source Routing Protocol," International Symposium on Wireless Pervasive Computing, Phuket, 2006.

[6]. Jung E and Vaidya N, "A Power Control MAC Protocol for Ad Hoc Networks," Proc. ACM MobiCom, pp. 36-47, 2002.

[7]. Kyasanur P, Choudhury R. and Gupta I, "Smart Gossip: An Adaptive Gossip-Based Broadcasting Service for Sensor Networks," Proc. Second IEEE Int'l Conf. Mobile Ad Hoc and Sensor Systems, pp. 91-100, 2006.

[8]. Laura Marie Feeney, "An Energy Consumption Model for Performance Analysis of Routing Protocols for Mobile Ad Hoc Networks", Mobile Networks and Applications, 2001, pp.239-249.

[9]. V.Ramesh et.al, "An Efficient Energy Management Scheme For Mobile Ad-hoc Networks", International Journal of Research and Reviews in Computer Science (IJRRCS) Vol. 1, No. 4, December 2010, pp.173-176.

[10]. Ashish K. Shukla and Neeraj Tyagi, "A New Route Maintenance in Dynamic Source Routing Protocol," International Symposium on Wireless Pervasive Computing, Phuket, 2006.

[11]. Charles E. Perkins and Elizabeth M. Royer, "Ad-Hoc On-Demand Distance Vector Routing," In Second 1EEE Workshop on Mobile Computing Systems and Applications, pages 90-100, February 1999.

[12]. Ashish Shukla, "Ensuring Cache Freshness in On-demand Routing Protocols for Mobile Ad Hoc Network: A Cross-layer Framework " IEEE CCNC, 2007.

[13]. Sangeetha et.al, "Energy Efficient Routing In MANET Using OLSR", International Journal on Computer Science and Engineering (IJCSE), Vol. 3 No. 4 Apr 2011, pp.1418-1421.

[14]. B. H. Liu, Y. Gao, C. T. Chou and S. Jha, "An Energy Efficient Select Optimal Neighbor Protocol for Wireless Ad Hoc Networks," Technical Report, UNSW-CSE-TR-0431, Network Research Laboratory, University of New South Wales, Sydney, Australia, October 2004.

[15]. L.M. Freeny, ―Energy efficient communication in ad hoc networks,‖ Mobile Ad Hoc Networking, Wiley-IEEE press, pp. 301-328, 2004.

[16]. S.Singh and C.S.Raghavendra, ‖PAMAS power aware multi-access protocol with signaling for ad hoc networks,‖ ACM Computer Communication Review, vol. 28(3), pp.5-26, July 1998.

[17]. Sofiane Boukli Hacene and Ahmed Lehireche, "Coherent Route Cache In Dynamic Source Routing For Ad Hoc Networks", Computer Science Journal of Moldova, vol.19, no.3(57), 2011, pp.304-319.

[18]. R.Bhuvaneswari & Dr.M.Viswanathan, " Demand Based Effecive Energy Utilization in Mobile Ad Hoc Networks", International Journal of Computer Science Issues, Vol.9, Issue2, No.2,March 2012, pp.439-445.

AUTHORS PROFILE

M.Viswanathan. Senior Deputy Director in Fluid Control Research Institute (FCRI), a Public Sector Undertaking under Government of India, Palakkad, Kerala, India. He obtained graduate degree in Electronics and Communication Engineering from the University of Madras, Madras, India, received his Master's Degree in Electronics Engineering from IIT Kanpur and Doctoral Degree in Electronics from Bharathiar University, Coimbatore, India. He has 25 years of vast experience and had undergone training at NEL, UK in the area of flow measurement and B&K, Denmark in the area of Noise and Vibration. He has published many Technical papers in International Journals and presented papers in conferences held in India and abroad.

R.Bhuvaneswari has received the B.E. Degree in Electronics and Communication Engineering from Govt. College of Technology, Bharathiar University, Coimbatore, Tamil Nadu, India in 1989, M.E.Degree in Applied Electronics from the Govt. College of Technology, Bharathiar University, Coimbatore, Tamil Nadu, India in 1994 and she is currently pursuing Ph.D. degree in Electronics and Communication Engineering from the Anna University of Technology Coimbatore Coimbatore, Tamil Nadu, India. Her areas of interests include Communication networks, Wireless Communication, Mobile Communication, Digital Communication, Biomedical Applications, Applied Electronics, Computer Networks, Mobile Adhoc Networks (WiFi, WiMax, HighSlot GSM) & Network Security. She has also presented recently two papers on Mobile Adhoc Networks in conferences held in India.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

ASSESMENT OF COBIT MATURITY LEVEL
WITH EXISTING CONDITIONS FROM AUDITOR

I Made Sukarsa [1], Maria Yulita Putu Dita [2], I Ketut Adi Purnawan [3]

[1,2,3] Faculty of Engineering, Information Technology Studies Program, Udayana University
Kampus Bukit Jimbaran, Bali, Indonesia

[1]e_arsa@yahoo.com,[2]dita_pink4ngel@yahoo.com,[3]dosenadi@yahoo.com

***Abstract*—COBIT is a method that provides a basic framework in creating an information technology appropriate to the needs of the organization by taking considering other factors that affect. COBIT can be used as a guide to conduct an audit of the feasibility of an investment in information technology that has been done by a company. COBIT has a measuring element of IT performance, a list of critical success factors and maturity level measurement. All these tools are designed to support the successful implementation of corporate governance on various objects in the field of IT. These research take a case studied at employment agencies which usually called BKD. Domain selected in this study is Delivery and Support (DS). The measurement level of maturity is seen that the whole process of IT is at a scale of 3, which means the level of maturity in BKD is defined. This shows that none of current IT process has the same level with the expected one. The whole process still has a gap to be closed. Appropriate IT processes are given the initial step for the development of IT models include DS1, DS5, DS7, DS10 and DS11 with the determination of CSF, KPI and KGI. Substantive tests performed in this study meet the sufficiency of the evidence in order to obtain a conviction of compliance with the conditions of the criteria. BKD substantive test results are already has the documentation to third parties (vendors) and documentation are clearly procedures for managing civil servants information system which usually called SIMPEG. But there are some things you may need to be added to the application, such as the lack of backup, recovery, an automated help menu in SIMPEG and password to be encrypted. Substantive test also intended to develop opinions, conclusions and recommendations for the management of BKD by improving the management of information systems in the future.**

Keywords-COBIT; Maturity Level; Substantive Test; Recommendation; IT Models

I. INTRODUCTION

BKD as a government agencies that deal with personnel issues can not be separated from the existence of aspects of centralized data management. Data management at BKD, as a process that is beginning to implementation management information systems to strengthen personnel administration in an effort to meet employee needs for information of accurate, accountable, and up to date data. Manual conversion data into digital data into a computerized database and applications in a container called a SIMPEG, is expected to increase the effectiveness and efficiency in the processing, storage, presentation and recap information related to staffing. If the system is not computerized information used properly it could lead to information needs to be blocked and will interfere with the performance of the relevant agencies. Utilization of IT to support the achievement of organizational goals and objectives must be balanced with effectiveness and efficiency of management. Therefore, IT audit should be done to maintain the security of information systems as an organizational asset, to maintain the integrity of information stored and processed and of course to increase the effectiveness of the use of IT and support efficiency in BKD. (BKD, 2011).

A good management for information systems can supported the company's performance. IT governance is managed properly can be used as landing in a large organization or a government. COBIT (Control Objectives for Information and related Technology) is one standard for IT audit can be used to measure. COBIT focuses on controls and provides a set of best practices for management. Such as ensuring the delivery of services and can provide the measurement and rate when errors occur. (COBIT 4.1, 2007)

In this study, COBIT is also used as tools for effective implementation of information systems within the company. Measurements were performed to determine the condition of the current IT governance in BKD are expected to set targets based on factors that influence, with the fundamental to the COBIT maturity model framework, so that the gap obtained from the maturity level. Then to determine whether a problem or irregularity actually occurred or not the substantive testing can enhance the acquisition of evidence in gaining confidence in the company's compliance with the criteria condition. Tests conducted on a review of several documents and procedures related to IT management and the testing of applications SIMPEG.

II. THEORETICAL FRAMEWORK

A. IT Governance

As mentioned previously, the application of good corporate governance in the company relies heavily on IT governance is carried out in earnest starting from top level management to the staff. IT governance plays a role in measuring the

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

company's business processes to ensure its effectiveness in supporting the goals and objectives of a company. The following is a description of the five sections that are focused in IT governance. (Gondodiyoto, 2007). These images below are descriptions of five sections that focused in IT governance.

Figure 1. IT Governance Focus Area
(COBIT 4.1, 2007. Page 6)

Explanation for the main focus areas of IT governance are as follows (COBIT 4.1, 2007):

a. Strategic Alignment is about focusing Strategic assurances as to the relationship between business and IT strategy and alignment between IT and business operations.
b. Value Delivery is included matters related to the delivery of value that focuses on optimizing costs and proving the existence of intrinsic value of IT.
c. Risk Management is about the application of IT to be accompanied by the identification of IT risks that impact can be properly resolved.
d. Resource Management is concerned about optimizing critical IT resources, including: applications, information, infrastructure and human resources. This area is key to optimizing knowledge and infrastructure.
e. Performance Measurement is about tracking and monitoring the implementation of the strategy, which runs the project fulfillment, resource usage, process performance and delivery by using a framework such as the balanced scorecard.

B. COBIT definition

COBIT (Control Objectives for Information and Related Technology) is a referral guide for IT governance to address the gaps that are owned by the business risks, control needs and technical issues. IT resources are highlighted COBIT, including the fulfillment of business requirements for effectiveness, efficiency, confidentiality integrity, availability, reliability compliance, and information. COBIT can provide a signal at danger or risk would appear to provide readiness to deal with it. COBIT is useful for the auditor as a technique that can assist in the identification of IT control issues.

COBIT can be used as a standard for the auditors, the management of an organization or user. COBIT users can obtain the advantage of confidence in the reliability of the applications used. While managers to profit-making investments in IT and infrastructure, developing the IT strategic plan, and determine the information architecture. (Gondodiyoto, Sanyoto, 2007).

C. COBIT Framework

COBIT Framework consists of three main parts, namely IT Process, IT Resources and Information criteria. In the picture below, indicated that the Information criteria are divided into seven information criteria are then grouped into three aspects, namely the quality requirements, fiduciary requirements and security requirements. COBIT IT resources highlights the five main sections, namely people, application systems, technology, facilities and data. For IT Process consists of domain, process and activities. (COBIT 3rd Framework, 2000).

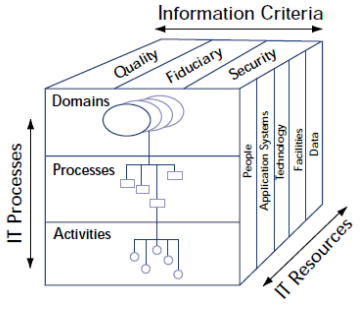


Figure 2. COBIT cube
(COBIT 3rd *Framework, 2000*. Page *16*).

D. COBIT Maturity Model

COBIT also provides IT process maturity level models to evaluate the maturity level of the organization to have. Assessment methods have COBIT is from a non-existent scale of 0 to 5-optimized. COBIT Maturity Model can be identified as follows:

• Where are the company's performance
• Comparison of current industry status
• Target companies for repairs
• Track the growth needed between 'as is' and 'to-be'

To make the results easily usable in management briefings, where they will be presented as a means to support the business case for future plans, a graphical presentation method needs to be provided (Figure 3).

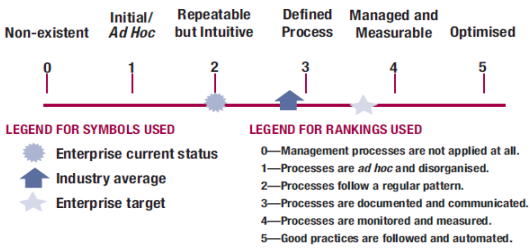


Figure 3. Maturity Model COBIT
(COBIT 4.1, 2007. Page 18)

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

The advantage of using COBIT maturity model is the management can easily know the condition of the company. 0-5 scale based on a simple maturity scale showing how the process evolved from the ability of a lack of optimized. (COBIT 4.1, 2007;18.).

E. Critical Success Factor (CSF)

Critical Success Factors is the most important thing that must exist within an organization or company because it can help the company achieve its goals through IT owned. Critical Success Factors in addition to providing a guideline for implementing management control over IT and its processes can also give a strategy, technical, organizational processes or procedural nature. Areas highlighted here is related to the ability and skills, focused and action oriented, and resource utilization (COBIT *Management Guidelines, 2000*).

F. KPI and KGI

Key Performance Indicator (KPI) and Key Goal Indicator is an indicator that measures are also provided for each of the COBIT IT processes. KPI are usually indicators of capabilities, implementation, and the ability of IT resources. KPI focuses on how the process is run, while KGI focuses on the process. Based on the principles of Balanced Score Card, then the relationship between the Key Performance Indicator targets and indicators are as follows (COBIT Management Guidelines, 2000) :

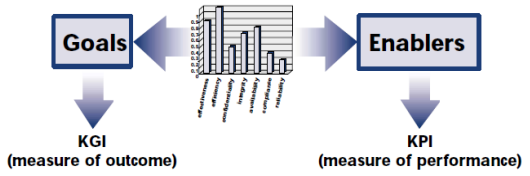


Figure 4. KPI and KGI relationship
(COBIT Management Guidelines, 2000. Page 20)

Key Performance Indicator and Key Goal Indicator have linkages and causal relationships in support of the IT processes, which shows how well the process can allow the objective can be achieved. Meanwhile, key goal indicators focusing on "what", while the Key Performance Indicator focused on "how". Usually, Key Objectives and Key Indicators Performance Indicators will often be the size of the Critical Success Factors (CSF) and when it is monitored and acted upon, it will identify opportunities for process improvement. These improvements have a positive influence on results. (COBIT Management Guidelines, 2000. Page 20).

G. Substantive Test

Substantive tests performed by the auditor as a follow-up audit to obtain reasonable assurance about whether the findings of the auditor while, prepare opinions and conclusions, and develop suggestions for improvement. The most important goal in performing substantive tests is to meet the substantive adequacy of the evidence by applying a broad and appropriate types of testing, as well as to enhance the acquisition of evidence to obtain reasonable assurance about compliance with the conditions of the field previously obtained criteria. Then, the results of the testing phase of the findings. The audit findings will stem the decline in the comparison condition (what is actually happening) with the criteria (what should happen), reveals the impact of differences in the conditions and criteria and to find the cause. (Nurharyanto, Ak., 2009).

III. METHODOLOGY

Information systems audit refers to the standard COBIT framework. Related to vision, mission, goals and targets in BKD mostly lead to the delivery and support services provided by a system of information technology (IT) that has been applied, the study also focuses on the domain Deliver and Support (DS), especially the DS1 up with the DS13. In the implementation of this study, where the case studies is the BKD.

This study describes how the application of IT Governance is happening at BKD. The research method used in this study is a qualitative method using case studies for helped the authors to obtain an understanding of an event. Studied as a case study of an integrated whole, where the goal is to develop a deep knowledge of the object in question, which means that case studies should be characterized as an exploratory and descriptive research. The steps undertaken in this study include the stages of domain selection, data collection, data processing and determination of recommendations, as seen in Figure 5 below, which is the sequence of research steps.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

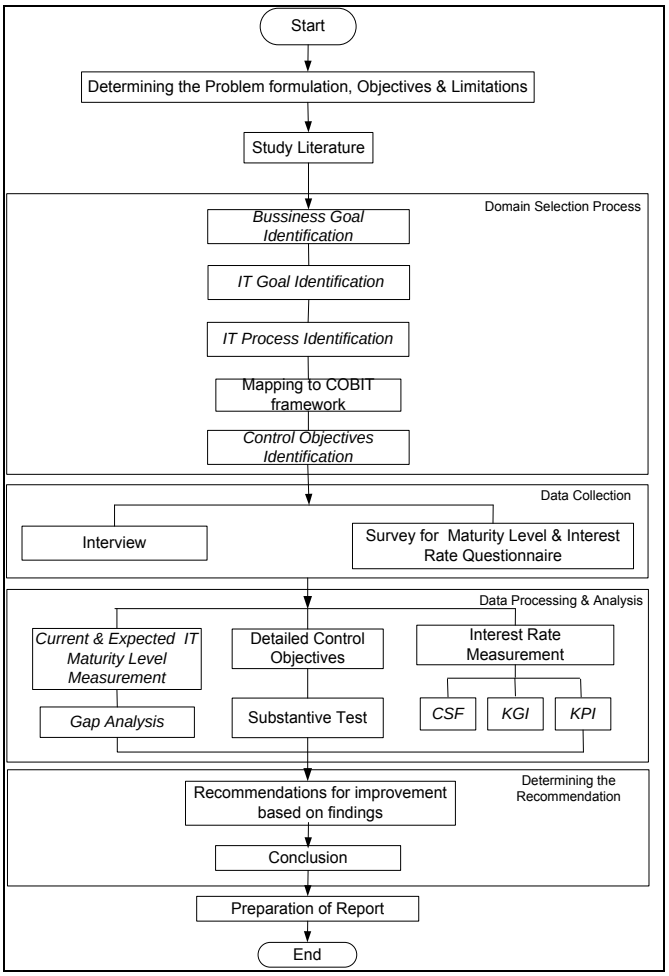


Figure 5. The Steps of Research

To conduct survey on IT governance, especially in the process of managing data is by using questionnaires and interviews.

The questionnaire is a collection of data by using a list of statements that are used to determine respondent's perceptions of several variables considered in the implementation of IT governance and management of information systems within the company. Data collected is taken directly from the data obtained from the respondents that the questionnaire addressed to the head section, sub.section and the staff members at BKD with a view to obtaining the target achievement and the assessment of the achievements that have been implemented.

This study uses two types of questionnaires, ie questionnaires to measure the maturity level and the importance of IT in DS domain using COBIT standards.

Interview process conducted to determine the existing business processes in the company. The first stage in the interview process is to identify the parties responsible for each process that takes place in the company. Interview technique is also a collection of data by direct questioning by the respondent in order to obtain information from the questionnaires have not been accommodated. Interviews were also conducted to determine the process, the stages are done now associated with information technology resource management, decision-making processes, information technology investment management processes and ideal expectations based on management's view of the company.

The design of this questionnaire refers to the COBIT Implementation Tool Set and questionnaire aims to obtain data or any official opinion of BKD as a party related to IT management. Questionnaire to determine the interest rate is developed to determine the importance of each IT process in a DS domain. Column containing the level of importance, respondents could choose one answer that is considered to represent actual field conditions by providing a tick (√) in the space provided. Later the results of this questionnaire will be calculated the score of each IT process is considered to have a high contribution to the business goals or have a high interest rate to be selected in the provision of recommendations to improve IT governance process. The following is a questionnaire designed for the interests of the DS domain of IT.

Importance				IT PROCESS *Deliver and Support* (DS) Domain	
Very Important	Somewhat Important	Not Important	Not Sure		
				DS 1	*Define and Manage Service Levels*
				DS 2	*Manage Third-party Services*
				DS 3	*Manage Performance and Capacity*
				DS 4	*Ensure Continous Services*
				DS 5	*Ensure System Security*
				DS 6	*Indentify and Allocate Cost*
				DS 7	*Educate and Train Users*
				DS 8	*Manage Service desk and incidents*
				DS 9	*Manage the Configurations*
				DS 10	*Manage Problems*
				DS 11	*Manage Data*
				DS 12	*Manage the Physical Environment*
				DS 13	*Manage Operations*

Figure 6. Importance Questionnaire

Examples of the draft questionnaire was also made in this study, the questionnaire for the measurement of the level of decency on the maturity level 0 to level the IT Process DS1.

IT Process DS1 Define and Manage Service Levels (1) (4) Do You Agree ?

IT Process	Define and Manage Service Levels							
IT Process Number	DS1	Maturity Level (2)	0	Not at all	A little	Quite a Lot	Completely	Value
No.	Statement (3)		Weight	0.00	0.33	0.66	1.00	
1	Management has not recognised the need for a process for defining service levels		1					
2	Accountabilities and responsibilities for monitoring them are not assigned		1					
		Weight Total =	2 (6)			Compliance Level =		0.00 (5)

Figure 7. Maturity Levels Questionnaire

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

In the design of the questionnaire above shows there are several components in the checklist. Component indicated by the number 1 is the name and number of IT processes are observed. Component indicated by the number 2 is the level of maturity that will be used to distinguish the contribution of each level. Component 3 contains a description of the statement used to guide the interview questions. Component 4 is a scoring guide as a number of observations and interviews of each statement is expressed. Component 5 is the sum of the value of each statement, which will be used as the contribution of each level and component 6 is the total weight of the total number of questions. Any item that is the question on the DS1 with a maturity level 0 as shown above is referring to the standard IT Governance Institute Team pages 104 in the book of COBIT 4.1.

IV. Results And Discussion

A. Determination Process Domain

Based on the mapping and identification of objectives and goals BKD with standard business goals and IT goals COBIT, the importance of the domain of IT processes that are relevant to the audit, namely:

Table 1. IT Determination Process in accordance with enterprise IT Goals

IT Process	***IT Domains***
PO1, PO2, PO3, PO4, PO5, PO6, PO7, PO8, PO9, PO10	*Plan and Organize*
AI1, AI2, AI3, AI4, AI5, AI6,AI7	*Acquire and Implement*
DS1, DS2, DS3, DS4, DS5, DS6, DS7, DS8, DS9, DS10, DS11, DS12, DS13	*Deliver and Support*
ME1, ME2, ME3, ME4	*Monitoring and Evaluate*

However, due to BKD is a government agency that specializes in managing all the data of personnel has the vision and mission and goals and objectives are more directed at the delivery of IT services for civil and environmental SKPD in Bali Province, such as increasing the professionalism of staff with training, setting security and data management including operational facilities, the study of this audit focuses only on the 13 IT processes in the Deliver and Support domain.

B. Measurement Maturity Level

Capability and maturity of each IT process in Deliver and Support domain will then be identified. Implementation level of maturity for BKD questionnaire will reveal the condition of maturity of each process at this time. Assessment of each IT process maturity level refers to the COBIT maturity model Guidelines Management. Value will indicate the level of maturity of IT process maturity level with a thorough identification of each level. Weighting is performed on an existing questionnaire is based on the following values (Pederiva, 2003)

Table 2. Questionnaires weighting

Answer	**Value**
Not at all	0
A little	0,33
Quite a lot	0,66
Completely	1

Then the mapping of the entire questionnaire with a weight value of the statement above will be summed and divided by the amount of the existing statement. Values obtained from the division is then a standard level of maturity in accordance with the table below. (Djatmiko, 2007)

Table 3. Assessment Criteria

Maturity Index	**Maturity Level**
0 – 0,50	0 – *Non-Existent*
0,51 – 1,50	1 – *Initial/ad hoc*
1,51 – 2,50	2 – *Repeatable But Intuitive*
2,51 – 3,50	3 – *Defined Process*
3,51 – 4,50	4 – *Managed and Measurable*
4,51 – 5,00	5 – *Optimised*

Level is determined based on the appropriateness of the COBIT framework provides grouping capability in managing the company's IT processes from level zero to level five (optimized). The thing to note is that the level is not intended to be a sequential increase that must be met starting from the lowest to highest. Fulfillment can do some level of decency for simultaneously. The point is the fulfillment of maturity may occur at some level zero to level five, then the level of compliance maturity calculated in accordance with the total of the multiplicative contribution to the level of appropriateness of the levels concerned. Thus, the determination of the same will be done at each level in the IT-related processes.

The following measurements will show the maturity level of an employee at BKD are processed using Microsoft Excel by taking a sample calculation for the DS1 from a respondent and starting from level 0 to level 5.

DS	Level	Weight	Criteria Value												Sum	Compliance Level	Contribution Level	Value
			1	2	3	4	5	6	7	8	9	10	11	12				
1	0	2	0,66	0,00											0,66	0,33	0,0	0,00
	1	4	0,66	0,66	0,66	0,00									1,98	0,50	0,3	0,15
	2	5	0,00	0,00	0,66	0,66	0,66								1,98	0,40	0,7	0,28
	3	6	0,66	0,66	0,66	0,66	0,66	0,66							3,96	0,66	1,0	0,66
	4	9	0,66	0,66	0,66	0,66	0,66	0,00	0,66	0,66	0,66				5,28	0,59	1,3	0,76
	5	6	0,66	0,66	0,66	0,66	0,66	0,66							3,96	0,66	1,7	1,12
																	Maturity level :	3.00

Figure 8. Examples of Maturity Level Measurement

Seen in the table above which is a process that occurs in the calculation to obtain the value of each level in the domain of DS1. One example at level 1, the weight of a column stating that there are large number of statements in each level, and each statement has a weight of 1, then at level 1, weighted equally, ie, weight = 1, resulting in a total weight of 4. The

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

result is the selection by choosing one of the following criteria: "Not at all", "A little", "Quite a Lot" or "Completely". Each criterion has a certain value which is then assessed based on the compliance level quotient between the sum value of each criterion statement with a total weight of the previously presented. Propriety maximum level is 1, which describes the related statements have been fully met. In the table shows that the level of appropriateness of IT processes to level 1 is at 0,5 which is the quotient between the total value of the criteria of 1,98 with a total weight of 4. Furthermore, the contribution of the process give you an idea how much influence the appropriateness of each IT process maturity level as a whole. Contribution is then multiplied by the level of appropriateness at each level of maturity. The results of time will be written in the column value, total of five levels later in the DS1 will be added together to determine the level of IT process maturity of one respondent.

Maturity target of IT processes are ideal conditions for the expected level of maturity, which will become a reference in a model of good IT governance. Maturity target of IT processes is determined by looking at the internal environment of business and the high expectations of the management board at BKD about COBIT IT processes to be applied. The vision and mission, goals, and objectives of IT adoption in BKD can be found several important issues that can be taken as a basis for consideration to determine the expected target of process maturity, which is evident in the goals and objectives of BKD itself. Based on consideration of several factors and the high expectations of the management ranks of the COBIT IT processes in DS domain, it can be concluded that the level of maturity that will become a reference in the IT governance model to be developed is on a scale of 5 which has been managed by optimal (optimized).

C. Gap Analysis Maturity of IT Processes

The table below shows the gap analysis of current business conditions (current maturity level) and expected (expected maturity level).

IT Process	*Gap Maturity Level*	Interest Rate of IT Process in BKD	
		Important	Not Important
DS1 - *Define and Manage Service Levels*	2,3	81,58	18,42
DS2 - *Manage Third-party Services*	2,1	78,08	21,92
DS3 - *Manage Performance and Capacity*	2,2	63,64	36,36
DS4 - *Ensure Continous Services*	2,0	65,15	34,85
DS5 - *Ensure System Security*	2,3	97,24	2,75
DS6 - *Indentify and Allocate Cost*	2,0	80,76	19,23
DS7 - *Educate and Train Users*	1,8	97,17	2,83
DS8 - *Manage Service desk and incidents*	2,1	38,10	61,91
DS9 - *Manage the Configurations*	1,9	31,58	68,42
DS10 - *Manage Problems*	1,8	89,01	10,99
DS11 - *Manage Data*	1,5	99,13	0,87
DS12 - *Manage the Physical Environment*	1,8	42,11	57,90
DS13 - *Manage Operations*	1,7	69,56	30,43

Figure 9. Gap for Maturity Level

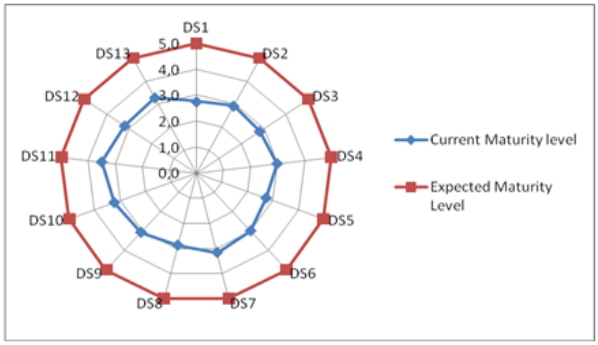


Figure 10 Graphic Display for Current and Expected Maturity Level

Based on the distribution of the maturity level (maturity level) IT processes COBIT on DS domain is shown in the graph above, it can be described as a condition in which all the conditions in these domains are at maturity level 3. This means that in general IT processes running on the BKD has been defined in the standards or procedures are documented and communicated through formal training and the implementation still depends on the individual whether to perform the procedure established or not. The procedure created is still limited to the form of formalization of existing practices. Ideal conditions are expected at maturity level 5 (optimized), a condition in which the process is carried out has undergone continuous improvement process and thus produce the best results. The use of integrated information technology to automate organizational environment, readily available tools and other support that can improve the quality and effectiveness of performance, and the organization is stable and able to adapt well.

D. Recommendation to Closed the Gap

Gap maturity level found on DS1 to DS13 process and can be addressed by BKD to conduct activities or adjustment measures as follows:

Table 4 Recommendations to Closed the Gap

Proses TI	Recommendations to closed the gap
DS1	a.BKD need to implementation the procedures to address the identified deficiencies of formal service level. b.Need agreement to the level of service that has begun to lead to business needs.
DS2	a.BKD need for support measures for early detection of potential problems with third-party services. b.Reviewing periodically at intervals specified in the contract signed with third parties.
DS3	a. Need for improved handling performance and capacity problems associated with such use of monitoring tools can automatically detect and fix problems related to performance and capacity, so as to impact later on the staff and

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

	users of IT services that are no longer doubt the ability of IT services.
DS4	a. BKD need for an integrated IT service processes in a sustainable manner with respect to external benchmarking and best practices. b. Increasing the understanding of practice and thoroughly enforced. c. BKD need ongoing systematic measurements for the goals and objectives towards the achievement of IT services.
DS5	a. Running the IT security responsibilities have been assigned consistently. b. Reporting the need for security that includes a clear business focus. c. BKD need for security training and set up it formally.
DS6	a. Monitoring and evaluation of the cost of services used to optimize the cost of IT resources. b. Improving cost management to the level of industry practice, which is based on the results of continuous improvement and comparison with other organizations.
DS7	a.The need for education and training process monitoring and detection of irregularities should be further improved. b.Applied to the analysis of the need for IT education and training issues.
DS8	a.Question need for tracking and automatic incident reporting system and formal implementation. b. IT services need to train personnel, and the process is enhanced through the use of special software. c.BKD need for comprehensive FAQs from a part of the knowledge base. d. Completion of the quick incidents consistent advice in a structured escalation process.
DS9	a. BKD need consistent action for physical verification and detection of irregularities further enhanced procedures.
DS10	a. Detection of violations of norms or standards that have been defined. b. Individual asset tracking and monitoring are used to protect IT assets and to prevent theft, abuse and harassment.
DS11	a.Institutionalization and seriousness to handle the training for data management staff members. b.The necessity of understanding for the needs in data management and understanding of all necessary actions within the organization. c.Responsibility for data ownership and data management are clear, widely known throughout the organization and updated in a timely manner.
DS12	a. BKD need for setting standards for all facilities, including site selection, construction, guarding, personnel safety, mechanical and electrical systems, and protection against environmental factors (eg, fire, lighting, flood). b.The need to document the security requirements of the physical environment and access is strictly controlled and monitored. c.The need for more stringent measures and continuous monitoring of access control and all visitors are escorted at all times.
DS13	a. Maintenance and service agreements with vendors that are formal. b. Need for regular reporting on the events and results to management tasks.

E. Measurement of Interest Rate

The collection of data on interest rates was conducted using questionnaires that have interest rate indicator assessment of the level of importance. Respondents were assigned to choose the right answer according to the condition of the company. Made to the weighting of each assessment of the importance of IT processes, namely:

a. For the assessment is very important given the value 4
b.For the assessment is Somewhat important given the value 3
c. For the assessment is not important given the value 2
d. For the assessment was not sure given the value 1

The results of the weighting calculation is then performed in such a manner as shown in figure 11 in order to get the final score with the level of the index as follows (Kurniawan, Erva. 2011) :

Table 5. Value dan Levels

Index of the Final Score	Levels
0 – 25	Not Sure
25 – 50	Not Important
50 – 75	Somewhat Important
75 – 100	Very Important

Interest Rate					Interest Rate				
Very Important	Somewhat Important	Not Important	Not Sure	Sum	Very Important	Somewhat Important	Not Important	Not Sure	Sum
a	b	c	d	e	f	g	h	i	j
n*4	n*3	n*2	n*1	∑1	$\frac{a}{e}$ %	$\frac{b}{e}$ %	$\frac{c}{e}$ %	$\frac{d}{e}$ %	∑2
(n = Amount of Data)									

Figure 11. The formula for measuring the rate of Interest

The results of the questionnaire data processing based on the importance of IT processes at BKD show there on the COBIT IT processes that have a value above 50. This value is

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

then compared with the index scoring, and shows the level is Somewhat important and very important. Assuming that the process has a value above 50 is a process that must exist. Process includes are DS1, DS2, DS3, DS4, DS5, DS6, DS7, DS10, DS11 and DS13.

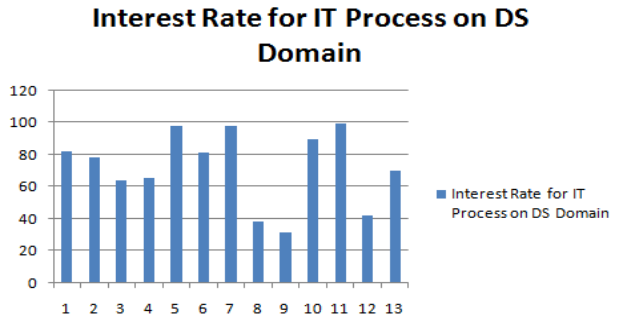


Figure 12. Score for each IT Process

F. Determination of CSF, KPI and KGI

Based on rank of interest rates, then selected five IT processes, namely DS1, DS5, DS7, DS10, DS11 with the highest score should be given guidance on IT governance model of CSF, KPI and KGI. Here's an example of CSF, KPI, KGI to DS2 (COBIT Management Guidelines, 2000; 70)

Table 6. an Example for CSF, KPI, KGI to DS5 COBIT

Process Name : DS5 Ensuring Security System
Business Target: Minimizing the impact of security vulnerabilities and incidents and maintain the integrity of information and processing infrastructure
IT process objectives: Monitoring, detecting, reporting and resolving security vulnerabilities, incidents and defining IT security policies, plans and procedures.
Critical Success Factor : • Management of user authorization • Management of disruption to system security • The overall security plan is developed that includes building awareness, establish clear policies and standards, identifying and implementing sustainable cost savings, as well as defining the monitoring and enforcement process • There is awareness that a good security plan must take time to develop • Management and staff have a general understanding of security requirements, vulnerabilities, threats and understand and accept responsibility for the security of self • A third party evaluation of security policies and architecture is periodically performed
Key Goal Indicator : • Decreasing the amount of disruption to the systems that affect business services • Alignment of access rights with organizational responsibilities • Reduce the number of new implementations delayed by security problems • Reduce the number of incidents involving unauthorized access, loss or destruction of information
Key Performance Indicator : • Frequency of service interruption due to disruption to business security systems • Percentage of users who do not access in accordance with the authority • The number of active monitoring system with the ability • Reduce the time to investigate security issues • The time lag between detection, reporting and action on security incidents • The number of days of training on IT security awareness

G. Risk of Findings and Recommendations of the Substantive Test

Substantive testing performed to meet the sufficiency of the evidence is by doing some of the review to obtain a conviction of BKD conformity with the conditions in the state is supposed to happen. Tests performed include the control of security management, control of SIMPEG applications, input control, process controls, output controls and database control.

Table 7. Risk and Recommendation Based on Substantive Test Findings

Risk	Recommendation
Control of Security Management	
There are still some staff who bring food and drinks to the server room or put them near the computer equipment will lead to a lack of security on the management of facilities and physical environment can harm and even damage the computer.	BKD in the firm should establish policies requiring staff not to bring food and drinks into the server room or near computer equipment
In the absence of disaster recovery plan in the application system SIMPEG, this will result in losses such as loss of data and sluggish handling when the system is susceptible to interference.	SIMPEG application system should come equipped with a disaster recovery plan to prevent bad things happen when the data processing.
Management Control Applications	
There are no age restrictions on the password system will cause the password easily recognized by people who are not responsible.	BKD should create a policy that requires staff to change passwords periodically.
With no limits on the system error in inputting the login access (password and username), it will provide convenience for people who do not have the authority to access	SIMPEG application system should provide limits in inputting system login access. Inputting errors should be limited to 3 times, if

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

into the application system SIMPEG.	it passes this limit then the system will automatically exit the application.
Input Control	
Result of the absence of color changes on the display screen if the data inputting errors occur, then the user is not aware of any errors when inputting, thus reducing the effectiveness and efficiency of users' work.	SIMPEG application system should be equipped with a color change of the display screen in case of inputting errors.
SIMPEG application system that does not provide functionality for back-up warning will result in user neglectful and at high risk for loss of data.	Should the warning be added to the application system data has not been in the back-up to avoid the loss of corporate data.
Output Control	
The absence of regular reporting procedures demand or request a new report in the application system SIMPEG will result in the timely distribution of reports to be reduced.	Procedures should be added routinely request or demand for new reports that are programmed into the application system SIMPEG
Process Control	
No data log in the application system causes every process that goes unrecorded, so tracking it is difficult to do if something goes wrong	SIMPEG application system should be added to the log data also needs to control every process that occurs.
Database Control	
The absence of policy on handling control file, this causes the control to data and data storage media in the event of a malfunction of data is inefficient.	Should implementation a policy on handling of the file system so that control can be done with back-up recovery quickly to avoid the risk of data loss.

V. CONCLUSION

Maturity level analysis shows that the whole process of IT in DS domain is mapped at level 3, which means management maturity level in BKD used COBIT 4.1 is defined. This shows that not a single information technology governance processes that already meet. The whole process still has a gap that must be covered. To achieve the expected level of maturity, a number of rules, policies, recommendations and suggestions for improvement of information technology governance model has been successfully created.

The analysis of questionnaire about the importance of these processes are feasible given the initial step for the development of IT models include DS1, DS2, DS5, DS6, DS7, DS10 and DS11 with the determination of CSF, KPI and KGI. Using these guidelines and indicators, the process of IT governance can be directed and driven by good information so that resources can be better utilized and will establish a standard model for the process.

The results for substantive test are BKD already has the documentation to third parties (vendors) and documentation are clear procedures for managing SIMPEG. But there are some things you may need to be added to the application, such as the lack of backup, recovery, an automated help menu in SIMPEG and password are not encrypted.

REFERENCES

[1] Djatmiko,B. 2007. "Information Systems Audit Process to Assess Service Delivery and Support Information Using the COBIT Framework". Thesis. Bandung: ITB.
[2] BKD. 2011. "SIMPEG-BKD". Bali.
[3] Dwiani, R. 2010. "IT Governance Implementation Using COBIT 4.1 Fremework" Thesis. Jakarta: Indonesia University.
[4] Gondodiyoto, S. 2007. Information Systems Audit + COBIT Approach. Jakarta: Mitra Wacana Media.
[5] IT Governance Institute Team. 2007. COBIT 4.1. USA: IT Governance Institute.
[6] IT Governance Institute Team. 2000. COBIT Management Guidelines. USA: IT Governance Institute.
[7] IT Governance Institute Team. 2000. COBIT Implementation Tool Set. USA : COBIT Steering Committee and the IT Governance Institute.
[8] IT *Governance Institute Team*. 2000. COBIT 3rd *Framework*. USA : COBIT Steering Committee and the IT *Governance Institute*..
[9] Kurniawan, E. 2011. Evaluation of IT Governance Using COBIT Framework Case Study: Provincial Government of Yogyakarta. Yogyakarta: UGM.
[10] Nurharyanto, Ak. 2009. Auditing. Bogor : JFA Training Certification Experts Exchange Formation Auditor.
[11] Pederiva, A. 2003. The COBIT Maturity Model in a Vendor Evaluation Case. Information System Control Journal Volume 3.
[12] Sarno, Riyanarto. 2009. Audit Systems & Information Technology. ITS Press : Surabaya.

AUTHORS PROFILE

I Made Sukarsa, ST, MT is a lecturer who worked at Faculty of Engineering, Information Technology Studies Program, Udayana University.

Maria Yulita Putu Dita is a student at Faculty of Engineering, Information Technology Studies Program, Udayana University. Her research interest on information systems audit using COBIT framework to get bachelor degree.

I Ketut Adi Purnawan, ST, M.Eng. is lecturer at Faculty of Engineering, Information Technology Studies Program, Udayana University.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Intrusion Detection and Prevention Response based on Signature-Based and Anomaly-Based: Investigation Study

Homam El-Taj
Fahad Bin Sultan University
Tabuk, Saudi Arabia.
heltaj@fbsu.edu.sa

Firas Najjar.
VTECH - LTD.
Riyadh, Saudi Arabia.
firas@vtech-sys.com

Hiba Alsenawi
Fahad Bin Sultan University
Tabuk, Saudi Arabia.
Habdelhakim@fbsu.edu.sa

Mohannad Najjar
Tabuk University
Tabuk, Saudi Arabia.
najjar@ut.edu.sa

***Abstract*: One of the fundamental topics in network Signature security is to detect intrusions and prevent them from exposing or destroying important information, or breaking down systems.**

In these systems the main problem is how to insure the abnormal activity is a harmful activity and what the prop irate response to stop the attack without affecting the whole process of the systems, because wrong response may affect the system more than the attempted intrusion, and because most organizations try to detect every intrusion, they examine every suspicious event; which means that more malicious events are detected but more resources are needed to differentiate actual intrusion from false malicious events. Also the Response for known attacks is accurate to stop them, because you know every step of the attacks and you know how to stop them, but when facing anomalies it's not clear is it attack and what the best way to response without affecting the whole system.

In this paper we will present the IDPS (Intrusion detection and prevention) techniques and their efficiency in preventing intrusions.

Keywords:*Network security, Intrusion Detection and Prevention Response, False Positive, False negative*

I. INTRODUCTION

Nowadays most commercial and government information systems are connected through the Internet, which will expose them to avenues of attacks. This becomes very accurate because of the increasing number of computer users, where the computer became an essential tool for life style. With it people can see news, send emails, pay by credit cards, study, and they can do many other activities.

These systems must be protected from unauthorized access that may expose critical information, by detecting any suspicious anomalies in the network traffic patterns due to Distributed Denial of Service (DDoS) attacks, worm propagation[1,2], viruses, Trojans and other kinds of malicious programs that introduce more panic into network society. Because of all this danger, securing such networks infrastructure has become a priority for most researchers.

In order to respond to this increasing threat the Information Technology security industry provides a range of tools known as vulnerability assessment tools as well as IDPS.

One of the major concerns of IDPS is to make sure the detection of intrusion and reporting it, once the detection is reliable, next step will be to protect the network (Prevention).

The major weakness in the IDS is the guarantee of intrusion detection and the right response to stop the intrusion that will make (IPS). This is the reason why in many cases IDSs are used together with a human expert. As Ahmed Patel, Qais Qassim, Christopher Wills[3] mentioned a well trained staff and analysts are required to continuously monitor the system to protect organizations critical information from attacks.

In this way, IDS is actually helping the network security officer and it is not reliable enough to be trusted on its own. The reason is the in ability of IDS systems to detect the new or altered attack patterns. Although the latest generation of the detection techniques has significantly improved the detection rate, still there is a long way to go[3].

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

On the hand IDPSs help to automate the response for system violation. And because most attacks have sequence of steps, IDPSs try to stop the attacker to move to next step.

II. IDPS INTRUSION DETECTION AND PREVENTION SYSTEM

Computer networks systems can be susceptible to many kinds of attacks. Securing such networks is a priority by detecting these attacks. IDS is as one of the main tools used for this propose. IDS is considered to be the first line of defense for any security system.

A. *History*

Before IDPS was known the process of detecting intrusions and responding for such intrusions was done manually, the system administrator was reading all system logs trying to detect abnormal activity. This approach took a lot of time and effort, and just specialized people could do it. Therefore the process of detecting and preventing intrusion had to be done automatically [4]. However not every anomaly can be considered as an attack or intrusion, and any wrong response will affect whole system.

It is necessary to point out the early IDPS Software (not Systems) was mostly individually developed, programmed and not widely spread, as only very few organizations needed this kind of technology before the dawn of the Internet age [4].

B. *Definition*

National Institute of Standards and Technology (NIST) [5] define (IDSs) as the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices.

NIST defines Intrusion prevention as the process of performing intrusion detection and attempting to stop detected possible incidents, on other words intrusion prevention (IPSs) system is an active intrusion detection system.

IDPSs will monitor computer system environment, identifying problems with the security polices, notify system administrator of abnormal event and security violation and try to stop intruders making successful attack by stopping the attack itself or by changing the configuration of security environment like routers.

C. *IDPS technologies*

The types of IDPS technologies as mentioned in NIST [5] depend on the type of events that they monitor and the way which they are deployed:

- Network-Based: monitors network traffic for particular network segments and analyzes the network and application protocol activity to identify suspicious activity. The main disadvantage of this technology it can't be used if encrypted communication is allowed
- Wireless: monitors wireless network traffic and analyzes it to identify suspicious activity involving the wireless networking protocols themselves. One of the disadvantage it cannot identify suspicious activity in the application or higher-layer network protocols.
- Network Behavior Analysis (NBA): Monitor network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware, and policy violations.
- Host-Based: Must be deployed on each protected machine (server or workstation) to monitors the operating system, applications, the host specific network traffic, and analyze the data to that machine such as system log files, audit trails and file system changes. Main disadvantages are the installation on every single host and the adaptation to the different platforms and operating systems.

Most IDPS technologies use multiple detection methodologies, either separately or integrated to provide more broad and accurate detection.

D. *IDPSs Methodologies*

The common methodologies that IDPSs uses to identify threats as NIST [5] mentioned are:

- Signature-based, (also denoted as misuse-based) seek defined patterns, or signatures, within the analyzed data. This methodology very effective detecting known threats and have small number of wrong detection, but ineffective detecting new threats or unknown one and the set of signature must be constantly update manually to new threat. For this purpose, there must be a signature database corresponding to known attacks.

- Anomaly-based, detectors attempt to estimate the ''normal'' behavior of the system to be protected, and generate an anomaly alert whenever the deviation between a given observation at an instant and the normal behavior exceeds a predefined threshold, it can

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

be very effective for detecting new threats, but it generates many False Positive alerts.

E. False Positive, False Negative

False positive occurs when your IDPSs generates an alert from normal user or system activity. If IDPSs generates too many false positives, then it will lose confidence in the capability of your IDPS to protect your network.

False negative occurs when an attack occurs against your system and the IDPSs fail to detect and notify the systems administrator. IDPSs must never generate false negatives. Most companies prefer the IDPSs generate more false positives rather than generating any false negatives [5].

Historically, IDPSs have been associated with high rates of false positives and false negatives. Most of the early technologies relied primarily on signature-based detection, which by itself is accurate only for detecting relatively simple well-known threats. Newer technologies use a combination of detection methods to increase accuracy and the breadth of detection, and generally the rates of false positives and false negatives have declined [6].

III. IDS INTRUSION DETECTION

Now we will make quick survey about the most popular IDSs systems based on the events that they are monitored and the methodology that they are using.

A. Host and network based

Intrusion may occur through hosts or networks, host-based Intrusion Detection (HIDS) examines many operations on the system, including function calls, files accessed, and so on. One common method for detecting anomalous user behavior is to establish a baseline of the operations that a user normally performs on the system. Then by monitoring deviations from the baseline, you can detect potentially malicious activity.

A network-based Intrusion Detection system (NIDS) monitor network traffic on packet level. The components are the network based IDS software, running on a dedicated host, connected to the network traffic with a network interface.

NIDS capture the network traffic from the wire as it travels to a host, then the captured packets analyzed and compare to a particular signature or for unusual or abnormal behaviors. Several sensors are used to sniff the packets on network which are basically computer systems designed to monitor the network traffic. If any suspicious or anomaly behavior occurs then they trigger an alert and pass the message to the central computer system or administrator (which monitors the IDS).

Host-based and network-based IDS normally maintain a database of system objects and also stores the system's normal and abnormal Behavior [7]. The database contains important information about system files, behavior and objects such as attributes, modification time, size, etc. If any suspicious or anomaly behavior occurs then it generates an alert and takes some appropriate response against detected threat or attack.

Researchers make studies on Host IDS and network IDS or both, SANS Institute [6] is example of using two technology, host-based IDS and network-based IDS, they Introduce software based solution which detects and protects the system from network layer up to application layer by known and unknown attacks. This software has great flexibility to set different type of filtering rules. The major drawback of this system is its high rate of false-positives. A lot of time and trained staff is required to monitor the IDS.

Muhammad Shibli and Sead Muftic [7] Provide host-based IDS to secure mobile agent. Secure mobile agent monitors the system, processes the logs, detects the attacks, and protects the host by automated real time response. Major disadvantage is that if the target of the attackers is mobile agent then it will be difficult to protect the system from being hacked. So it needs to adopt some security infrastructures for the protection of mobile agent.

Another research on host-based IPS done by M. Laureano, C. Maziero1, and E. Jamhour [8], they proposed architecture to protect Host-based IDS through virtual machine by observing the system behavior or monitor the system inside a virtual machine. This technique is efficient, duplication of real operating system, invisibility and inaccessibility to intruders. Multiple virtual machines can run simultaneously on same hardware.

David Wagner and Paolo Soto. [9] Examined technique on host-based which shows that how application interacts with the operating system and how to defraud IDS and make intrusion without detection, by using the technique of sequence matching, inserting malicious sequence.

B. Artificial intelligence intrusion detection

Application of the artificial intelligence is widely used for the IDS purpose. Researchers have proposed several approaches in this regard. Some of the researchers are more interested in applying rule based methods to detect the intrusion.

1) A Bayesian network

A Bayesian network is a probabilistic graphical model (a type of statistical model) that represents a set of random variables and their conditional dependencies via a directed acyclic graph.

Bayesian network methodology has a unique feature. For a given consequence, using the probability calculations Bayesian methodology can move back in time and find the cause of the events.

This feature is suitable for finding the reason for a particular anomaly in the network behavior. Using Bayesian algorithm, system can somehow move back in time and find the cause for

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

the events. This algorithm is sometimes used for the clustering purposes as well. D. Bulatovic, D. Velasevic [10] and M. Bilodeau, D. Brenner [11] are examples of this approach. Kruegel C., Mutz D., Robertson W. and Valeur F. Bayesian pointed out , a serious disadvantage of using Bayesian networks is that their results are similar to those derived from threshold-based systems, while considerably higher computational effort is required [12].

2) Data Mining and IDS

Data mining (DM), also called Knowledge-Discovery in Database, is the process of automatically searching large volumes of data for patterns using association rules.

Data Mining used in many computational techniques from statistics, information retrieval, machine learning and pattern recognition. The main function of data mining is to classify the captured events, as normal, or malicious, or as a particular type of attack [12, 13, 14].

Data mining can be done online [15] (real time) or offline [14, 16, 17, 18, 19].

Many researcher uses data mining to solve the intrusion detection problem. Researchers such D. Barbara, J. Couto, S. Jajodia, N. Wu, Ken. Yoshida, Lee W., and Stolfo S.J. [20, 21, 22, 23].

3) Markov

Markov chain is a set of states that are interconnected through certain transition probabilities, which determine the topology and the capabilities of the model. During a first training phase, the probabilities associated to the transitions are estimated from the normal behavior of the target system. The detection of anomalies is then carried out by comparing the anomaly score (associated probability) obtained for the observed sequences with a fixed threshold.

A hidden Markov model (HMM) is a statistical model where the system being modeled is assumed to be a Markov process with unknown parameters, and the challenge is to determine the hidden parameters from the observable parameters. The extracted model parameters can then be used to perform further analysis, for example for pattern recognition applications. A HMM can be considered as the simplest dynamic Bayesian network. Example of researcher work on that field Mahoney M.V., Chan P.K. Yeung DY, Ding Y. Este´vez-Tapiador J.M., Garcı´a-Teodoro P., and Dı´az-Verdejo J.E [24, 25, 26].

4) Fuzzy Logic

Fuzzy logic is derived from fuzzy set theory under which reasoning is approximate rather than precisely deduced from classical predicate logic.

Fuzzy logic is very appropriate for using on intrusion detection [27]; one reason is that usually there is no clear boundary between normal and anomaly events. The use of fuzziness of fuzzy logic helps to smooth the abrupt separation of normality and abnormality.

John E. Dickerson, Julie A. Dickerson, Susan M. Bridges, M. Vaughn Rayford M. Botha and R. von Solms are examples of those researchers that follow this approach [28, 29, 30]. Some researchers even used a multidisciplinary approach, for example, Gomez et al. [31] have combined fuzzy logic, genetic algorithm and association rule techniques in their work. Cho [32] reports a work where fuzzy logic and Hidden Markov Model (HMM) have been deployed together to detect intrusions. In this approach HMM is used for the dimensionality reduction.

Although fuzzy logic has proved to be effective, especially against port scans and probes, its main disadvantage is the high resource consumption involved. On the other hand, it should also be noticed that fuzzy logic is controversial in some circles, and it has been rejected by some engineers and by most statisticians, who hold that probability is the only rigorous mathematical description of uncertainty[30].

5) Artificial Neural Network

An artificial neural network (ANN) is a mathematical model or computational model that is inspired by the structure and/or functional aspects of biological neural networks. Neural networks have been adopted in the field of anomaly intrusion detection, mainly because of their flexibility and adaptability to environmental changes and to provide an unsupervised classification method to overcome the curse of dimensionality for a large number of input features. Since the system is complex and input features are numerous, clustering the events can be a very time consuming task. Using the Principle Component Analysis (PCA) or Singular Value Decomposition (SVD) methods can be an alternative solution [33]. However, if not used properly both of these methods can become computationally expensive algorithms. At the same time, reducing the number of features will lead to a less accurate model and consequently it will reduce the detection accuracy [34, 35, 36].

IV. IPS INTRUSION PREVENTION

Seeing the intrusion is thing and stopping it is another thing, seeing the attack occur will terrify the users of IT security, well trained IT security must deal with such attacks. If the highest priority of IT security is to stop intrusion then IDS just like an alert.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

IDS detect abnormal activity and generate alerts, but it do nothing to break the attack, just notify the system administrator, the notified administrator must respond quickly to block the attack, but for big companies IDSs will generate thousand to millions of alerts per day, most of them are false positive ones, It will be very difficult for the administrator to analyze all alerts, and make the right response for each one of them, so most intrusion are detected after the attacks.[5]

On other hand Intrusion Detection and Prevention System (IDPSs) Works like Intrusion Detection System (IDS) it detect abnormal activity but the only difference that IDPSs can respond to a detected threat by attempting to prevent it from succeeding, the main problem is: what is the exact repose for a specific threat, wrong response may affect the system more than the intruder will [5].

Many organizations choose to decrease false negatives at the cost of increasing false positives, which means that more malicious events are detected but more analysis resources are needed to differentiate false positives from true malicious events. The major problems in the IDPSs is the guarantee of the intrusion detection, and make the right response to stop the attack, this is the reason why in many cases IDPSs are used together with a human expert.

Anomaly-based IDPSs produce many false positive alert, this will need a lot of calculating time and resources, [37] discusses the foundations of the main Anomaly-Based intrusion detection technologies, together with their general operational architecture, and provides a classification for them according to the type of processing related to the ‘‘behavioral’’ model for the target system, there is many techniques enhancing the detection face and decreasing the false positive, [38] Make a review of using computational intelligence in intrusion detection system, characteristics of computational intelligence (CI) systems, such as adaptation, fault tolerance, high computational speed and error resilience in the face of noisy information.

Most researchers study the behavior of the intruders and attacks, and generate alerts to notify the system administrators, [39] worked on finding attack steps that are correlated in an attack scenario. They use algorithm to correlate multi-step cyber attacks in real time and constructing attack scenario system based on modeling multi-step cyber attacks. When generating alerts, the algorithm turns them into corresponding attack models based on the knowledge base and correlates them, whether alert or not is based on the weighted cost in the attack path graph and the attack degree of the corresponding host. And attack scenarios can be constructed by correlating the attack path graphs.

Ning P., Cui, Y., Reeves, D., Xu, [40] introduce framework that correlates alerts on the basis of prerequisites and consequences of attacks. To make successful attack you must actualize necessary conditions which called Prerequisites. And the results of the attacks called consequences. The framework matches the consequences of some prior alerts with the prerequisites of some new ones, to generate attack scenarios which are the combination of steps that attackers use in their attacks. They show the logical connection between otherwise independent IDS alerts. A successful attack arises from sequence of scenarios and each scenario may contain sub-scenarios. Then they represent each attack scenarios as a hyper alert correlation graph, which uses nodes to represent alerts and edges to represent the relationships between the alerts.

Dr. Eric Cole [41] presents a method to profile and identify attackers by analyzing attack scenarios and profile attributes. It creates profiling for the attacker techniques and steps which will be used by the intrusion detection system, and to predict attacker behavior.

V. CONCLUSION

Anomaly-based IDS is the best way to detect novel attacks, but it leads to high false positive alert which decrease the reliability of the IDS, usually for that a hybrid approach is used. In the hybrid approach, the signature-based approach is used together with the anomaly-based approach, in this way; the second approach is mostly used to detect novel attacks while the accuracy of the first approach (signature based approach) will provide a reliable detection for the known attacks.

IDPS has additional features to secure computer network system. The additional features identifying and recognizing suspicious threat trigger alert, event notification, through responsible response. In this preliminary observation from previously researchers, a hybrid technique is one good solution to classify and detect intrusion threat. Proposed hybrid IDPS takes the advantages to increase accuracy and precision normal or suspicious threat. For novel attacks (Anomaly-based detection) it will be difficult to choose the right response specially not all anomalies are threats.

Making response for the attacks detected by Signature-based detection is accurate, but for anomaly-based there is no clear response, deep studies on attacks behavior and what the best response to stop them without affecting the whole system will help the response for anomaly-based detection, specially most attacks have multi steps to achieve their goal, there must be technique that study attacks behavior and compare the sequence of events with these attacks’ behaviors to predict the consequence of next step, and make appropriate response minimize and prevent loses.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

REFERENCES

[1] Christos Douligeris, Aikaterini Mitrokotsa, "DDoS attacks and defense mechanisms:classification and state-of-the-art" ,Computer Networks:The International Journal of Computer and Telecommunications Networking, Vol. 44, Issue 5 , pp: 643 - 666, 2004.

[2] Z. Chen, L. Gao, K. Kwiat, "Modeling the spread of active worms,Twenty" Second Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM), Vol. 3, pp. 1890 1900, 2003.

[3] Ahmed Patel, Qais Qassim, Christopher Wills. "A survey of intrusion detection and prevention systems", Information Management & Computer Security Journal (2010).

[4] Allen J, Christie A, Fithen W, McHugh J, Pickel J, Stoner E. "State of the practice of intrusion detection technologies", Carnegie Mellon University Technical Report CMU/SEI-99- TR-028; 2000. CSI/FBI annual computer crime and security survey. ComputerSecurityInstitute,http://www.gocsi.com.

[5] Karen Scarfone,Peter Mell."Guide to Intrusion Detection and Prevention Systems (IDPS. National Institute of Standards and Technology(NIST),Feb 2007

[6] Host Intrusion Prevention Systems and Beyond, SANS Institute (2008).

[7] Muhammad Awais Shibli, Sead Muftic. "Intrusion Detection and Prevention System using Secure Mobile" Agents, IEEE International Conference on Security & Cryptography (2008).

[8] M. Laureano, C. Maziero1, E. Jamhour. "Protecting Host-Based Intrusion Detectors through Virtual" Machines,The International Journal of Computer and Telecommunications Networking (2007).

[9] David Wagner, Paolo Soto. "Mimicry Attacks on Host Based Intrusion" Detection Systems, 9th ACM Conference on Computer and Communications Security (2002).

[10] D. Bulatovic and D. Velasevic, "A distributed intrusion detection system based on bayesian alert networks," Lecture Notes in Computer Science (Secure Networking CQRE (Secure) 1999), vol. 1740,pp. 219–228, 1999.

[11] M. Bilodeau and D. Brenner, "Theory of multivariate statistics. Springer". Verlag : New York, 1999.Electronic edition at ebrary, Inc.

[12] Kruegel C., Mutz D., Robertson W., Valeur F. Bayesian "event classification for intrusion detection". In: Proceedings of the 19th Annual Computer Security Applications Conference; 2003.

[13] Ghosh,A.K.,A. Schwartzbard, and M. Schatz,"Learning program behavior profiles for intrusion detection", In Proc. 1st USENIX, 9-12 April, 1999

[14] Kumar, S., "Classification and Detection of Computer Intrusion", PhD.thesis, 1995, Purdue Univ., West Lafayette

[15] [5] D. Barbara, N. Wu, and S. Jajodia, "Detecting novel network intrusions using bayes estimators," in Proceedings of the First SIAM International Conference on Data Mining (SDM 2001), Chicago, USA, Apr. 2001.

[16] W. Lee, S.J.Stolfo et al, "A data mining and CIDF based approach for detecting novel and distributed intrusions", Proc. of Third International Workshop on Recent Advancesin Intrusion Detection (RAID 2000),Toulouse, France.

[17] Lee, W., S. J. Stolfo, and K. W. Mok, "A data mining framework for building intrusion detection models," In Proc. of the 1999 IEEE Symp. On Security and Privacy, Oakland, CA, pp. 120132. IEEE Computer Society Press, 9-12 May 1999

[18] Eric Bloedorn et al, "Data Mining for Network Intrusion Detection: How to Get Started," Technical paper, 2001.

[19] Singh, S. and S. Kandula, "Argus a distributed network intrusion detection system," Undergraduate Thesis, Indian Institute of Technology, May 2001.

[20] D. Barbara, J. Couto, S. Jajodia, and N. Wu, "Special section on data mining for intrusion detection and threat analysis: Adam: a testbed for exploring the use of data mining in intrusion detection," ACM SIGMOD Record, vol. 30, pp. 15–24, Dec. 2001.

[21] D. Barbara, N. Wu, and S. Jajodia, "Detecting novel network intrusions using bayes estimators," in Proceedings of the First SIAM International Conference on Data Mining (SDM 2001), Chicago, USA, Apr. 2001.

[22] Ken. Yoshida, "Entropy based intrusion detection," in Proceedings of IEEE Pacific Rim Conference on Communications, Computers and signal Processing (PACRIM2003), vol. 2, pp. 840–843. IEEE, Aug. 2003.

[23] Lee W., Stolfo S.J. Data mining approaches for intrusion detection.In: Proceedings of the 7th USENIX Security Symposium(SECURITY-98); 1998. p. 79–94

[24] Mahoney M.V., Chan P.K. "Learning nonstationary models of normal network traffic for detecting novel attacks". Proceedings of the Eighth ACM SIGKDD; 2002. p. 376–85.

[25] Yeung DY, Ding Y. "Host-based intrusion detection using dynamic and static behavioral models. Pattern Recognition` 2003;36(1) 229–43.

[26] Este´vez-Tapiador J.M., Garcı´a-Teodoro P., Dı´az-Verdejo J.E. "Detection of web-based attacks through Markovian protocol parsing" Proc. ISCC05; 2005 p. 457–62.

[27] J.E. Dickerson, J. Juslin, O. Loulousoula, and J. A. Dickerson, "Fuzzy Intrusion Detection", IFSA World Congress and 20th North American Fuzzy Information Processing Society (NAFIPS) International Conference, 2001, pp1506-1510.

[28] John E. Dickerson and Julie A. Dickerson, "Fuzzy network profiling for intrusion detection," Proceedings of NAFIPS 19th International Conference of the North American Fuzzy Information Processing Society, pp. 301–306, Atlanta, USA, July 2000.

[29] Susan M. Bridges and M. Vaughn Rayford, "Fuzzy data mining and genetic algorithms applied to intrusion detection," Proceedings of the Twenty-third National Information Systems Security Conference. National Institute of Standards and Technology, Oct. 2000.

[30] M. Botha and R. von Solms, "Utilising fuzzy logic and trend analysis for effective intrusion detection," Computers & Security, vol. 22, no. 5, pp. 423–434,2003.

[31] J. Gomez and D. Dasgupta, "Evolving fuzzy classifiers for intrusion detection," Proceedings of the 2002 IEEE Workshop on the Information Assurance, West Point, NY, USA, June 2001.

[32] S. B. Cho, "Incorporating soft computing techniques into a probabilistic intrusion detection system," IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICSPART C: APPLICATIONS AND REVIEWS, vol. 32, pp. 154–160, May 2002.

[33] M. Analoui, A. Mirzaei, and P. Kabiri, "Intrusion detection using multivariate analysis of variance algorithm," Third International Conference on Systems, Signals & Devices SSD05, vol. 3, Sousse,Tunisia, Mar. 2005. IEEE.

[34] Ste. Zanero and Sergio M. Savaresi, "Unsupervised learning techniques for an intrusion detection system," Proceedings of the 2004 ACM symposium on Applied computing, pp. 412–419, Nicosia, Cyprus Mar. 2004. ACM Press.

[35] H. Gunes Kayacik, A. Nur Zincir-Heywood, and Malcolm I. Heywood, "On the capability of an som basedintrusion detection system," Proceedings of the International Joint Conference on Neural Networks, vol. 3, pp. 1808–1813. IEEE, IEEE, July 2003.

[36] J. Z. Lei and Ali Ghorbani, "Network intrusion detection using an improved competitive learning neural network," Proceedings of the Second Annual Conference

[37] P. Garcıa-Teodoro, J. Dian-Verdejo, G. Macia-Fernandez, and E. Vazquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," Computer & Security, vol. 28, 2009, pp. 18-28.

[38] S.X. Wu and W. Banzhaf, "The use of computational intelligence in intrusion detection systems : A review," Applied Soft Computing, vol. 10, 2010, pp. 1-35.

[39] Modeling Zhijie Liu; Chongjun Wang; Shifu Chen; Nat."Correlating Multi-Step Attack and Constructing Attack Scenarios Based on Attack Pattern". Information Security and Assurance, 2008. ISA 2008. International Conference

[40] Ning, P., Cui, Y., Reeves, D., Xu, D." Techniques and Tools for Analyzing Intrusion Alerts". ACM Transactions on Information and System Security, Vol. 7, No. 2. May 2004.

[41] Dr. Eric Cole "Constructing Attack Scenarios for Attacker Profiling and Identification"

Extended Sakai-Kasahara Identity-Based Encryption Scheme to Signcryption Scheme

Hussein Khalid Abd-Alrazzaq[1]

[1] College of Administration and Economic-Ramadi, Anbar University,
Anbar, Iraq
hu_albasri@yahoo.co.uk

***Abstract*— Identity-Based Signcryption (IBSC) is a better approach would be to exploit the similarities between IBE and IBS in order to provide a dual-purpose IB Encryption-Signature (IBSE) scheme based on a shared infrastructure, toward efficiency increases and security improvements. In this paper describes a new identity-based signcryption scheme built upon SK scheme. It combines the functionalities of signature and encryption and it is prove security in a formal model under computational assumptions and in the random oracle model. As a result, this paper propose a new secure identity-based signcryption (IBSC) scheme that is also compare it with the other from efficiency points of view.**

Keywords: Public Key Cryptography, Identity-Based Cryptography, Identity-Based signcryption, Sakai-Kasahara IBE

I. Introduction

The notion of identity-based (IB) cryptography was proposed by Shamir [1] as a specialization of public key (PK) cryptography which dispensed with the need for cumbersome directories, certificates, and revocation lists. This concept have advantageous over the traditional public key cryptosystems (PKC), it is used to eliminate the complexity of using digital certificates to public key register, where the public key of a user (in IBC) can be derived from public information that uniquely identifies the user Because of this, IB systems implement an automatic directory with implicit binding, without the need for costly certification and public key publication steps. Although public keys can be computed by anyone from public information, the corresponding private key can only be extracted by a trusted authority called the private key generator (PKG). The PKG has custody of a master secret, which allows it to compute any private key in the IB system. The PKG can be thought of as an identity-based analog to the CA at the helm of a traditional public key infrastructure [2].

Identity-Based Signature schemes (IBS) have been devised since 1984 But a satisfying Identity-Based Encryption scheme (IBE) only appeared in 2001 by Boneh and Franklin gave a practical Identity-Based Encryption scheme that relies on the bilinear Diffie-Hellman problem for its security. It uses a complicated mathematical transformation called the Tate pairing [3].

The concept of public key signcryption schemes was found by Zheng in 1997 [4]. The idea of this kind of primitive is to perform encryption and signature in a single logical step in order to obtain confidentiality, integrity, authentication and non-repudiation more efficiently than the sign-then-encrypt approach. Several efficient signcryption schemes have been proposed since 1997 and a first example of formal security proof in a formal security model was published in 2002 [5]. However, until 2002, none of these schemes were identity based

II. Sakai-Kasahara Identity-Based Encryption (SK-IBE)

Sakai-Kasahara IBE an example of the family of "exponent inversion" schemes, in which a private key of the form $g^{1/a}$ is used to decrypt a ciphertext. SK-IBE is a secure IBE scheme based on the k-BDHI problem, while. The security of BF-IBE is based on the BDH problem. The advantage of SK-IBE is that it has better performance than BF- IBE, particularly in encryption. SK-IBE is faster than BF-IBE in two aspects. First, in the Encrypt algorithm of SK-IBE, no pairing computation is required because $\hat{e}\ (P_1, P_2)$ can be pre-computed. Second, in operation of mapping an identity to an element in G1 or G2, the map to point algorithm used by BF-IBE is not required. Instead of that, SK-IBE makes use of an ordinary hash-function, this avoids a modular exponentiation. Therefore SK-IBE provides an attractive performance; also SK-IBE is secure against adaptive chosen ciphertext attacks in the random oracle model based on the *q*-BDHI assumption [6].

In these schemes, a string representing an identity is hashed to an integer that is then used in the encryption and decryption operations. An SK-IBE scheme consist four steps [7]:

- Setup takes as input k, and returns a master public key M_{pk} and a master secret key M_{sk}.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

- Extract takes as input M_{pk}, $M_{sk}$and $ID_A \in \{0,1\}$ an identifier string for entity A, and returns the associated private key dA.
- Encrypt takes as input M_{pk}, ID_A and a message m , and returns a ciphertext *C*.
- Decrypt takes as input M_{pk}, ID_A, d_A and *C*, and returns the corresponding value of the plaintext *m*

III. The Identity-Based Signcryption Primitive

An Identity-Based Signcryption scheme, or IBSC, comprises four algorithms: Setup, Extract, Signcrypt, and Unsigncrypt. In a (two-layer) IBSC with detachable signature, the signcryption/unsigncryption algorithms are the composition of explicit subroutines: Signcrypt = Encrypt ° Sign and Unsigncrypt = Verify ° Decrypt.

In summary, Setup generates random instances of the common public parameters and master secret; Extract computes the private key corresponding to a given public identity string; Signcrypt produces a signature for a given message and private key, and then encrypts the signed plaintext for a given identity (note that the encryption routine may specifically require the signature as input); Decrypt decrypts a ciphertext using a given private key; Verify checks the validity of a given signature for a given message and identity. Messages are arbitrary strings in $\{0,1\}^*$. the functions that compose a generic IBSC scheme are as follows [2]:

- **Setup**: produces a pair (msk, mpk), where msk is a randomly generated master secret and mpk the corresponding common public parameters.
- **Extract** (mpk, msk, ID): On input ID, computes a private key sk which corresponding to the identity *ID* under (msk, mpk).
- **Signcrypt** (mpk, IDS, IDR, skS, m): The sequential application of
  - **Sign** (mpk, ID_S, sk_S, m): On input (ID_S, sk_S, m), outputs a signature *s*, for sk_S, under mpk, and some ephemeral state data r .
  - **Encrypt** $(mpk, ID_R, sk_S, m, s, r)$: On input (ID_R, sk_S, m, s, r), outputs an anonymous ciphertext *C*, containing the signed message (m, s) encrypted for the identity ID_Runder mpk.
- **Unsigncrypt** (mpk, sk_R, C): The sequential application of
  - **Decrypt** (mpk, sk_R, C): On input (sk_R, C), outputs a triple (ID_S, m, s) (containing the purported sender identity and signed message obtained by decrypting *C* by the private key sk_Runder mpk).
  - **Verify** (mpk, ID_S, m, s): On input (ID_S, m, s), outputs "true" or "false" (indicating whether *s* is a valid signature for the message *m* by the identity ID_S, under mpk).

IV. Complexity Assumption

Strong Diffie-Hellman (q-SDH): *F*or an integer $q, and\ x \in z_p^*, P \in G_1$, given $(P, xP, x^2P, \dots, x^qP)$ computing $\left(h\ \frac{1}{h+x}P\right)\ where\ h \in z_p^*\ is\ hard$ [5].

The Bilinear Diffie-Hellman Problem (BDHP): let $\mathbb{G}_1$, $\mathbb{G}_T$ two groups of prime order *q*, $\hat{e}: \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_T$, be bilinear map, *P* be a generator of $\mathbb{G}_1$. The BDHP is: given *P*, *aP*, *bP*, *cP*, where *a*, *b* $c \in Z_p^*$ calculate $\hat{e}(P, P)^{abc}$. Solving the BDHP is no more difficult than calculating discrete logarithms in either G_1 or G_T .If it can find the value of *c* by calculating the discrete logarithm of *cP* in $\mathbb{G}_1$, then it can calculate $\hat{e}(aP, bP)^c = (\hat{e}(P, P)^{ab})^c = (\hat{e}(P, P)^{abc}$ or, if it can find the value of *c* by calculating the discrete logarithm of $\hat{e}(P, cP) = \hat{e}(P, P)^c$ in $\mathbb{G}_T$then it also calculate $\hat{e}(P, P)^{abc}$ in a similar way[3].

***q*-Bilinear Diffie-Hellman Inversion Problem (*q*-BDHIP):** let $\mathbb{G}_1$, $\mathbb{G}_T$ two groups of prime order *q*, $\hat{e}: \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_T$, be bilinear map, *P* be a generator of $\mathbb{G}_1$. The *q*-BDHIP is: given *P*, *aP*, a^2P, ... , a^qP, calculate $\hat{e}(P, P)^{\frac{1}{a}}$. Solving the *q*-BDHIP is difficult as calculating discrete logarithms in either G_1or G_T. if it can find the value of a by calculating the discrete logarithm of aP in G_1, then it can calculate $\frac{1}{a}$ and then calculate$\hat{e}(P, P)^{\frac{1}{a}}$. Or if it can find the value of a by calculating the discrete logarithm of $\hat{e}(P, aP) = \hat{e}(P, P)^a$ in G_T then it also calculate $\hat{e}(P, P)^{\frac{1}{a}}$ in a similar way [6].

Decisional Bilinear DH Inversion Problem (q-DBDHI): For an integer $q, and\ x, r \in z_p^*$, $P_2 \in \mathbb{G}_1$, $P1 = \psi(P_2), \hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_T$, distinguishing between the distributions $(P_1, P_2, xP_2, x^2P_2, \dots, x^qP_2, \hat{e}(P_1, P_2)^{1/x})$ and $(P_1, P_2, xP_2, x^2P_2, \dots, x^qP_2, \hat{e}(P_1, P_2)^r)$ is hard [6].

V. The Proposed Scheme

In this paper proposed identity-based signcryption scheme through modification on Sakai-Kasahara IBE to build efficient signcryption schemes. There are many of authors have proposed various new identity-based signcryption schemes, but this paper proposed new scheme belong to the family of "exponent inversion" schemes. This scheme acquires its power form the *q*-bilinear Diffie-Hellman inversion problem which is depending on the elliptic curve discrete logarithm.

A. Sakai-Kasahara Identity-Based Signcryption (SK-IBSC)

The proposed scheme involves three roles: the Private Key Generator (PKG), the sender *S*, and the message recipient *R*. It consists of four algorithms: Setup which is used to generate public parameters used throughout the life of the system, Extraction which used to generate private key correspond with the user's identity, Signcrypt

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

which used to sign and encrypt the message by the sender, and Unsigncrypt which used to verify and decrypt the message by the recipient. The details of them are described as below.

Setup: Let P be a generator of $\mathbb{G}_1$. Pick a random $s, a \in \mathbb{Z}_p^*$ and set $P_1 = sP$, $P_2=aP$. Additional cryptography hash functions used to add chosen-ciphertext security, as in SK IBE full scheme, H_1:$\{0, 1\}^* \rightarrow \mathbb{Z}_p$, H_2: $\mathbb{G}_T \rightarrow \{0, 1\}^n$, $H_3 : \{0, 1\}^n \rightarrow \mathbb{Z}_p^*$, $H_4 : \{0,1\}^n \rightarrow \{0,1\}^n$.The master secret for SK-IBSC is s and a , the public parameters are: q (order of $\mathbb{F}q$), $E/\mathbb{F}q$, p (Prime number: $p \mid \#E(\mathbb{F}q)$, $\mathbb{G}_1$ and $\mathbb{G}_T$ are Cyclic group where $\langle P\rangle$ and $\hat{e}\langle(P,P)\rangle$ generated of them, Respectively,$\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_T$, n,P,P_1,P_2, $v=\hat{e}(P,P)$ H_1, H_2, H_3, H_4).

Extraction: Given a user's identity (*ID*), PKGC generates the Private key corresponding to ID, as following:

1. computes the hash value $q_{ID} = H_1(ID)$
2. computes the corresponding private key $d_{ID} = \frac{1}{s+q_{ID}} P$

Signcrypt: the sender encrypts the message *M* with recipient's ID (ID_R) as public key, and sign M with his private key (d_{ID_S}) as in the following steps:

1. Compute a public key of recipient $q_{ID_R} = H_1(ID_R)$
2. $Pick\ a$ random $x, \sigma \in \mathbb{Z}_p^*$
3. Compute $r = H_3(M, \sigma, x)$
4. Compute $U = r\left(P_1 + q_{ID_R}P\right) = r\left(s + q_{ID_R}\right)P$
5. Compute $K = H_2(v^r)$
6. Compute $z = \sigma \oplus K$
7. Compute $Y = xP$
8. Compute $W = xd_{ID_S} + zP_2$
9. Compute $C = M \oplus \sigma$
10. send (C, W, U, z, Y) as ciphertext

Unsigncrypt: the recipient Input his/her private key (d_{ID_R}), ciphertext (C, W, U, z, Y) and sender's public key (ID_S) to decrypt and verify, as in the following steps:

1. Compute a public key of sender $q_{ID_S} = H_1(ID_S)$
2. Compute $K = H_2(\hat{e}\left(U, d_{ID_R}\right))$
3. Compute $\sigma = z \oplus K$
4. Compute $M = C \oplus \sigma$
5. $If\ \hat{e}\left(W, q_{ID_S}P + P_1\right) = \hat{e}(Y,P)\hat{e}(zP_2, q_{ID_S}P + P_1)$ then the signature is true.

The consistency is easy to verify by the bilinearity of the map. Indeed, We have $\hat{e}\left(W, q_{ID_S}P + P_1\right) = \hat{e}(Y,P)\hat{e}(zP_2, q_{ID_S}P + P_1)$, where $\hat{e}\left(xd_{ID_S}, q_{ID_S}P_1\right) = \hat{e}(Y,P)$and $\hat{e}\left(zP_2, q_{ID_S}P + P_1\right) = \hat{e}(zP_2, q_{ID_S}P + P_1)$ Anyone can be convinced of the message's origin by using Z to retrieve the message and verify the signature without error that is mean this message not modified. The knowledge of the plaintext m is not required for the verification.

B. Analysis of the Scheme

Correctness

$$K = H_2\left(\hat{e}\left(U, d_{ID_R}\right)\right)$$

$$= H_2\left(\hat{e}\left(r\left(P_1 + q_{ID_R}P\right), \frac{1}{s+q_{ID}}P\right)\right)$$

$$= H_2(\hat{e}\left(r\left(s + q_{ID_R}\right)P, \frac{1}{s+q_{ID}}P\right))$$

$$= H_2\left(\hat{e}(rP,P)^{\left(s+q_{ID_R}\right)*\frac{1}{s+q_{ID_R}}}\right) = H_2(\hat{e}(P,P)^r)$$

$$= H_2(v^r)$$

$$\hat{e}\left(W, q_{ID_S}P + P_1\right) = \hat{e}\left(xd_{ID_S} + zP_2, q_{ID_S}P + sP\right)$$

$$= \hat{e}\left(x\frac{1}{s+q_{ID}}P + zaP, (q_{ID_S} + s)P\right)$$

$$= \hat{e}(x\frac{1}{s+q_{ID_S}}P, (q_{ID_S} + s)P)\ \hat{e}(zaP, (q_{ID_S} + s)P)$$

$$= \hat{e}(P,P)^{x\frac{1}{s+q_{ID_S}}*(q_{ID_S}+s)}\ \hat{e}(P,P)^{za(q_{ID_S}+s)}$$

$$= \hat{e}(P,P)^x\ \hat{e}(P,P)^{za(q_{ID_S}+s)}$$

$$\hat{e}(Y,P)\hat{e}\left(zP_2, q_{ID_S}P + P_1\right)$$

$$= \hat{e}(P,P)^x\hat{e}\left(zaP, \left(q_{ID_S} + s\right)P\right)$$

$$= \hat{e}(P,P)^x\hat{e}(P,P)^{za\left(q_{ID_S}+s\right)}$$

Security

Unforgeability: Since the signcryption produce of modified the as the Sakai-Kasahara IBE scheme, forging a ciphertext for any message m is equivalent to forge a Sakai-Kasahara scheme, because the proposed scheme based on the same computational problem. It has unforgeability against adaptive chosen message attacks (in the random oracle) assuming the q-BDHI problem is hard. Therefore, the attacker needs to use the privet key of the true sender if he wants to forge the original signature. Because that impossible the attacker must replace his identity form his private key $\frac{1}{s+q_{ID_{Attacker}}}P$ with identity of original to general forged private key for sender $\frac{1}{s+q_{ID_S}}P$. In order do this process; the attacker must solve the q-BDHI problem.

Confidentiality: Because the *U* contains secret random number and public of recipient, this information only intended recipient can compute *K* and recover *m*. because the K compute form v^r and r included in U, therefore, only the person that has the private key which is correspond with identity used in a U, can computes a K, $K = H_2(\hat{e}\left(U, d_{ID_R}\right))$**.** If the attacker can extract the r form U then he can retrieve the plaintext. But he cannot do that, only If he can find the value of *r* by calculating

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

the discrete logarithm of rP from $r(P_1 + q_{ID_R}P)$. In our scheme, the confidentiality is the same as the Sakai-Kasahara, unsigncryption phase, anyone can not retrieve the message without has the intended private key.

Verifiability: Anyone can verify the signature by step 5 of Unsigncryption, so our scheme provides the public verifiability without need to secrete parameters.

Non-Repudiation: The scheme provides nonrepudiation. the sender use his private key in signcrypt, in order to prevent the sender attempts deny the fact that she/he is signcrypted the message multiply the private key of sender with x which is used to generate the r, alse add the last with zP which is produce form XOR between K and σ, and z is necessary to retrieve the message. Therefore; if recipient use the z to decrypt the message and use it with public key of the sender and x to verify the signature, then the sender cannot deny.

C. Efficiency

It now assesses the comparative efficiency of some identity-based signcryption schemes, implemented according to their original descriptions. Table-1 summarizes the number of relevant basic operations underlying several identity-based signcryption. It only consider the pairing, point multiplication, exponentiation computation, and hash

Table 1, The computation necessary for various IBSC

Scheme	Sign/Encrypt				Decrypt/Verify			
	Pairings	exp	mul	hashs	Pairings	exp	mul	hash
Boyen-IBSC [8]	1	1	3	5	4	-	2	6
Libert-Quisquater-IBSC [9]	2	-	3	3	4	-	1	3
Malone-Lee [10]	1	-	3	3	4	-	1	2
Chen-Malone-Lee [11]	1	-	3	4	3	-	1	4
Our scheme	-	1	4	3	4	-	2	2

VI. Conclusion

In this paper, it has proposed extended the Sakai-Kasahara IBE scheme to build a new efficient identity based signcryption scheme that provides a best security than other scheme (such as Malone-Lee's scheme) because it satisfies security under q-BDHI assumption which is a stronger assumption than the difficulty of the computational bilinear problem. In addition, this scheme is derivation from Sakai-Kasahara full-scheme then it is resistant to chosen plaintext attacks, adaptive chosen-identity attacks, chosen-ciphertext attacks, and adaptive chosen-identity attacks. This scheme is more efficient than the approach consisting in combining the Sakai-Kasahara encryption scheme with a signature. Our scheme seems to be a reasonable base for the security of cryptosystems comparative with the others.

Reference

[1] A. Shamir, Identity Based Cryptosystems and Signature Schemes, Advances in Cryptology - Crypto' 84, LNCS 0196, Springer, 1984.

[2] AlexanderW. Dent · Yuliang Zheng, " Practical Signcryption", springer, 2010.

[3] Sufyan T. Faraj Al-Janabi, Hussein Khalid Abd-Alrazzaq,"Combining Mediated and Identity-Based Cryptography for Securing E-Mail", Springer-Verlag Berlin Heidelberg, 2011.

[4] Y. Zheng, H. Imai, Efficient Signcryption Schemes On Elliptic Curves, Proc. of IFIP/SEC'98, Chapman & Hall, 1998.

[5] J. Baek, R. Steinfeld, Y. Zheng, "Formal Proofs for the Security of Signcryption", Proc. of PKC'02, LNCS 2274, Springer, pp. 81-98.

[6] Cheng, Zhaohui and Chen, Liqun (2005), "Security proof of Sakai-Kasahara's identity-based encryption scheme", 10th IMA International Conference on Cryptography and Coding, Cirencester, UK, Springer-Verlag, pp. 442-459

[7] Martin, L.: Introduction to Identity-Based Encryption. Artech House Inc. (2008).

[8] X. Boyen. Multipurpose identity-based signcryption: A Swiss army knife for identity-based cryptography). In D. Boneh, editor, Advances in Cryptology – Crypto 2003, volume 2729 of Lecture Notes in Computer Science, pages 383–399. Springer, 2003.

[9] Benoit Libert, Jean-Jacques Quisquater, "A new identity based signcryption scheme from pairings", ITW2003, Paris, France, 2003

[10] J. Malone-Lee. "Identity-based signcryption". Cryptology ePrint Archive, Report 2002/098, 2002. http://eprint.iacr.org/2002/098.

[11] L. Chen and J. Malone-Lee. Improved identity-based signcryption. In PKC'05, volume 3386 of LNCS, pages 362{379. Springer, 2005.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Multi-Pixel Steganography

Dr. R. Sridevi
Department of Computer Science & Engineering
JNTUH College of Engineering
Hyderabad, A.P., INDIA
sridevirangu@yahoo.com

G. John Babu
Department of Computer Science & Engineering
Sreekavitha Engineering College
Khammam- A.P. - INDIA
johnbabug@gmail.com

***Abstract*— With the advent of digital images information hiding in images known as Image steganography has gained wide acceptance as a means covert communications. This paper presents an innovative technique to hide the information in images. For any steganographic technique the evaluating parameters are deformation of cover image by the hidden message and the amount of hidden message. The former parameter should be minimum where as the payload or the size of information that can be hidden should be maximum. The proposed technique offers high payload with minimal distortion of the cover image.**

Keywords-component; Steganography, Information hiding, Pixel value differencing, hiding capacity

I. INTRODUCTION

Steganography is defined as the practice of undetectably altering a Work to embed a secret message[1]. Information hiding (or data hiding) is a general term encompassing a wide range of problems beyond that of embedding messages in content. The term *hiding* here can refer to either making the information imperceptible (as in watermarking) or keeping the existence of the information secret. The explosion of Internet and multimedia content has paved the way for increasing focus on the methods of digital steganography. The goal of steganography is to convey a secret message under a cover and concealing the very existence of information[2]. Any method of steganography involves a medium to hide the secret data referred to as cover medium. Cover media for steganography includes, text, images, audio, video etc. Among these images have been the best suitable medium for the steganography, due to the redundancy in the digital images. The original image in which the secret message is referred to as cover image and the altered image in which a secret data is embedded is called a stego-image. The performance of a steganographic method can be evaluated by the similarities between the cover image and stegoimage. An efficient steganographic method produces a stego image that is very similar to the cover image [3]. The art of detecting the existence of secret message is called steganalysis. Digital image is an array of numbers that indicate light intensities at various points called pixels[4]. A gray scale image consists of pixels with intensity range [0,255]. Black is represented by pixel value 0and white color is represented by pixel value 255. Each pixel value can be represented by a 8 bit binary number. These pixel values are manipulated or modified as per the steganographic scheme to embed a secret message.

II. METHODS OF STEGANOGRAPHY

In this section we would like to review some of the existing and related methods. A mostly widely used method is Least Significant Bit method.(here onwards referred to as LSB method) In this method the least significant bit(s) are replaced by the secret message bits. And the receiver will arrange all the least significant bit(s) of the binary values of the pixels to get the secret message. Though LSB method is simple and easy to implement it is very vulnerable to the lightest modifications in stego image[4]. Many steganalysis methods have been proposed to detect LSB replacement and it is even possible to estimate the length of secret message hidden in cover image[4][5][6]. Many modifications have been proposed in the past decade for this LSB method to make it more effective and efficient [7][8]. Numerous Spatial domain steganographic techniques have been proposed in the past decade. Some of the related methods to the proposed method in this paper are Wu and Tsai's pixel value differencing method and Chang and Tseng's side match method.

III. Review of Related Methods

Wu and Tsai scheme[9] was a major breakthrough in spatial domain techniques. This method has produced high quality stego images when compared with LSB and other peer methods. The cover images used in the PVD method are supposed to be gray scale images. In the embedding phase a difference value d is computed from every non-overlapping block of two consecutive pixels, say p_i and p_{i+1} of a given cover image. The way of partitioning the cover image into two-pixel blocks runs through all the rows of each image in a zigzag manner. Assume that the gray values of p_i and $p_{i+1}$are g_i and g_{i+1}, then d is computed as $g_{i+1} - g_i$ which may be in the range from -255 to 255. A block with d close to 0 is considered to be an extremely smooth block, whereas a block with d close to -255 or 255 is considered as a sharply edged block. The method only considers the absolute values of d (0 through 255) and classifies them into a number of contiguous ranges, such as Rk where $k=1,2,\ldots,q$. These ranges are assigned indices 1 though n. The lower and upper bound

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

values of *Rk* are denoted by *lk* and u*k*, respectively. The width of *Rk* is u*k*-lk+1.In PVD method, the width of each range is taken to be a power of 2. Every bit in the bit stream should be embedded into the two-pixel blocks of the cover image. Given a two-pixel block *B* with gray value difference *d* belonging to *k*th range, then the number of bits, say n, which can be embedded in this block, is calculated by n=log (uk-lk+1) which is an integer. A sub-stream S with *n* bits is selected from the secret message for embedding in *B*. A new difference *d'* then is computed with equation 1.

$$d' = \begin{cases} l_k + b & d \geq 0 \\ -(l_k + b) & d < 0 \end{cases} \quad (1)$$

where *b* is the value of the sub-stream *S* . Because the value *b* is in the range [0, u_k-l_k], the value of *d'* is in the range from *lk* to *uk* . If we replace *d* with *d*', the resulting changes are presumably unnoticeable to the observer. Then *b* can be embedded by performing an inverse calculation from '*d'* to yield the new gray values (gi*, gi+1*) for the pixels in the corresponding two-pixel block (p_i,p_{i+1}) of the stego-image. The inverse calculation for computing (gi*, gi+1*) from the original gray values (g_i, g_{i+1}) of the pixel pair is based on a function given in equation 2.

$$(g_i^*, g_{i+1}^*) = \begin{cases} (g_i - \lceil m/2 \rceil, g_{i+1} + \lfloor m/2 \rfloor) \text{ if } d \text{ is odd} \\ (g_i - \lfloor m/2 \rfloor, g_{i+1} + \lceil m/2 \rceil) \text{ if } d \text{ is even} \end{cases} \quad (2)$$

where *m* is $|d' - d|$. The embedding is only done for pixels which their new values would fall in the range of [0,255]. In the extracting phase, the original range table is necessary. It is used to partition the stego-image by the same method used for the cover image. Calculate the difference value d*(p_i, p_{i+1}) for each block of two consecutive pixels Then, find the optimum Ri of the d* same as in the hiding phase. Subtract l_i which is the lower bound of the range R_i from d*(p_i, p_{i+1}) and b_0 is obtained. The b0 value represents the secret data in decimal number. Transform b0 into binary with t bits, where t = [$\log_2 w_i$]. The t bits can stand for the original secret data of hiding. Existing steganalysis methods could not detect the data embedding by PVD Method. The only disadvantage of this method is that the embedding capacity reduces considerably compared with LSB and other related methods.

A considerable improvement of PVD method has been proposed with a title 'Pixel Value Differencing Method with Modulus function'. This method has produced high quality stego images than those produced by PVD method[10] with same embedding capacity. This method adjusts the modulus of the sum of two consecutive pixels to embed a secret message instead of pixel value difference adjustment used in PVD method. This method has shown considerable improvement in stego image quality.

IV. Proposed Embedding Method

The major disadvantage of the PVD modulus method is that the embedding capacity is moderate, when compared to LSB and other methods. In the proposed method an attempt has been made to enhance the embedding capacity within the acceptable limits of quality for stego-images. In this method a group of four pixels is considered as a block, as shown in the figure below.

$P_{(x,y)}$	$P_{(x+1,y)}$
$P_{(x,y+1)}$	$P_{(x+1,y+1)}$

Fig: 1

The whole image is divided into the blocks of four group pixels. i.e in a 512x512 image can be divided into 256 x 256 blocks. One of such blocks is shown in the above figure. The top left pixel is taken as the reference pixel and the pixel value difference between the three other pixels and the referenced pixel is calculated.

$$d_0 = P_{(x+1,y)} - P_{(x,y)}$$

$$d_1 = P_{(x,y+1)} - P_{(x,y)}$$

$$d_2 = P_{(x+1,y+1)} - P_{(x,y)}$$

A range table has been used for embedding process. Range table is table of different ranges with in 0-255. Each range width is taken as some power of 2. And number of bits that can be embedded is determined by the width of the range in which the pixel value difference falls. The range table used in the proposed method is shown in the figure 2.

	width	No. of bits that can be hidden
0 7	8	3
8 15	8	3
16 31	16	4
32 63	32	5
64 127	64	6
128 255	128	7

Fig 2.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

For each d_i value suitable range is chosen from the range table and the number of bits t_i that can be embedded in that pixel pair is calculated from the width of the range $|w_i|$. For each of three blocks the secret data binary bits(t_i number of bits) are converted to decimal equivalents v_i. For each pixel pair in the block F_{rem} is calculated from the following equation.

$$F_{rem(i)} = (P_{(i,x)} + P_{(i,y)}) \bmod v_i$$

By using the following criterion Compute the modified values of the three pixel pairs

case 1:

$$F_{rem(i)} > v \quad and \quad m \le \frac{2^{t_i}}{2} \quad \text{and } P_{(i,x)} \ge P_{(i,y)}$$

$$P^*_{(i,x)} = P_{(i,x)} - \lceil m/2 \rceil \; ; \; P^*_{(i,y)} = P_{(i,y)} - \lfloor m/2 \rfloor$$

case 2:

$$F_{rem(i)} > v \quad and \quad m \le \frac{2^{t_i}}{2} \quad \text{and } P_{(i,x)} < P_{(i,y)}$$

$$P^*_{(i,x)} = P_{(i,x)} - \lfloor m/2 \rfloor; \; P^*_{(i,y)} = P_{(i,y)} - \lceil m/2 \rceil$$

case 3:

$$F_{rem(i)} > v \quad and \quad m > \frac{2^{t_i}}{2} \quad \text{and } P_{(i,x)} \ge P_{(i,y)}$$

$$P^*_{(i,x)} = P_{(i,x)} + \lfloor m_1/2 \rfloor; \quad P^*_{(i,y)} = P_{(i,y)} + \lceil m_1/2 \rceil$$

case 4:

$$F_{rem(i)} > v \quad and \quad m > \frac{2^{t_i}}{2} \quad \text{and } P_{(i,x)} < P_{(i,y)}$$

$$P^*_{(i,x)} = P_{(i,x)} + \lceil m_1/2 \rceil \; ; \quad P^*_{(i,y)} = P_{(i,y)} + \lfloor m_1/2 \rfloor$$

case 5:

$$F_{rem(i)} \le v \quad \text{and} \quad m \le \frac{2^{t_i}}{2} \quad \text{and } P_{(i,x)} \ge P_{(i,y)}$$

$$P^*_{(i,x)} = P_{(i,x)} + \lfloor m/2 \rfloor \; ; \quad P^*_{(i,y)} = P_{(i,y)} + \lceil m/2 \rceil$$

case 6:

$$F_{rem(i)} \le v \quad \text{and} \quad m \le \frac{2^{t_i}}{2} \quad \text{and } P_{(i,x)} < P_{(i,y)}$$

$$P^*_{(i,x)} = P_{(i,x)} + \lceil m/2 \rceil; \; P^*_{(i,y)} = P_{(i,y)} + \lfloor m/2 \rfloor$$

case 7:

$$F_{rem(i)} \le v \quad \text{and} \quad m > \frac{2^{t_i}}{2} \quad \text{and } P_{(i,x)} \ge P_{(i,y)}$$

$$P^*_{(i,x)} = P_{(i,x)} - \lceil m_1/2 \rceil \; ; P^*_{(i,y)} = P_{(i,y)} - \lfloor m_1/2 \rfloor$$

case 8:

$$F_{rem(i)} \le v \quad \text{and} \quad m > \frac{2^{t_i}}{2} \quad \text{and } P_{(i,x)} < P_{(i,y)}$$

$$P^*_{(i,x)} = P_{(i,x)} - \lfloor m_1/2 \rfloor \; ; P^*_{(i,y)} = P_{(i,y)} - \lceil m_1/2 \rceil$$

where $m = |F_{rem(i)} - w|$ and $m_1 = 2^{t_i} - |F_{rem(i)} - w|$

From the above criterion new values for the four pixel block are calculated. And from among the three pairs present in the block, the pair which produces minimum Mean Square Error(MSE) is chosen as the reference pair. Keeping the values of the reference pair as constant, other two pixels values are adjusted with offset. The total number of bits embedded is $t_1 + t_2 + t_3$.

V. PROPOSED EXTRACTION METHOD

The extraction method is quite simple and the the range table used in the embedding process is supposed to be available in extraction process. The stego-image is divided into blocks of four pixels, same as in the embedding process. For each pair the difference d_i is calculated. And for each d_i the suitable range is identified and the number of bits embedded is computed($t_i = \log_2|w|$). F_{rem} is calculated for each pair. That value of F_{rem} is the decimal equivalent of the binary bits embedded.

VI. RESULTS & ANALYSIS

To demonstrate the accomplished performance of proposed approach in capacity of hiding secret data in the stego-image, and Stego-image quality, I have conducted different experiments using twelve images Baboon, Boat, Couple, Elaine, Jesse, Jet, Leena, Man, Peppers, Tank, Tiffany, and Truck, with range widths 8,8,16,32,64,128 in the range table. The proposed method is proved to be facilitating higher embedding capacity than the PVD modulus method. The results are shown in the table1.

Capacity in Bytes			
image	PVDM	Proposed	%increase
Baboon	57162	89315	56.25
Boat	52428	78732	50.17
Couple	51604	78431	52.00
Elaine	50021	75589	51.11
Jesse	55283	82627	49.50
Jet	51301	77817	51.70
Lena	51233	76762	49.83
Man	53940	81268	50.66
Peppers	50922	76647	50.52
Tank	50111	76104	51.87
Tiffany	50821	76203	50.00
Truck	49704	76194	53.30

Table1 : Hiding Capacity

PSNR VALUES			
	PVD	**PVDM**	**Proposed**
Baboon	36.86	40.19	32.82
Boat	38.97	42.086	36.48
Couple	40.259	43.471	36.43
Elaine	42.737	45.494	39.51
Jesse	36.973	40.201	34.21
Jet	40.26	43.406	36.59
Lena	41.09	44.017	38.05
Man	36.973	41.162	35.05
Peppers	40.693	43.552	37.30
Tank	42.752	45.498	39.32

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Tiffany	40.861	44.149	37.84
Truck	43.226	45.908	39.55

Table 2: PSNR values

Signal-to-noise (SNR) measures are estimates of the quality of a reconstructed image compared with an original image. The basic idea is to compute a single number that reflects the quality of the reconstructed image. Reconstructed images with higher metrics are judged better. In fact, traditional SNR measures do not equate with human subjective perception. Signal-to-noise measures are easier to compute. We have to note that higher measures do not always mean better quality.

The actual metric we will compute is the peak signal-to-reconstructed image measure which is called PSNR. Assume we are given a source image f(i,j) that contains N x N pixels and a reconstructed image F(i,j) where F is reconstructed by decoding the encoded version of f(i,j). Error metrics are computed on the luminance signal only so the pixel values f(i,j) range between black (0) and white (255).

First we compute the mean squared error (MSE) of the reconstructed image as follows

$$MSE = \frac{\sum[f(i,j) - F(i,j)]^2}{N^2}$$

The summation is over all pixels. The root mean squared error (RMSE) is the square root of MSE. Some formulations use N rather N^2 in the denominator for MSE.

PSNR in decibels (dB) is computed by using

$$PSNR = 10 \log_2 \frac{255}{MSE}$$

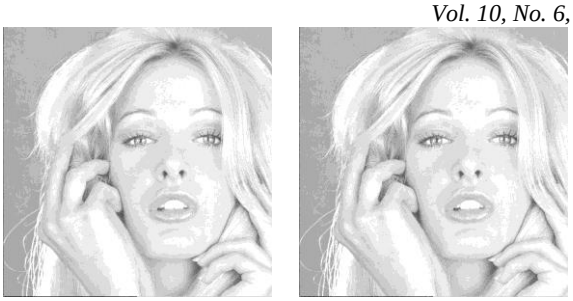
Typical PSNR values range between 20 and 40. The actual value is not meaningful, but the comparison between two values for different reconstructed images gives one measure of quality. The PSNR values of the twelve test images with the proposed method are calculated. These values are compared with the PSNR values with Pixel Value Differencing Method, Pixel Value Differencing with Modulus function method Triway Pixel Value Differencing method . The results have been shown in table 2.

From the these results it can be inferred that the proposed method produces stego-images with acceptable PSNR.

No reliable steganalytic technique has been proposed in the literature for PVD based methods. The RS steganalysis method is not effective on PVD based methods as that method was devised for LSB steganography[3].

The stego- images are shown in the figure 3.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500



PVDM method Proposed method

Figure 3 : Stego- images

VII. STEGANALYSIS

It has been already proved that Steganalysis methods such as RS-steganalysis cannot detect steganography using PVD with modulus function. No other methods are suitable to detect this technique.

VIII. CONCLUSION

It is proved by the experimental results that the proposed method offers high capacity than the Pixel Value Differencing method(PVD), Pixel Value Differencing with modulus function method(PVDM). PSNR values for the stego images obtained by the proposed method are well above the acceptable limit of 20-35. Thus it can be concluded that the proposed method is a method which offers high pay load with acceptable quality of Stego images.

REFERENCES

[1] Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom ,Jessica Fridrich and Ton Kalker, " Digital Watermarking and Steganography" 2nd Edition, Morgan Kaufmann Publishers, 2008.

[2] Huaiqing wang and shuozhong wang, "Cyber Warfare:Steganography vs. Steganalysis" communications of the ACM , Vol. 47, 2004, pp.76-82

[3] Chung-Ming Wang, Nan-I Wu, Chwei-Shyong Tsai, and Min-Shiang Hwang, "A high quality steganographic method with pixel-value differencing and modulus function" The Journal of Systems and Software, vol.81, 2008, pp.150–158

[4] Johnson, N. and Jajodia, S. "Exploring steganography: Seeing the unseen", IEEE Computers. Vol.31, 1998, pp.26–34.

[5] C.-K. Chan, and L.M. Cheng , "Hiding data in images by simple LSB substitution" Pattern Recognition, vol.37, 2004, pp. 469 – 474

[6] Fridrich, J., Goljan, M., Du, R., "Detecting LSB steganography in color and gray-scale images". Mag. IEEE Multimedia (Special Issue on Security) ,2001, pp. 22–28.

[7] C.C. Chang, J.Y. Hsiao, and C.S. Chan, "Finding optimal LSB substitution in image hiding by dynamic programming strategy", Pattern Recognition, vol.36, 2003, pp.1583–1595.

[8] R.Z. Wang, C.F. Lin, and J.C. Lin, "Image hiding by optimal LSB substitution and genetic algorithm", Pattern Recognition, vol. 34, 2001, pp.671–683.

[9] Da-Chun Wu, and Wen-Hsiang Tsai, "A steganographic method for images by pixel-value differencing" Pattern Recognition Letters vol. 24, 2003, pp.1613–1626.

[10] Chung-Ming Wang, Nan-I Wu, Chwei-Shyong Tsai, and Min-Shiang Hwang, "A high quality steganographic method with pixel-value differencing and modulus function", The Journal of Systems and Software, vol. 81,2008, pp.150–158

AUTHORS PROFILE

Dr. Sridevi Rangu obtained B.E (Computer Science and Engineering) from Madras University, chennai, and M.Tech (Computer Science and Technology) from Andhra University Visakapatnam in 1999 and 2003 respectively. She is having nearly 12 years of teaching experience. Since November,2006 she is working as an Associate professor in JNTU Hyderabad. She pursued Ph.D. from faculty of Computer Science and Engineering JNTU Hyderabad in December,2010. Area of research interest are Network security, Intrusion Detection and Computer Networks.
She is Guiding 6 Ph.D students in the area of network security and guided more than 25 M.tech students.Published 7 research papers in various Internal Journals and conferences. She achieved best Paper Award in ICSCI-2008, Pentagram Research Center ,Hyderabad ,India , 2008.

Mr. G. John Babu, has completed his masters degree in computer science from JNTUH Hyderabad, and currently doing research on Steganalysis. His research interests include Steganography, Steganalysis and watermarking.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Design of 16 bit low power processor

Khaja Mujeebuddin Quadry
Member IEEE,
Professor, Department of ECE
Royal Institute of Technology & Science,
Chevella, R. R. Dist. A. P. India
Email: mujeebqd@yahoo.com

Dr. Syed Abdul Sattar,
Professor & Head, Department of ECE
Royal Institute of Technology & Science,
Chevella, R. R. Dist. A. P. India
Email: syedabdulsattar1965@gmail.com

***Abstract*— This paper describes the design of low power 16 bit processor. The processor is designed to incorporate 25 basic instructions involving Arithmetic, Logical, Data transfer, Branching, Control instructions. It is expandable up to 32 instructions based on the user requirements To implement these instructions the design incorporates various design blocks like Control Logic Unit (CLU), Arithmetic Logic Unit (ALU), program Counter (PC), instruction register (IR), Memory , Clock, Generator, Register and Additional glue logic. The processor has been realized using Verilog HDL, functionality is verified by writing the test programs using XILINX 9i ISE. Power estimation is done using X power tool, synthesis is done for SPARTAN 2E, SPARTAN 3E, and VIRTEX 5 FPGA. Comparison of synthesis results for various FPGA technologies has been carried out. The simulations results depict that total dissipated power by the processor to be approximately varying from 25mW to 267mW with the maximum frequency of operation ranging 30.931MHz to 122.018MHz. The bit stream file generated is successfully generated loaded in to SPARTAN 3E FPGA and tested the results using chip scope pro tool.**

Keywords-16 bit processor; FPGA; lopower design; styling; insert

I. INTRODUCTION

The reduced instructions set computer (RISC) use simple instructions and have small instructions set compared to complex instruction set computer (CISC). It has become a mainstream movement to improve computing power and keep cost of design time low by using RISC processor. It is basically designed in order to achieve faster executions. The striking feature of RISC is that it executes instructions in short clock cycles [1]. Almost all instructions have simple register addressing. Due to the simplification of the instructions and their format control logic designed is very much simplified. As power has become an important aspect in the design of general purpose processors. Low power consumption helps to reduce the heat dissipation, lengthen battery life and increase device reliability [2]. The minimization of power dissipation is done at various levels of design process by applying various low power techniques.

II. DESIGN OF 16-BIT RISC CPU

The overall architecture of a RISC Processor consists of three functional units: a processor, a controller, and memory as shown in Figure 1 program instructions and data are stored in memory. Instructions are fetched synchronously from memory, decoded, and executed .The instruction register contains the instruction that is currently being executed; the program counter contains the address of the next instruction to be executed; and the address register holds the address of the memory location that will be addressed next by a read or write operation.

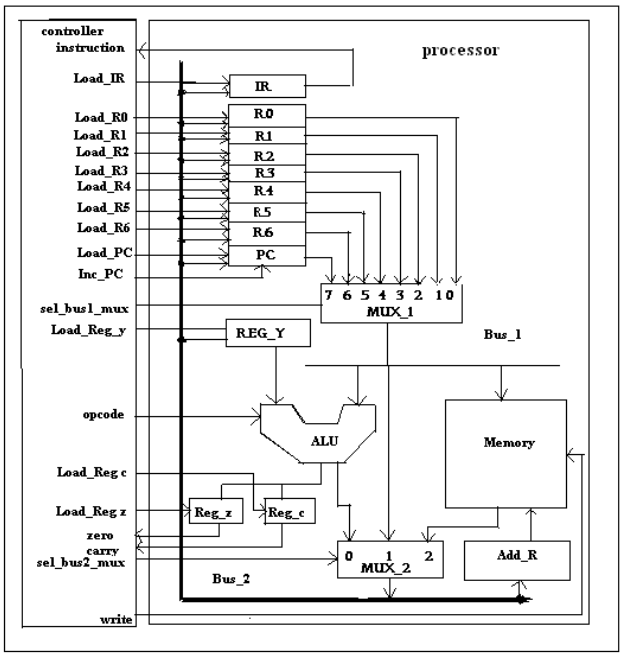


Figure 1. RISC Processor architecture

A. RISC Processor

The processor includes registers, data-paths, control lines, and an ALU capable of performing arithmetic and logic operations on its operands, subject to the op-code held in the

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

instruction register. A multiplexer Mux_1 determines the source of data that is bound for Bus_1, and Mux_2 determines the source of data bound for Bus_2, and loaded into the instruction register. A word of data can be fetched from memory, and steered to a general-purpose register or to the operand register (Reg_Y) prior to an operation of the ALU. The result of an ALU operation can be placed on Bus_2, loaded into a register, and subsequently transferred to memory. A dedicated registers (Reg_Z, Reg_c) holds the flags indicating zero and carry generated respectively after an ALU operation .

B. *RISC Controller*

The timing of all activity is determined by the controller. The controller steers the data to the proper destination, according to the instruction being executed. Thus, the design of the controller is strongly dependent on the specification of the machine's ALU and data path resources and the clocking scheme available. In this a single clock is used, and execution of an instruction is initiated on a single edge of the clock (i.e. the rising edge).The controller monitors the state of the processing unit and the instruction to be executed and determines the value of the control signals. The controller's input signals are the instruction word and the zero, carry flags from the ALU. The signals produced by the controller are identified as follows.

1) *Controller signals*

- *Load-Add-Reg* -Loads the address register,
- *Load-PC*- Loads Bus_2 to the program counter,
- *Load-IR*- Loads Bus_2 to the instruction register
- *Inc-PC*- Increments the program counter,
- *Set_Bus_1_Mux*-Selects among the Program-Counter, R0 to R6 to drive Bus_1,
- *Set_Bus_2_Mux*- Selects among ALU-out, Bus_1, and memory to drive Bus_2,
- *Load_R0* -Loads general-purpose register R0,
- *Load_R1*-Loads general-purpose register R1,
- *Load_R2*-Loads general-purpose register R2,
- *Load_R3*-Loads general-purpose register R3,
- *Load_R4* -Loads general-purpose register R4,
- *Load_R5*-Loads general-purpose register R5,
- *Load_R6*-Loads general-purpose register R6,
- *Load_Reg_Y*-Loads Bus_2 to the register Reg_Y,
- *Load_Reg_Z*-Loads the register Reg_Z,
- *Load_Reg_C* Loads the register Reg_C,
- *Write*-Loads Bus_1 into the SRAM memory at the location specified by the address register. The control unit produces the control signals to load registers, selects the path of data through the multiplexers, determines when data should be written to memory, and controls the three-state busses in the architecture.

C. *RISC Processor Instruction set*

The machine is controlled by a machine language program consisting of a set of instructions stored in memory. So in addition to depending on the machine's architecture, the design of the controller depends on the processor's instructions set (i.e., the instructions that can be executed by a program). A machine language program consists of a stored sequence of 16-bit words (2 bytes). The format of an instruction of RISC Processor can be long or short, depending on the operation.

opcode					source			Destination		
0	0	0	0	1	0	0	1	0	1	1

Figure 2. Instruction format Short Instruction

opcode					source			Destination		
0	0	1	0	0	0	1	0	?	?	?

Address									
0	0	1	0	0	1	0	1	0	0

Figure 3. Instruction format Long Instruction

Short instructions have the format shown in Figure 2. Each short instruction requires 2 bytes of memory. The word has a 5-bit op-code, a 3-bit source register address, and a 3-bit destination register address. A long instruction requires 4 bytes of memory. The first word of a long instruction contains a 5-bit op-code. The remaining 6 bits of the word can be used to specify address of a pair of source and destination registers, depending on the instruction. The second word contains the address of the memory word that holds an operand required by the instruction. Figure 3. shows the 4-byte format of a long instruction. The program counter holds the address of the next instruction to be executed. When the external reset is asserted, the program counter is loaded with 0, indicating that the bottom of memory holds the next instruction that will be fetched. Under the action of clock, for single-cycle instructions, the instruction at the address in the program

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

counter is loaded into the instruction register and the program counter is incremented. An instruction decoder determines the resulting action on the data paths and the ALU. A long instruction is held in 4 bytes, and an additional clock cycle is required to execute the instruction. In the second cycle of execution, the second byte is fetched from memory at the address held in the program counter, and then the instruction is completed. Intermediate contents of the ALU may be meaningless when two-cycle operations are being executed. The RISC Processor instruction set is summarized in TABLE I

TABLE I. INSTRUCTION SET TABLE

Instruction	Instruction Word			Action
	opcode	src	dest	
NOP	00000	??	??	None
ADD	00001	src	dest	dest <= src +dest
SUB	00010	src	dest	dest <= src -dest
AND	00011	src	dest	dest <= src &dest
NOT	00100	src	dest	dest <= ~src
RD	00101	??	dest	dest<= memory [Add_R]
WR	00110	src	??	memory [Add_R]<=src
JMP	00111	??	??	PC<= memory [Add_R]
JZ	01000	??	??	PC<= memory [Add_R]
OR	01001	src	dest	dest <= src | dest
XOR	01010	src	dest	dest <= src ^dest
INC	01011	src	dest	dest <= src+1
DEC	01100	src	dest	dest <= src-1
MUL	01101	src	dest	dest <= src *dest
SHL	01110	src	dest	dest <= src <<1
SHR	01111	src	dest	dest <= src>>1
ROL	10000	src	dest	dest<= rotate left src by 1 bit
ROR	10001	src	dest	dest<= rotate right src by 1 bit
ADC	10010	src	dest	dest <= src +dest+carry
SBC	10011	src	dest	dest <= src – dest - carry
RLC	10100	src	dest	dest<= rotate left src by 1 bit through carry
RRC	10101	src	dest	dest<= rotate right src by 1 bit through carry
IN	10110	src	dest	dest<= port[Add_R]
OUT	10111	src	dest	port[Add_R]<=src
HALT	11111	??	??	Halts execution until reset

III. RISC PROCESSOR CONTROLLER DESIGN

The machine's controller is designed as an FSM. Its states are specified, according to the architecture, instruction set, and clocking scheme used in the design. This is accomplished by identifying what steps must occur to execute each instruction. We have used an ASM chart to describe the activity within the Processor, and to present a clear picture of how the machine operates under the command of its instructions.

The machine has three phases of operation: fetch decode, and execute as shown in Figure4. Fetching retrieves an instruction from memory, decoding decodes the instruction, manipulates data paths, and loads registers; execution generates the results of the instruction. The fetch phase will require two clock cycles – one to load the address register and one to retrieve the addressed contents from memory. The decode phase is accomplished in one cycle.

The execution phase may require zero, one, or two more cycles, depending on the instruction. The NOT instruction can execute in the same cycle that the instruction is decoded; single-word instructions, such as ADD, take one cycle to execute, during which the results of the operation are loaded into the destination register. The source register can be loaded during the decode phase. The execution phase of 2 word instruction will take one cycle to load the address register with the second word, and one to retrieve the word from the memory location addressed by states listed below, with the control actions that must occur in each state.

A. Controller states

- S_idle: State entered after reset is asserted and no action takes place, The FETCH state is further divided in to two more states S_ fet1 and S_fet2.

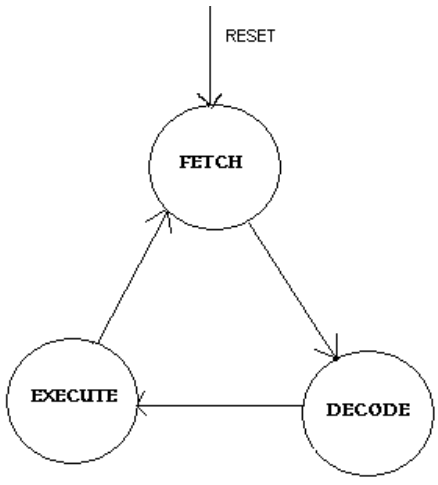


Figure 4. State machine of Controller

- S_ fet1:Load the address register with the contents of the program Counter. (PC is initialized to the starting address by the reset action). The state is entered at the

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

first active clock after reset is de-asserted, and is revisited after a NOP instruction is decoded.

- S_fet2: Load the instruction register with thw word addressed by the Address register, and increment the program counter to point To the next location in memory, in anticipation of the next Instruction or data fetch.
- S_dec: Decode the instruction register and assert signals to control Data paths and register transfers.

The Execute state is divided in to S_ex1, S_rd1, S_rd2, S_wr1, S_wr2, S_br1, S_br2, S_halt.

- S_ex1: Execute the ALU operation for a single-byte instruction, Conditionally assert the zero flag, carry flag and load the destination Register.
- S_rd1: Load the address register with the second byte of a RD instruction, and increment the PC.
- S_rd2: Load the destination register with the memory word addressed by the byte loaded in S_rd1.
- S_wr1: Load the address register with the second byte of a WR instruction, and increment the PC.
- S_wr2: Load the destination register with the memory word addressed by the byte loaded in S_wr1
- S_br1: Load the address the register with the second byte of a BR instruction and increment the PC.
- S_br2: Load the program the counter with the memory word addressed by the byte loaded in S_br1
- S_halt : default state to trap failure to decode a valid instruction.

The partitioned ASM chart for the controller of RISC Processor have been built, entire machine is described using verilog HDL, for the given architectural partition. This process has been done in stages. First, the functional units are declared according to the partition of the machine. Then their ports and variables are declared and checked for syntax. Then the individual units are described, debugged, and verified. The last step is to integrate the design and verify that it has correct functionality. The top level verilog HDL module RISC_Processor_16_bit integrates the modules of the architecture of Figure 1 and were presented first. Three modules are instantiated; processing-unit, control unit and Memory-unit, with instant names M0-processor, M1-Controller, and M2-Mem respectively. The parameters declared at this level of the hierarchy size the data paths between the structural/functional units. The verilog model of the machine processor is describe the architecture; register operations that are represented by the functional units shown in Figure 1 The processor instantiates several other modules which are also declared the simulation results can be seen in the Figure 5.

IV. RESULTS & CONCLUSION

The design of a 16-Bit non-pipelined RISC processor has been presented. The processor has been designed for executing the instruction set comprising of 25 instructions in total. It is shown that it can be expandable up to 32 instructions, based on the user requirements. A memory unit with 16 bit word size and 256 locations also designed and integrated with the processor to store the machine code of the program to be executed.

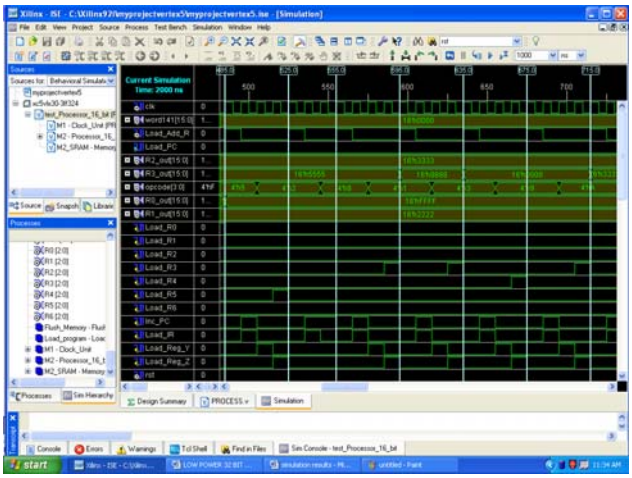


Figure 5. Simulation result

The RISC processor for embedded and portable application has been designed and verified. The low power techniques employed are reducing the supply voltage, clock gating, and resource sharing. Frequency of operation is also selected according to the timing report and power budget. Gray code is used for state encoding as it consumes less power compare to binary coding.

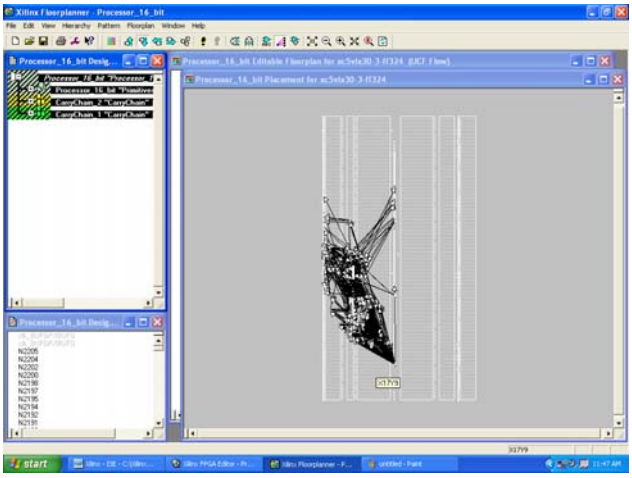


Figure 6. Floor plan for VIRTEX 5

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

The designed processor executing memory read, write, branch instructions in 5 clock cycles (fetch, decode, execute), arithmetic and logical instructions are executed in 3 to 4 clock cycles. Synthesis report for the target device xc5vlx30-3-ff324 (VIRTEX 5) shows that the design has 9 Levels of Logic with a delay of 8.196ns corresponds to a maximum frequency on operation 122.018MHz, and for a target device xc2s50e-6-ft256 (SPARTAN IIE) the delay is 32.330ns corresponds to Maximum Frequency: 30.931MHz.Post map static timing analysis is performed by assigning the user constraints and verified the timing constraints met. The floor plan of the design for VIRTEX 5 is shown in the Figure 6. Bit stream file is generated for SPARTAN 3E xc3s500e-5 device with FG320 package and successfully loaded and contents of the memory are verified using chipscope-pro after executing the application programs it is observed that the power saving is about 21% after applying the low power techniques.

ACKNOWLEDGMENT

.
I would like to thank Dr. K. Soundara Rajan, Professor Dept of ECE, JNTU Anantapur, A.P.India for the time to time discussions

REFERENCES

[1] M. Quigley, B. Gerkey, K. Conley, J. Faust, T. Foote, J. Leibs, E. Berger, R. Wheeler, and A. Ng, "Ros: an open-source robot operating system," in Proc. of the IEEE Intl. Conf. on Robotics and Automation (ICRA) Workshop on Open Source Robotics, (Kobe,Japan), May 2009.

[2] Nidhi Maheshwari, Pramod Kumar Jain, D.S. Ajnar "A 16-Bit Fully Functional Single Cycle Processor" Proc. International Journal of Engineering Science and Technology (IJEST) ISSN : 0975-5462 Vol. 3 No. 8 August 2011 p 6219-6226

[3] Samiappa Sakthikumaran, S. Salivahanan, V. S. Kanchana Bhaaskaran "16-Bit RISC Processor Design for Convolution Application" proceedings of IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011 978-1-4577-0590-8

[4] Youngjoon Shin, Chanho Lee, and Yong Moon, "A Low Power 16-Bit RISC Microprocessor Using ECRL Circuits", ETRI Journal, Volume 26, Number 6, December 2004.

[5] Yasuhiro Takahashi, Toshikazu Sekine, and Michio Yokoyama, "Design of a 16-bit Non-pipelined RISC CPU in a Two Phase Drive Adiabatic Dynamic CMOS Logic," International Journal of Computer and Electrical Engineering, Vol. 1, No. 1, April 2009 1793-8198.

AUTHORS PROFILE

Dr.Syed Abdul Sattar received M.Tech(DSCE) and PhD from JNTU Hyderbad India. He has published many papers in International/National journals. He is felleow of Institution of Electronics and Telecommunication Engineers India Life member of Indian society for Technical Education.

Khaja Mujeebuddin Quadry (Member IEEE), Received Diploma in Electronics and communication engineering from state board of Technical Education A.P India in 1993, BE Degree in Electroics and Communication Engineering from Osmania University in 1997, ME Degree in VLSI & Embedded system Design from Osmania University in 2007. He is a Life member of Institution of Electronics and Telecommunication Engineers India.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Integration Of Floating Point Arithmetic User Library To Resource Library Of The CAD Tool For Customization

R.Prakash Rao,
Associate professor,
St.Peter's Engineering College,
Maisammaguda,Hyderabad, India.
rachurivlsi@gmail.com.

Dr.B.K.Madhavi, Professor,
Geetanjali College of Engineering
& Technolog, Cheryala,
Hyderabad, India.
bkmadhavi2009@gmail.com.

***Abstract* - Towards the integration of analog and digital circuitry, various approaches have been emerged. To achieve better integrity, mixed-signal designs have recently attain the greater significance. In various real time applications such as RF Systems, Communication Systems, Networking Systems etc., mixed signal integrated circuits are emerging. Because the use of both digital system and analog system on a single platform, the approachability is quite complex. Where digital systems are complex with synchronization problem, design of analog circuitry is too typical. Due to various CAD tools usage, the bottleneck of integration is also challenging. Hence, here our aim is to develop a generic modeling of analog-digital mixed signal design tool for easy to handle and low complex in approach. Hence, here our work focused on integrating multiple features of required analog design parameters to the digitally defined CAD tool. It is also focused to have a user friendly tool with various optimizing possibilities for easy designing and testing purpose.**

Keywords-RF Systems; mixed signal designs; analog circuitry; integration; CAD tool; testing.

I. INTRODUCTION

In the past, designers have used a variety of simulation methodologies to verify designs that contained both analog and digital circuits. At the very highest levels of abstraction, system designers have used C/C++ and Matlab to model systems that would be implemented with analog and digital circuits; but this approach usually doesn't try to represent any implementation issues. At the next level down in the hierarchy, designers have used Saber by Analogy and similar tools to model mixed-signal systems. At the lowest level of abstraction, designers have modeled all the analog and digital circuits at the transistor level and used Spice-like simulators, or reduced-complexity transistor-level simulators.

Designers are just beginning to use the VHDL and Verilog AMS languages, and this approach fits somewhere in the middle compared to the above levels. The AMS extensions allow a designer to use VHDL or Verilog to describe analog circuits at different levels of abstraction, ranging from behavioral to structural. The AMS description is usually then translated to a netlist and simulated with a Spice-like simulator.

Another approach offered by major CAD companies is to provide a simulation environment that allows the user to choose from different levels of abstraction for a given simulation. Digital blocks are represented with an HDL and simulated with an HDL simulator, analog blocks are represented with transistors or an AMS HDL and simulated with a Spice-like simulator. A software backplane allows the HDL and Spice simulators to communicate via interprocess communication. Typically lower levels of abstraction translate to slower simulation time. Consequently, simulating large mixed-signal designs solely at the transistor level with a standard Spice-like simulator may not be practical. The benefits of Spice simulation tools are that they provide the most detailed level of modeling and analysis including: DC, transient, small signal AC, and zero's/pole's of filters . The costs of Spice simulation are often long simulation times and tedious design entry.

II. PROPOSED DESIGN

Traditionally, if a system consists of both analog and digital systems on the same platform called mixed-signal systems, neither the analog tools nor the digital tools will support mixed signal designs. These mixed signal designs are used most-widely in DSP systems for audio and video purposes. So, to simulate such mixed signal designs, presently the dedicated floating point arithmetic units are used in the CAD tools like XILINX new version ISE tool [10] with the latest target devices like Vertex, Kintex etc. These dedicated floating point arithmetic units need to buy from different vendors. But, here we are proposing that after the extensive study of the ModelSim tool flow, instead of buying the dedicated floating pint arithmetic units from different vendors , we have integrated the floating point arithmetic features to the ModelSim tool in

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

which earlier we would have simulated the fixed point numbers only. So that now the upgraded ModelSim tool can be used to perform the complete DSP operations[4] like video and audio.

Since, the analog signal is decomposed or reconstructed with the signal samples and those signal samples could be defined with floating point arithmetic[1] like 0.0,0.2,0.4,0.6,0.8,1.0 and 1.0,0.8,0.6,0.4,0.2,0.0, as a continuous wave signal shown in fig.1, these floating point features of analog signals had been added to the resource library of the CAD tool, hence, the particular tool will be upgraded with both the analog and digital features .

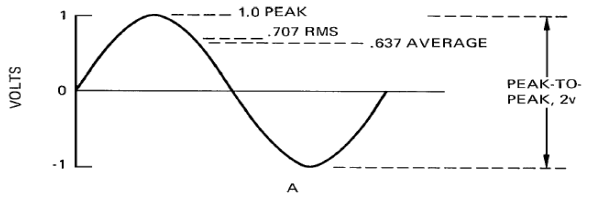


Fig1: Continuous wave signal

So, here we have designed the floating point adder, multiplier, deviser, square root functions and integrated to the ModelSim tool. In DSP, some algorithms like Lifting scheme algorithm or Daubechy's algorithm[6][9] will produce the floating point co-efficients while analyzing coder or decoder operations used for audio or video. Hence such systems could be designed using the upgraded ModelSim tool, hence it is more economical comparing with dedicated floating point arithmetic units.

III. Floating Point Arithmetic

There are several ways to represent real numbers on computers. Fixed point places a radix point somewhere in the middle of the digits, and is equivalent to using integers that represent portions of some unit. For example, one might represent 1/100ths of a unit; if you have four decimal digits, you could represent 10.82, or 00.01. Another approach is to use rational, and represent every number as the ratio of two integers; Floating-point representation - the most common solution - basically represents reals in scientific notation. Scientific notation represents numbers as a base number and an exponent.

For example, 123.456 could be represented as 1.23456×10^2. In hexadecimal, the number 123.abc might be represented as $1.23abc \times 16^2$. Floating-point solves a number of representation problems. Fixed-point has a fixed window of representation, which limits it from representing very large or very small numbers. Also, fixed-point is prone to a loss of precision when two large numbers are divided. Floating-point, on the other hand, employs a sort of "sliding window" of precision appropriate to the scale of the number. This allows it to represent numbers from 1,000,000,000,000 to 0.0000000000000001 with ease.

A. IEEE 754 Floating Point Standard

IEEE 754 floating point standard is the most common representation today for real numbers on computers. The IEEE (Institute of Electrical and Electronics Engineers) has produced a Standard to define floating-point representation and arithmetic. The standard brought out by the IEEE come to be known as IEEE 754[5]. The IEEE Standard for Binary Floating-Point Arithmetic (IEEE 754) is the most widely used standard for floating point computation, and is followed by many CPU and FPU implementations.[2]

The standard defines formats for representing floating-point numbers including negative numbers and denormal numbers special values i.e. infinities and NANs together with a set of floating-point operations that operate on these values. It also specifies four rounding modes which are round to zero, round to nearest, round to infinity and round to even and five exceptions including when the exceptions occur, and what happens when they do occur. Dealing with fixed-point arithmetic will limit the usability of a processor. If operations on numbers with fractions (e.g. 10.2445), very small numbers (e.g. 0.000004), or very large numbers (e.g. 42.243x105) are required, then a different one representation is in order is the floating-point arithmetic[4].

IV. Upgrading the CAD Tool

A. General

Since, ModelSim is the user friendly tool, in our work we have chosen ModelSim tool, and upgraded the features. ModelSim is a verification and simulation tool for VHDL, Verilog, SystemVerilog, SystemC, and mixed-language designs. Hence, here we are going to upgrade the ModelSim simulation environment[12].

B. Simulation flow in ModelSim

The below fig 4.1 shows the basic steps for simulating a design in ModelSim.

1. Creating the working library

In ModelSim, all designs are compiled into a library. We start a new simulation in ModelSim by creating a working library called "work". "Work" is the library name used by the compiler as the default destination for compiled design units.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

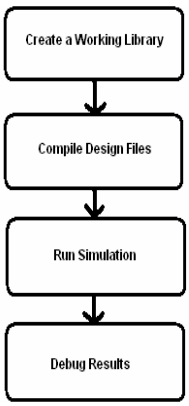


Figure 4.1: Basic Simulation Flow Diagram

2. Compiling the design

Before we simulate a design, we must first create a library and compile the source code into that library as given below.

i) Create a new directory and copy the design files for this lesson into it. Start by creating a new directory for this exercise.

ii) Start ModelSim if necessary.

- Use the ModelSim icon in Windows. Upon opening ModelSim for the first time, we will see the Welcome to ModelSim dialog. Click **Close**.
- Select **File > Change Directory** and change to the directory you created in step (i).

iii) Create the working library.

- Select **File > New > Library**.This opens a dialog where you specify physical and logical names for the library. We can create a new library or map to an existing library. We will be doing the former.
- Type **work** in the Library Name field if it is not entered automatically Click **OK**.

ModelSim creates a directory called *work* and writes a specially formatted file named *_info* into that directory. The *_info* file must remain in the directory to distinguish it as a ModelSim library. Do not edit the folder contents from your operating system; all changes should be made from within ModelSim. ModelSim also adds the library to the list in the Workspace and records the library mapping for future reference in the ModelSim initialization file (*modelsim.ini*). When you pressed OK in above step, several lines were printed to the Main window Transcript pane:

```
vlib work
vmap work work
# Copying C:\modeltech\win32/../modelsim.ini to modelsim.ini
# Modifying modelsim.ini
# ** Warning: Copied C:\modeltech\win32/../modelsim.ini to modelsim.ini.
# Updated modelsim.ini.
```

The first two lines are the command-line equivalent of the menu commands you invoked. Many menu-driven functions will echo their command-line equivalents in this fashion. The other lines notify you that the mapping has been recorded in a local ModelSim initialization file. After creating the working library, compile the design units into it. The ModelSim library format is compatible across all supported platforms. We can simulate your design on any platform without having to recompile your design. With the working library created, we are ready to compile your source files. We can compile by using the menus and dialogs of the graphic interface, as in the Verilog or VHDL.

V. DESIGN ALGORITHMS

a) Addition

We now present the basic description of the floating-point addition which gives a general idea of how it can be performed.

- If any of the input operand is a special value, the result is known before hand, thus all the computation can be bypassed.
- Mantissas are added or subtracted depending on the effective operation:
  $S = (mx \pm (my \times 2ey - ex) \times 2ex$ if ex _ ey,
  $((mx \times 2ex - ey) \pm my) \times 2ey$ if ex < ey.
- In order for the addition or subtraction to take place the binary point must be aligned. To achieve this, the mantissa of the smaller operand is multiplied by 2 difference of the exponents . This process is called alignment.
- The exponent of the result is the maximum of ex and ey; ez = max(ex, ey).
- If eop is addition, a carry-out can be generated and if eop is subtraction, cancellation might Occur. In each case normalization is required and consequently the exponent ez is updated.
- The exact result S is rounded to fit in the target precision. Sometimes rounding causes an overflow of the mantissa; a post-normalization is required.
- Determine exceptions by verifying the exponent of the result.

***b)** Multiplication*

We now present the basic description of floating-point multiplication[11]

- Verification of special values: if any of the input operandnis a special value, the result is known beforehand and thus no computation is required.
- Mantissas are multiplied to compute the product as $P = mx \times my$.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

- The exponent of the result is computed as ez = ex + ey − 127. In biased representation, the bias 127 (for single precision) has to be subtracted.
- The sign of the result is computed as sz = sx XOR sy.
- The product might be unnormalized. In this case, normalization is required and consequently the exponent ez is updated.
- The exact result P is rounded according to the specified mode to produce the mantissa of the result mz. In case of post-normalization, it is necessary to increment the result exponent as ez = ez + 1.
- Determine exceptions by verifying the exponent of the result. When overflow occurs, the result is ±1 and when underflow occurs, the result is zero or a subnormal number (if the gradual underflow is supported in the implementation).

c) *Division*

The basic description of floating-point division[3] can be given as follows:

- Mantissas are divided and the quotient Q = mx/my is computed.
- The intermediate result exponent is computed as ez = ex − ey + B.
- The sign of the result is computed as sz = sx XOR sy.
- If mx < my, normalization is required and consequently the result exponent is updated as ez = ez − 1.
- The exact quotient Q is rounded to fit in the target precision. In case of division, rounding never causes an overflow of the mantissa; thus post-normalization is not required.
- Exceptions are determined by verifying the exponent of the result.

d) *Square root*

The basic description of floating-point square root[3] can be given as follows.

- If the unbiased exponent ex − 127 is odd, a new mantissa is formed as mx, 2mx. This allows to have an integer result exponent.
- Obtain the square root as T =pmx.
- The intermediate result exponent is computed as ez = b(ex + B)/2c.
- The sign of the result is sz = 0. No normalization is required .
- Round T according to the rounding mode. A post-normalization step might be required. Neither underflow nor overflow can occur .

VI. RESULTS

a) Adder

The following snapshot shown in fig 6.1 had been taken from upgraded ModelSim after the timing simulation of the floating point Adder.

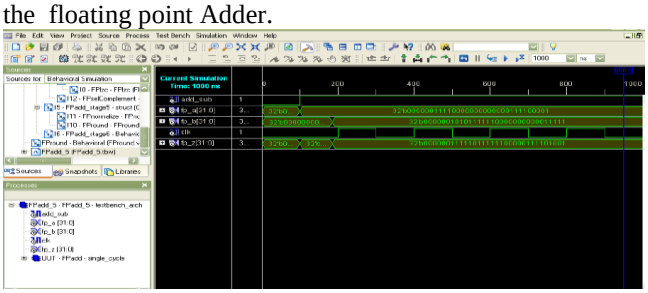


Figure 6.1: Output of Single Precision Floating Point Adder when above input's were given

b) Multiplier

The following snapshot shown in fig 6.2 had been taken from upgraded ModelSim after the timing simulation of the floating point multiplier.

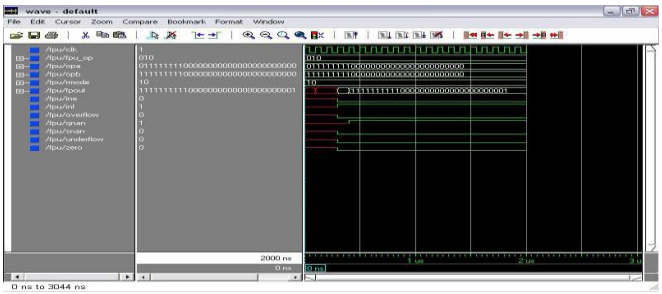


Figure 6.2: Output of Single Precision Floating Point Multiplier when above input's were given

c) Division

The following snapshot shown in fig 6.3 had been taken from upgraded ModelSim after the timing simulation of the floating point divisor.

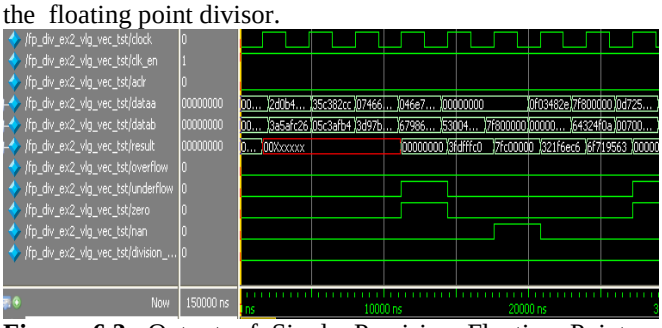


Figure 6.3: Output of Single Precision Floating Point divisor when above input's were given

d) Sqare Root

The following snapshot shown in fig 6.4 had been taken from upgraded ModelSim after the timing simulation of the floating point sqare root.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

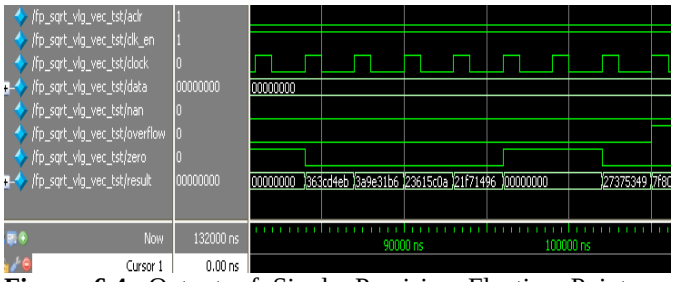


Figure 6.4: Output of Single Precision Floating Point square root when above input's were given.

VII. CONCLUSION

Here, we have added the analog features in the form of floating point notation, defined in the working library to the resource library of the CAD tool of ModelSim PE10.1b successfully. Using this novel tool, different arithmetic operations have been performed for addition, multiplication, division and square root on different floating point numbers. It has been used IEEE 754 standard based floating point representation. The design algorithms have been coded in VHDL[7]. As a case study, we have to take any of analog mixed signal DSP application[8], which could be modeled using the upgraded ModelSim PE 10.1b tool without using VHDL-AMS extensions. This type of modeling is called RMS(Rachuri Mixed Signal) Modeling. There are significant advantages using RMS modeling, primarily in the aspects of simulation speed and portability of models and cost.

REFERENCES

[1]. D. Goldberg, "What every computer scientist should know about floating-point arithmetic" pp. 5-48 in ACM Computing Surveys vol. 23-1 (1991).
[2]. Charles Farnum, "Compiler Support for Floating-Point Computation" Software Practices and Experience, pp. 701-9 vol. 18, July 1988.
[3]. M. Leeser, X. Wang, " Variable Precision Floating Point Division and Square Root", Department of Electrical and Computer Engineering Northeastern University.
[4]. Taek-Jun Kwon, Jeff Sondeen, Jeff Draper USC Information Sciences Institute Design Trade-Offs institute "Floating-Point Unit Implementation for Embedded and Processing-In-Memory Systems" 4676 Admiralty Way Marina del Rey, CA 90292 U.S.A.
[5]. IEEE computer society: IEEE Standard 754 for Binary Floating-Point Arithmetic, 1985.
[6]. Raguveer M.Rao, Ajit S. Bopatikar "Wavelet transforms introduction to theory and application, Addison-weswley, 2001.
[7]. J.Bhaskar,"AVHDL primer" Pearson education,2004.
[8] C. Burus, et al. Introduction to Wavelets and Wavelet Transformation A Primer. Prentice Hall, 1998.
[9] K. K. Parhi, VLSI Digital Signal Processing Systems, Design and Implementation, John Wiley & Sons, NY, 1999.
[10] System Generator for DSP *User Guide* UG640 (v4.1) April 24, 2012
[11] *Xilinx XAPP467 Using* Embedded Multipliers in Spartan-3 FPGAs – May 13,2003.
[12]Pedro Echeverrıa, Miguel Angel Sánchez, Marisa López-Vallejo, "Development of a Standard Single Floating-Point Library and its Encapsulation for Reuse" p99.pdf in DCIS2009.unizar.es/FILES/CR2.

Authors Profile

Mr.R. Prakash Rao, received his M.Tech degree from College of Engineering , Andhra University,Vizag,India and B.Tech degree from Siddardha College of Engineering, Nagarjuna University,Guntur,India. Presently he is working as HOD in St.Peter's Engineering College, Hyderabad. He published 08 papers in various National and International Journals and Conferences. He got best faculty award during 2009-2010 in ASTRA, Hyderabad. He has guided 02 M.Tech projects and about 25 B.Tech projects in various levels. His research interest includes VLSI,Microwave Engineering.

Dr. B.K. Madhavi, received Ph.D from JNTU, Hyderabad. She completed ME from BITS-PILANI in the specialization of Microelectronics. She published 24 research papers in various National and International Journals and Conferences. Presently she is guiding 10 PhD Students and guided several BTech and MTech Projects. She is also being reviewed research papers for IETE. She participated in several workshops, summer and winter schools, National, International conferences and also organized several National level workshops, student paper contests, and seminars etc. Her research interest includes Microelectronics (VLSI Design, Low Power VLSI, MixedSignal Processing), Wireless communications.

V-Diagnostic: A Data Mining System For Human Immuno- Deficiency Virus Diagnosis

Omowunmi O. Adeyemo[1] **Adenike O. Osofisan**

Department of Computer Science
University of Ibadan
Ibadan, Nigeria
[1] Correspondence Author: wumiglory@yahoo.com

Abstract— A very serious health problem and life threatening diseases that has taken over the world medical scene from early 80s up to the present is Acquired Immune Deficiency Syndrome(AIDS), which is a result of Human Immuno-Deficiency Virus (HIV) in the body system. The World Health Organization through the support of United Nations advocates avoidance of unsafe sex, use of unsterilized sharp object and regular tests to ascertain ones HIV status. The campaign on HIV/AIDS is not effective especially on issues that relate to diagnosing of HIV at the early stage, it is most threatened because of discrimination against people living with the virus and lack of testing and counselling centre, most especially in rural areas of developing countries like Nigeria. Therefore, this paper focuses on the development of a Neural Network Based Data Mining System that could learn from historical data containing symptoms, mode of transmissions, region and status of patient which is used to predict or diagnose a patient HIV status. The system offers a very simple interactive platform for all any type of users providing self-diagnosis against this life threatening and deadly virus.

Keywords- Data Mining; Back Propagation Neural Network, Medical; AIDS; Symptoms and HIV

I. INTRODUCTION

The Human Immunodeficiency Virus (HIV) is a pathogen that results in Acquired Immunodeficiency Syndrome (AIDS). It has been the most significant emerging infectious agent of the last century and threatens to continue to create health, social and developmental problems in the millennium. The virus is indeed a great challenge to science and mankind. HIV and AIDS is very harmful to man and therefore reduces the life expectancy. Current data from sentinel surveillance sites throughout the countries shows that the virus is still spreading; both men and women are affected especially young and middle age and that infection occurs at youthful age and usually through heterosexual contact. The mode of transmission has posed enormous challenge to researches. It is known that the virus can pass from one person to another through different means. People are told to undergo HIV test to know if they have the disease, but unfortunately some are even dead if before the result is out, because most of the patient does not go for test on time and they may even have the type of HIV that does not reflect on time and sometimes the medical procedure may be tasky. HIV/AIDS has high rate of spreading in sub Saharan African countries, especially Nigeria. It has affected Nigeria both socially and economically. The HIV results in the destruction of the body's immune system rendering it unable to fight off opportunistic infections and therefore resulting in AIDS.

The aim of this study is to develop a system that can be used to know the HIV status of a patient. This will serve as another alternative to assist the doctors for quick intervention in taking care of the infected patient, and this will in turn reduced the spread of HIV disease. The model can be deployed to different Local, State, federal, Teaching Hospitals, non-governmental organization, and even health centres to allow massive diagnosis of patient status. This will help to determine the existence or non existence of the virus in a person and it can immediately assist the government in their preventive policy because it will now be easier to know and monitor the trend of the spread because there will be availability of the model at anytime. The model will be able to keep the status of each patient after diagnosis which can help the government at any time to know the trend of the spread in each location in Nigeria. This will help to project resources to the appropriate places by determining the status of each patient instead of waiting for the laboratory test that might be delayed until the immune system is totally destroyed. The model is expected to reduce the death rate and increase the life expectancy of Nigerians.

1. DATA MINING

Many authors have offered different classifications of the processes that are collectively known as data mining. The most appropriate of these definitions seems to be the one that identifies two classes of data mining processes. These are descriptive and predictive data mining [5]. It has been suggested that descriptive data mining essentially is a subset of predictive data mining. That is, in order to perform predictive data mining successfully, one most probably will have to perform a descriptive data mining first and then use the information and the results of this

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

process to complete the predictive data mining. Descriptive and predictive data mining share several common processes. Descriptive data mining is very useful for getting an initial understanding of the presented data. It is an exploratory process and attempts to discover patterns and relationships between different features present in the database [5].

Predictive data mining is a super set that should include descriptive data mining as part of its processes. During the predictive data mining, the descriptive data mining processes are used as a prelude to development of a predictive model. The predictive model can then be used in order to answer questions and assist the data miner in identifying trends in the data. What is most interesting about predictive data mining that distinguishes it from the descriptive data mining is that it can identify the type of patterns that might not yet exist in the dataset but has the potential of developing. Unlike the descriptive data mining that is an unsupervised process, predictive data mining is a supervised process. Predictive data mining not only discovers the present patterns and information in the data it also attempts to solve problems. Through the existence of modelling processes in the analysis the predictive data mining can answer questions that cannot be answered by other techniques. Tools that are used in the predictive data mining process include decision trees, neural networks, genetic algorithms and fuzzy systems. In the oil and gas industry, there are many field related operations that can benefit from the tools and capabilities that data mining has to offer [5].

The process of data mining consists of three stages:
a. Initial exploration
b. Model building or pattern identification with validation/verification.
c. Deployment, which is the application of the model to new data in order to generate predictions.

The exploration stage usually starts with data preparation that may involve cleaning data, data transformations, selecting subsets of records and in case of data sets with large numbers of variables ("fields") the performing of some preliminary feature selection operations to bring the number of variables to a manageable range depending on the statistical methods, which are being considered. Depending on the nature of the analytic problem, this first stage of the process of data mining may just be a simple choice of straightforward predictors for a regression model or to elaborate exploratory data analyses using a wide variety of graphical and statistical methods in order to identify the most relevant variables and determine the complexity and/or the general nature of models that can be taken into account in the next stage. The model building and validation stage involves considering various models and choosing the best one based on their predictive performance that is explaining the variability in question and producing stable results across samples. This is actually a very elaborate process and there is a variety of techniques developed to achieve this goal. Many of them are based on the so-called "competitive evaluation of models," that is, applying different models to the same data set and then comparing their performance to choose the best. The Deployment stage involves using the model selected as being the best in the previous stage and applying it to new data in order to generate predictions or estimates of the expected outcome.

2. RELATED WORKS

Betechuoh et al. [1] compared computational intelligence methods to analyze HIV in order to investigate which network is best suited for HIV classification. The methods analyzed are autoencoder multi-layer perceptron (MLP), autoencoder radial basis functions (RBF), support vector machines (SVM) and neuro-fuzzy models (NFM). The autoencoder multi-layer perceptron yields the highest accuracy of 92% amongst all the models studied. The autoencoder radial basis function model has the shortest computational time but yields one of the lowest accuracies of 82%. The SVM model yields the worst accuracy of 80%, as well as the worst computational time of 203s. The NFM yields an accuracy of 86%, which is the second highest accuracy. The NFM, however, offers rules, which gives interpretation of the data. The area under the receiver operating characteristics curve for the MLP model is 0.86 compared to an area under the curve of 0.87 for the RBF model, and 0.82 for the neuro- fuzzy model. The autoencoder MLP network model for HIV classification is thus found to outperform the other network models and is a much better classifier.

Betechuoh et al. [2] in their paper introduced a new method to analyse HIV using a combination of autoencoder networks and genetic algorithms. The proposed method is tested on a set of demographic properties of individuals obtained from the South African antenatal survey. When compared to conventional feed-forward neural networks, the autoencoder network classifier model proposed yields an accuracy of 92%, compared to an accuracy of 84% obtained from the conventional feed-forward neural network models. The area under the ROC curve for the proposed autoencoder network model is 0.86 compared to an area under the curve of 0.8 for the conventional feedforward neural network model. The autoencoder network model for HIV classification, proposed in this paper, thus outperforms the conventional feed-forward neural network models and is a much better classifier.

According to Chaturvedi [4], the Human Immunodeficiency Virus / Acquired Immunodeficiency syndrome (HIV/AIDS) is spreading rapidly in all regions of the world. But in India it is only 20 years old. Within this short period it has emerged as one of the most serious public health problems in the country, which greatly affect the socio-economical growth. The HIV problem is very complex and ill defined from the modelling point of view. Keeping in the view the complexities of the HIV infection and its transmission, it is difficult to make exact estimates of HIV prevalence. It is more so in the Indian context, with its typical and varied cultural characteristics, and

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

its traditions and values with special reference to sex related risk behaviours. Therefore, he developed a good model which will help in making exact estimates of HIV prevalence that may be used for planning HIV / AIDS prevention and control programs. In this paper Neuro-Fuzzy approach was used to develop dynamic model of HIV population of Agra region and the output generated was reliable..

In Sardari [6], a brief history of ANN and the basic concepts behind the computing, the mathematical and algorithmic formulation of each of the techniques, and their developmental background is presented. Based on the abilities of ANNs in pattern recognition and estimation of system outputs from the known inputs, the neural network can be considered as a tool for molecular data analysis and interpretation. Analysis by neural networks improves the classification accuracy, data quantification and reduces the number of analogues necessary for correct classification of biologically active compounds. Conformational analysis and quantifying the components in mixtures using NMR spectra, aqueous solubility prediction and structure-activity correlation are among the reported applications of ANN as a new modelling method. Ranging from drug design and discovery to structure and dosage form design, the potential pharmaceutical applications of the ANN methodology are significant. In the areas of clinical monitoring, utilization of molecular simulation and design of bioactive structures, ANN would make the study of the status of the health and disease possible and brings their predicted chemotherapeutic response closer to reality.

Studies were also carried out on the management of HIV/AIDS Management in communities [3, 7]. Charles *et al.* [3] focused on dimensional modelling of HIV patient information using open source modelling tools. It aims to take advantage of the fact that the most affected regions by the HIV virus are also heavily resource constrained (sub-Saharan Africa) whereas having large quantities of HIV data. Two HIV data source systems were studied to identify appropriate dimensions and facts these were then modelled using two open source dimensional modelling tools. Use of open source would reduce the software costs for dimensional modelling and in turn make data warehousing and data mining more feasible even for those in resource constrained settings but with data available.

3. METHODOLOGY

3.1 Data Collection

Data was collected from repositories of HIV inpatients and outpatient in one of the Nigerian hospital. The data set consist of input factors or variables and an output variable. The input factors or variables represent the symptoms that influence the presence of HIV/AIDS in a person. The input used are: Loss of appetite, Weight loss, Night sweat, Lymphoma, Recurrent pneumonia, frequent fever, Skin rash, joint pain & stiffness, Infections, Memory loss. The output is the HIV/AIDS status of the person.

3.2 Pre-processing

The dataset was cleaned, formatted and normalized before it was organized into a database. Microsoft SQL Server was used to construct the database with entity such as patient, symptoms and patient status. Twelve thousand exemplars were used for training the system.

3.3 Data Processing

At this stage supervised learning predictive data mining was employed. A back propagation neural network with one hidden layer was in developing the system. A thousand epoch was set for the system. An Artificial Neural Network (ANN) is a class of very powerful, general-purpose tools that may be applied to prediction, classification and clustering for decision making purpose. ANN has been developed as generalizations of mathematical models of biological nervous systems. A first wave of interest in neural networks (also known as connectionist models or parallel distributed processing) emerged after the introduction of simplified neurons by. The basic processing elements of neural networks are called artificial neurons, or simply neurons or nodes. In a simplified mathematical model of the neuron, the effects of the synapses are represented by connection weights that modulate the effect of the associated input signals, and the nonlinear characteristic exhibited by neurons is represented by a transfer function. The neuron impulse is then computed as the weighted sum of the input signals, transformed by the transfer function. The learning capability of an artificial neuron is achieved by adjusting the weights in accordance to the chosen learning algorithm. The basic architecture consists of three types of neuron layers: input, hidden, and output layers. In feed-forward networks, the signal flow is from input to output units, strictly in a feed-forward direction. The data processing can extend over multiple (layers of) units, but no feedback connections are present. Recurrent networks contain feedback connections. Contrary to feed-forward networks, the dynamical properties of the network are important. In some cases, the activation values of the units undergo a relaxation process such that the network will evolve to a stable state in which these activations do not change anymore. A neural network has to be configured such that the application of a set of inputs produces the desired set of outputs. Various methods to set the strengths of the connections exist. One way is to set the weights explicitly, using a priori knowledge. Another way is to train the neural network by feeding it teaching patterns and letting it change its weights according to some learning rule. In figure 1, a feed forward neural network is presented having four input layers, five hidden layers and one output.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

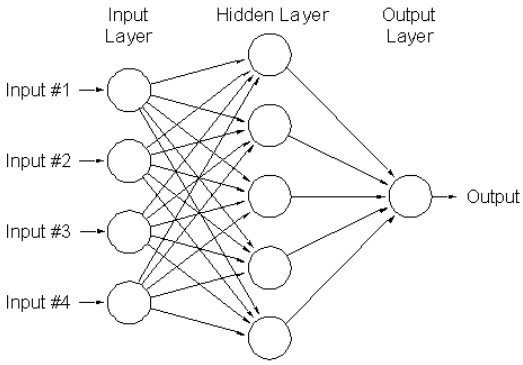


Figure 1: A Feed-Forward Neural Network

4. V-Diagnostic Tool

The system is a Data Mining System for Human Immuno-Deficiency Virus Diagnosis. The system user interface has three menus: 1. Patient 2. Operation; and 3. Statistics. At the Patient side as presented in figure 4, symptoms for each patient can be selected and prediction performed. In the operation menu as presented in figure 3, data can be generated to train the ANN system. This data can thereafter be used for training the data and even cross–validated. The third menu contains components that can be used to monitor statistics and prevalence of HIV. It has a module that records each prediction made as well as location of patients.

In this predictive system, the neural network was used to create and train a MLP neural network architecture. The network implemented consisted of an input layer, representing different inputs symptoms of individuals, mapped to an output layer representing the HIV status of individuals via the hidden layer. The network thus mapped the input of individuals to the HIV status. An error, however, exists between the individual's predicted HIV status (output vector) and the individual's actual HIV status (target vector) during training, which can be expressed as the difference between the target and output vector. The output of prediction reports either "The result of this system has shown that you are HIV negative" or "result of this system has shown that you are not HIV negative." The latter means the person has the HIV while the former means the person does not have HIV.

Figure 2: V-Diagnostic System

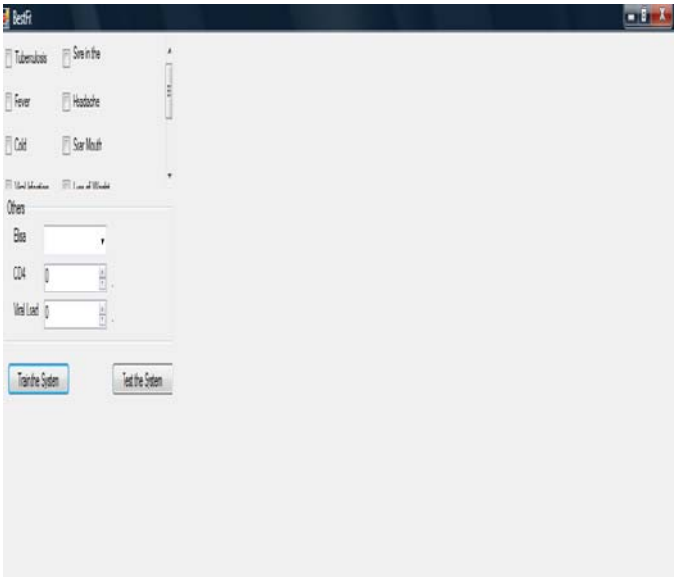


Figure 3: Training of Neural Network

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Figure 4: Diagnosis of HIV using Neural Network

5. Conclusion

In this work, an artificial neural network was used to diagnose patient of their HIV status. The data used for training was obtained from some the hospitals across Nigeria.The neural network generated reliable predicted output as a result of series of test carried out and the accuracy of prediction. The system cannot only be used to determine patient HIV status, but can also be used to monitor HIV prevalence. Based on the system output, back propagation feed forward neural networks forms a good system that can be used to diagnose HIV. In future research, we are working on feature selection and optimization of the solution.

REFERENCES

[1] Betechuoh, B.L. Marwala T. And Manana, J.V. (2008). Computational Intelligence for HIV Modelling. International Conference on Intelligent Engineering Systems INES 2008 on page(s): 127 – 132

[2] Betechuoh B.L., Marwala T. and Tettey T. (2006). Autoencoder networks for HIV classification, current science, Vol. 91, No. 11, 10 December 2006.

[3] Charles D. Otine, Samuel B. Kucel, Lena Trojer. (2010). Dimensional Modeling of HIV Data Using Open Source. World Academy of Science, Engineering and Technology (63)2010.

[4] Chaturvedi D.K. (2005). Dynamic Model of HIV/AIDS Population of Agra Region. September 2005

[5] Mohaghegh, S., (2003), Essential Components of an Integrated Data Mining Tool for the Oil and Gas Industry, With an Example Application in the DJ Basin. Paper SPE 84441, Proceedings, 2003 SPE Annual Conference and Exhibition, October 4-October 8, Denver, Colorado.

[6] Sardari S, Sardari D. (2002). Applications of artificial neural network in AIDS research and therapy. Curr Pharm Des., 8(8):659-70.

[7] Vararuk A., Petrounias L. and Kodogiannis V. (2007). Data mining techniques for HIV/AIDS data management in Thailand.Journal of Enterprise Information Management , Volume 21 (1).

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

A WEB-BASED SYSTEM TO ENHANCE THE MANAGEMENT OF ACQUIRED IMMUNODEFICIENCY SYNDROME (AIDS)/ HUMAN IMMUNODEFICIENCY VIRUS (HIV) IN NIGERIA

BY

Agbelusi Olutola
Department of Computer Science,
Rufus Giwa Polytechnic,
Owo, Nigeria.
tola52001@yahoo.com

Aladesote O. Isaiah,
Department of Computer Science,
Rufus Giwa Polytechnic,
Owo, Nigeria.
lomjovic@yahoo.com

Makinde O. E.
Department of Computer Science,
Ajayi Crowther University,
Oyo, Nigeria
Oludayo_makinde@yahoo.com

Aliu A. Hassan
Department of Mathematics & Statistics,
Rufus Giwa Polytechnic,
Owo, Nigeria.
ahaliu@ymail.com

ABSTRACT: *Acquired Immunodeficiency Syndrome (AIDS), a global disease, caused by the Human Immunodeficiency Virus (HIV) is arguably the greatest health problem of this age and there is need to make first class information on the management of HIV/AIDS available through the use of Web-Based Technology. This paper examined the various ways of contacting HIV and the effort made by Information and Technology to make life easier for people living with the virus in Nigeria. Questionnaires were distributed to Doctors and people living with HIV/AIDS to access their knowledge and belief about the said disease. MySQL was used to generate the database, to store all the vital information about the patients, their Doctors and their complaints.*
PHP programming for the implementation of the interfaces, Dreamweaver HTML for the design of the web-based application, T-test and Microsoft Excel were used for the analysis of data collected. The study looked into the occupation, age range and the marital status of different categories of people living with the virus. It was discovered that there were quite large numbers of people who are living with the virus.

Keywords: HIV; t-test; database; Web-based technology; Serodicordant couple; Antiretroviral Therapy (ART); MySQL; PHP; HTML.

INTRODUCTION

Acquired Immunodeficiency Syndrome (AIDS), a global disease, caused by the Human Immunodeficiency Virus (HIV) is arguably the greatest health problem of this age, since the first case was diagnosed in the USA in 1981, the disease has spread dramatically with cases reported worldwide [4] . Situations with HIV/AIDs have made it imperative for countries like Nigeria to evolve and strengthen strategies for care and support of people living with the disease. The development of Antiretroviral Therapy (ART) cast a big ray of hope in clinical management

of HIV/AIDS. ART does not really cure the disease but when used in proper combination, can reduce the replication of the virus and enhanced restoration of immune system in the infected individual. The optimal combination of ART which is known as HAART (Highly Active Antiretroviral therapy) has significantly reduced the mortality in people living with the virus. The beneficial attributes of HAART have encouraged several developed and developing countries to adopt its use [4].

In Nigeria, the first two cases of HIV/AIDS were identified in 1985 and were reported at an international HIV/AIDS conference in 1986. In 1987, the Nigerian health sector established the National Aids Advisory Committee which was shortly followed by the establishment of the National Expert Advisory Committee on AIDS (NEACA) [8].

The three main transmission routes for HIV in Nigeria include:

* Heterosexual sex: Approximately 80-95 percent of HIV infections in Nigeria are as a result of heterosexual sex. Factors contributing to this include: a lack of information about sexual health and HIV, low level of condom use, and high level of sexually transmitted diseases. Women are mostly affected by HIV. In 2009, women accounted for 56 percent of all aged 15 and above living with the virus.
* Blood transfusions: HIV transmission through unsafe blood, account for the second largest source of HIV infection in Nigeria. Not all hospitals in Nigeria have the technology to effectively screen blood, and therefore there is a risk of using contaminated blood. The Nigerian Federal Ministry of Health has responded by backing legislation that requires hospitals to only use blood from National Blood Transfusion Service, which has far more advanced blood-screening technology.
* Mother-to-child transmission. Each year about 57,000 babies are born with HIV. It is estimated that 220,000 children are living with HIV in Nigeria, most of who became infected from their mothers. (Weekly news digest by Global advocacy for HIV in Nigeria (2010)).

PROBLEM DEFINITION

One of the recently debated issues has been the extent of HIV/AIDS epidemic in Nigeria [3].Despite the fact that some scientists have made effort to manage AIDS with HAART (HAART – Highly Active Antiretroviral therapy), some infected individuals still succumb to death due to reasons such as: ignorance, lack of information on how to get access to HIV/AIDS treatment and care, lack of power and control for women, lack of

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

proper information on nutrition and exercise, discrimination and rejection from the general society and lack of courage to go for counseling.

The need to work on the above listed problems is necessary and important for any nation to control the number of people infected with HIV/AIDS and help those already living with the virus to live a longer possible life.

The improvement in life expectancy brings scrutiny on issues of long term drug toxicity. High among those concerns is the possibility of progressive Neuro cognitive damage associated with HIV, ART effectively reduces HIV RNA in cerebrospinal fluid, as well as in plasma; however, the effect in intrathecal immuno activation is less well studied.

Another concern regarding the increasing numbers of individuals receiving ART is the possibility of transmission of drug resistant variance. Drug resistant viruses may decline to a level undetectable by conventional sequencing (minority resistance variant). The field has now focused on the best approach to identify minority variant and whether their detection is important for both variant and patient management.

A proposed web-based user interface for the management of HIV/AIDS is designed to solve the above stated problem. This system is expected to provide the following solutions: adequate and first hand information about HIV/AIDS (i.e causes, treatments, preventions, mode of transmission, latest news on the virus etc), an interface where a patient can communicate with the doctor, latest health news and medication request details.

REVIEW OF RELATED WORKS

Antiretroviral drugs can have toxic side effects, however, there is no evidence that anti-HIV drugs cause the severe immune deficiency typical of AIDS. There are abundant evidences that currently recommended that causes of antiretroviral therapy can improve the length and quality of life of HIV positive people.

Trinidad and Tobago has recently been taking steps to combat HIV/AIDS. A national consultation has resulted in a five year National HIV/AIDS strategic plan. This recognizes that HIV/AIDS is a development issues and seeks a holistic, expanded and coordinated response.

An HIV prevention program for Africa-America women was to test the efficacy of a sexual risk reduction intervention to enhanced safer sex practices and reduces sexually transmitted infections (Chlamydia, gonorrhea and trichomonas) among African-American HIV serodicordant couples. The 8-session HIV prevention program focuses on enhancing cultural/ethnic pride, HIV transmission risk-reduction knowledge, couples sexual communication skill, male and female condom use self- efficacy and relationship satisfaction. Couples are observed for 1-year to assess changes in risk behaviors, psychosocial

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

mediators and sexually transmitted infections 1-year after the HIV prevention program.

[1] investigate the management of HIV through the use of data mining techniques, patterns in HIV/AIDS patient data. These patterns can be used for better management of the disease and more appropriate targeting of resources.

[10] used the advanced statistical techniques and the development of additional technologies for assessing the biological aspect. The nervous system-immune system relationship should enable PNI (psycho neuro immunology) to evolve. In turn, this will enable clinicians to better assess their patients' needs and treat their diseases.

Laurie and his colleague used quantitative research techniques to build a capacity of Kenyan institution to carry out HIV/AIDS prevention and control activities by strengthening and institutionalizing IEC (Information, Education and Communication) media and materials development skill among the programme staff of Kango.

[6] uses Multi Layer Backward Neural Network Model (MLFB) by back propagation algorithm to describe the regimens specification for the HIV/AIDS patients, based on the patients' unique factors like age, weight, HB, CD4 AND CD8.

[5] examined both HIV-positive and HIV-negative subjects who were either heavy drinkers or light drinkers. Her study assessed the levels of two molecules called PCR and ATP, which reflect the cell's energy metabolism as well as of a group of compounds called PDE, which represent breakdown products of molecules found in the cell membranes. Her study found that chronic consumption was associated with lower concentrations of PDE, PCR and ATP in white matter of the region surrounding the ventricles.

Eileen and her colleagues worked in the respond to diagnostic and therapeutic advances to improve standardization and comparability of surveillance data regarding persons at all stages of HIV disease.

THE WEB-BASED SYSTEM

Web-based system technically refers to those applications or services that are resident on a server that is therefore accessible from anywhere in the world via the web. As a matter of fact, it provides a very good interface to enable easy interaction between the system and the user. The system provides features that are specifically designed to enhance the management of people living with the virus and also provide adequate information that will bring about reduction in the spread of the virus. When the website is uploaded; the home page is the first page that will come up where the user signs in by supplying username and password.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

RESEARCH METHODOLOGY

The study was carried out at the Federal Medical Centre, Owo in Ondo State. An extensive literature review on the management of HIV was carried out. The collection of data used is through the administration of structured questionnaire by the Doctors and the HIV/AIDS patients, basically to access the knowledge and belief about the virus. The following tools were used during the course of this research work: MySQL, to generate the database used to store all the vital information about the patients, their Doctors and their complaints, PHP programming was used for the implementation of the interfaces, Dreamweaver HTML; for the design of the web-based application and t- test was used to carry out the comparison analysis test between the respondents of HIV positive and negative respond through the use of SPSS 17 for the analysis of data collected and the Microsoft Excel was adopted to depict the data presentation of the data collected.

ANALYSIS OF THE QUESTIONAIRE

Two structured questionnaires were used to gather information from each of the factors concerned during the course of this research work, one for the Doctors and the second one is for the people living with the virus. Ms-Excel was used for the analysis of the data collected.

Fig 1.1

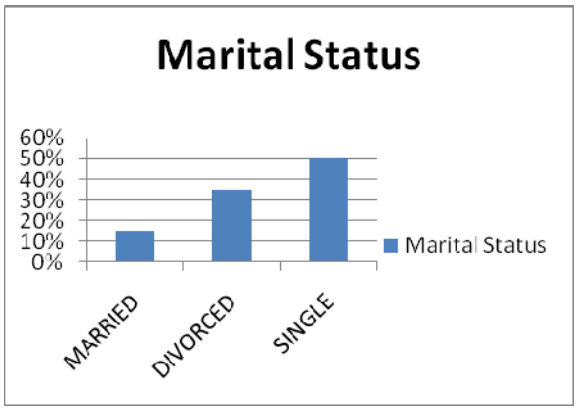


Fig 1.2

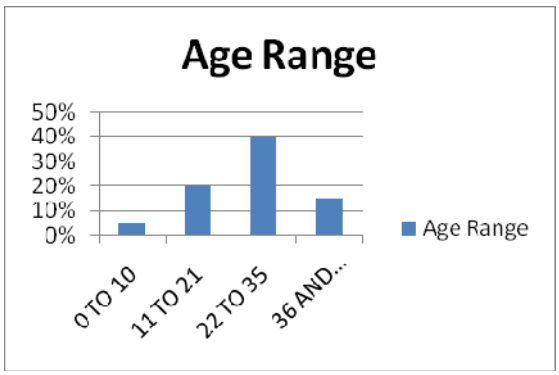
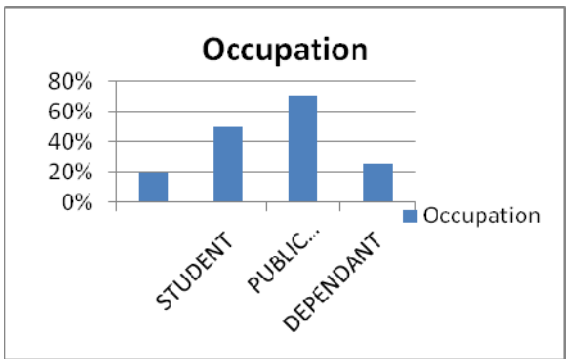


Fig 1.3



http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Table (i)

Paired Samples Statistics

		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	HIV Positive	21.47	15	11.532	2.977
	HIV Negative	17.00	15	12.689	3.276

Table (ii)

Paired Samples Test

		Paired Differences					t	Df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference Lower	Upper			
Pair 1	HIV Positive - HIV Negative	4.467	23.625	6.100	-8.616	17.550	0.732	14	0.476

Having observed from the paired-wise samples test result obtained from the table (i) & (ii) above, the average values with the variability's (standard deviation value) are (21.47, 11.532) and (17.00, 12.689) for HIV positive and negative respectively and the t-value (0.732) obtained is not significant at 0.476 test significant value. The output result shows that there is no different in standard of living in the response of the respondent concerning HIV positive and negative that undergoes treatment in the hospital.

RESULTS AND DISCUSSIONS

Figure 1.1 shows the marital status of people living with HIV/AIDS. The chart analysis shows that 35% are divorced men and women, 50% are single and 15% are married among those that are living with the virus.

Figure 1.2 shows the age range of people living with the virus. The chart shows that between the ages of 0-10 is 5%, ages 21-31 is 20%, ages 22-35 is 50% and 36 and above is 25%.

Figure 1.3 presents occupation of HIV/AIDS patients. 15% belong to people in private services, 40% are students, 30% are public servants and 15% are dependant.

Table (i) and (ii) output results show that there is no significant in the response of the respondent concerning HIV positive and negative in term of living condition with the treatment undergoes in the hospital.

The different categories of analysis discussed above shows that there is a need for quick and urgent intervention of Information and Communication Technology to make first class information and awareness about HIV/AIDS available to all the people living with the said virus through the use of Web-based technology. This will go a long way in managing people living with HIV/AIDS and as well as bringing about reduction in the spread of the disease.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

REFERENCES

[1] A. Vararuk, I. Petrounias, V. Kodogiannis, v. "Data Mining Techniques for HIV/AIDs Data Management in Thailand", Journal of Enterprise Information Management. Vol. 21, Iss:1, pp. 52 – 70, October 2009.

[2] Aids control and prevention (AIDSCAP) project, final report for the AIDSCAP program in Kenya. Arlington, VA: family health international. 1997.

[3] B. Laurie, "Surveillance case definitions for HIV infection and AIDS REVISED", Med Scape Medical New. December 10, 2008.

[4] J. Durgavish et al, "Nigeria: Rapid Assessment of HIV/AIDS care in public and private sectors", US Agency for International Development. August 2004.

[5] J. Dieter, "Effect of alcohol and HIV infection on central Nervous system", National institute on Alcohol Abuse and alcoholism of the National Alcohol Research & Health. Vol. 25, No 4, 2001.

[6] J. Gehrke, R. Ramakrishnan, "Database Management System" second edition, McGraw-Hill Higher Education. 2000.

[7] M. Lilly, P. Balasubramanie, "Multilayer Feed Backward Neural Network Model for Medical Decision Support: Implementation of back propagation Algorithm in HIV/AIDS regimen. International Journal of Reviews in Computing. Vol. 1, December 2009.

[8] O. Adeyi et al, "AIDS in Nigeria: A nation on the threshold: The epidemiology of HIV/AIDS in Nigeria", Harvard Center for Population and Development Studies.2006.

[9] O. G. Lala et al, "Web-Based Systems for the Management of HIV/AIDS", 4th International Conference on ICT Applications (AICTTRA). Pp 140 – 150, September 2009.

[10] R. Seth et al, "Psychoneuro Immunology: An analysis of HIV and Cancer", URJHS vol. 9, 2008.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

APPENDIX

Home page

Doctor page

Login

Patient page

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Data Mining System For Quality Prediction Of Petrol Using Artificial Neural Network

Omowumi O. Adeyemo[1] Adenike O. Osofisan Ebunoluwa P. Fashina
Kayode Otubu

Department of Computer Science
University of Ibadan
Ibadan, Nigeria
[1]Correspondence Author: wumiglory@yahoo.com

Abstract— The increasing cry of the masses over poor quality of petroleum products most especially petrol has poised researchers and refinery engineers to devise a way of telling the class of quality of products expected from a sample crude oil without having to refine it. To this end, a system that can predict the quality and class of petrol expected from a sample crude oil is desired. Getting such accurate predictions for the class and hence the quality of petrol however can be tasking for humans. This work presents a data mining system, which implemented a multi-layer neural network trained with the back propagation training algorithm. The focus, however, was on petrol because of its significance and wide usage. The outcome generated by the system shows that multilayer perception back propagation neural network could successfully classify and predict the quality of petrol.

Keywords- Petrol; Multilayer Perceptron; Data Mining; Quality; Back Propagation

I. INTRODUCTION

Today, organizations are accumulating vast and growing amounts of data in different formats. The patterns, associations, or relationships among all these data can provide information. However, the vast and fast-growing amount of data normally exceeds human ability for comprehension and analysis without powerful tools. As a result, data collected in large data sources become "data tombs"- data archives that are seldom visited. Even when the databases serve as information sources, poor decisions are made because the decision makers do not have appropriate tools to extract the valuable knowledge embedded in the vast amount of data.

In fact, refinery engineers have based decisions on crude oil refining on the rule of thumb for many years. With the invention of data mining, the challenges are surmountable. Data Mining refers to the nontrivial extraction of implicit, previously unknown and potentially useful information from data in databases [7]. It is a key step of knowledge discovery in databases (KDD). In other words, data mining involves the systematic analysis of large datasets using automated methods. By probing data in this manner, it is possible to prove or disprove existing hypotheses or ideas regarding data or information while discovering new or previously unknown information. It is noted for its Pattern Recognition ability that ensures that information is obtained from vague data [3]. In particular, unique or valuable relationships between and within the data can be identified and used proactively to categorize or anticipate additional data.

1.1 ARTIFICIAL NEURAL NETWORKS

Artificial Neural Networks (ANNs) are biologically inspired structures composed of elements that perform in a manner analogous to the most elementary functions of the biological neuron. ANN can modify its behavior in response to the environment. Thus, given a set of inputs (and perhaps with desired outputs), ANN self-adjust to produce consistent responses. ANNs are capable to perform tasks like learning, memorize, experience and generalize. Neural Networks, also known as Neural Computing, is a field of research in artificial simple intelligence. It is the study of networks of adaptable nodes which, through a process of learning from task examples, store experimental knowledge and make it available for use. A Neural Network is a group of processing elements where one subgroup makes independent computations and passes the result to a second subgroup. Each subgroup may, in turn, make its independent computations and the result to yet another subgroup. Finally, a subgroup of one or more processing elements determines the output of the network.

Neural Computing derives its name from the fact that it is a field that tries to mimic the functions that the biological neural system of the human brain performs. Neural Networks have been able to exhibit some very interesting and important features that are peculiar to the brain. One such feature is learning. It is necessary at this point to address the need to imitate the biological neural system, as adopted in neural computing ([8].

Learning, for example, is the way by which, as children, we pick up speech, learn to write, eat and drink and develop our own set of standards and morals. On the other hand, learning in computer systems often requires the building of a rule-base which must provide for all possible combinations that are often endless [4]. Artificial Neural Networks (ANN) , which emerged as a major paradigm for

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

data mining applications were inspired by biological findings relating to the behavior of the brain as a network of units called neurons.

While there are numerous different (artificial) neural network architectures that have been studied by researchers, the most successful applications in data mining of neural networks have been multilayer feed-forward networks. These are networks in which there is an input layer consisting of nodes that simply accept the input values and successive layers of nodes that are neurons. The outputs of neurons in a layer are inputs to neurons in the next layer. The last layer is called the output layer.Layers between the input and output layers are known as hidden layers. Figure 1 presents a diagram for this architecture.

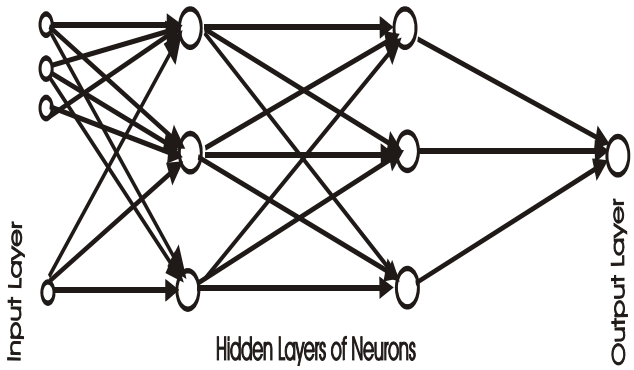


Fig1. Multilayer Neural Networks

Neural networks are of particular interest because they offer a means to efficiently model large and complex problems in which there may be hundreds of predictor variables that have many interactions. Neural nets may be used in classification problems (where the output is a categorical variable) or for regressions (where the output variable is continuous).

1.2 RELATED WORKS

Artificial Neural Network (ANN) has been applied in several areas of crude oil content prediction. One of it is the work done by Linde et al. [2] where ANN was used for Air-to-Fuel Ratio (A/F) Estimation in Two-Stroke Combustion Engines. Though most of the larger engines in automobile have sensors but there are a number of problems with these sensors. Part of the problem is that it is expensive, slow, sensitive to pollution and gives only a binary input i.e. indicating whether the A/F is above or below a factory set value. This necessitates the need to seek for other ways of measuring Air-to-fuel Ratio. They used ion-current measurements and artificial neural networks to estimate A/F is developed and evaluated. The tests have also shown that it is possible to extract other information from this signal, like misfiring, the fuel quality, and others. The result should be seen as a first step towards a complete, self-tuning engine control system.

Commuri et al. [5] developed a neural network-based Intelligent Asphalt Compaction Analyzer (IACA). IACA was a novel neural network-based approach. It is contrary to existing techniques where a model is developed to fit the experimental data and to predict the density of the mat. Their's was a model-free approach which used pattern-recognition techniques to estimate the density. The neural network was first trained using several vibration patterns corresponding to different density levels to extract the features from the vibrations of the compactor and used these features to estimate the level of compaction. The IACA output was continuously available to the operator in real time and could serve as a useful guide during the compaction process.

She et al. [6], proposed an expert control strategy based on a combination of back propagation networks, mathematical models and rule models to compute and track the target percentages accurately. The previously used conventional computation methods involve constructing mathematical models to predict quality based on measured data for coal blending and distillation, and then computing the target percentages using the models. The models mainly employed linear system identification techniques, such as the least-squares method. However, it is difficult to get accurate percentages by conventional methods because the computation is based solely on the mathematical models, which do not describe the exact relationships among the parameters that characterize the quality of the coal blend and coke, and the quality and percentage of each type of coal. The system used empirical knowledge to solve the control problem. The strategy was implemented in a hierarchical configuration with two controllers that does not have the drawbacks of the conventional methods.

In another related work, Akinyokun et al. [1] used an Unsupervised Self Organizing Map (SOM) of neural networks for the determination of oil well lithology and fluid contents. Their work was based on fuzzy inference rules derived from known characteristics of well logs. The application was justified because the interpretation of the clusters generated by the SOM neural networks represents the characterization of the contents.

Despite the contributions of these works, none has been able to result in a generic and robust intelligent system that can analyze the huge amount of crude oil data and predict quality of petrol expected from a given crude oil. These are achievable using multilayer perceptron neural network whose topology can be altered at any time and generate very accurate prediction. This kind of system is required by refiners who require a powerful and robust tool that can help analyze the huge amount of data in an attempt to predict the class and quality of petrol expected from a given sample of crude oil. With such predictor, the refiners can tell if the desired class of petrol can be obtained from the sample crude oil without having to refine it. This of course eliminates incurable of more cost of computing and products.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

1. METHODOLOGY

The data used for the prediction is crude oil exploratory data obtained from a refinery in Nigeria. Data Preparation is performed on the acquired data. The data acquired is highly susceptible to noise, and inconsistent. This is due to the huge size or human error. Thus, data to be fed into the Neural Network has to be preprocessed in order to help improve the accuracy of the algorithm. There are a number of data preprocessing techniques. They include data cleaning, data integration, data reduction, and data transformations. This work performs data transformations, specifically normalization (Min-max normalization). The model algorithm is back propagation and can only work on data input within the range of 0 and 1. Therefore Min-max normalization is performed to transform the attribute data. In the normalization, attribute data are scaled so as to fall within a small specified range of -1.0 to 1.0 and 0.0 to 1.0. This is linear transformation. It improves the accuracy and efficiency of the mining algorithm. Min-max normalization, used for this project, performs a linear transformation on the original data. This is done to transform the attributes into a form usable for model algorithms.

Since there are no clear rules as to the number of hidden layer units, this work uses Neural Network with 1 layer each for the input, hidden and output. Network design is a trial-and-error process and may affect the accuracy of the resulting trained network. The initial values of the weights may also affect the resulting accuracy. Once a network has been trained and its accuracy is not considered acceptable, the training process is repeated with a different network topology or a different set of initial weights. In this work, Multi-Layer Perceptrons (MLPs), a special architecture of ANNs are implemented using backpropagation algorithm. This work implements two versions (modes) of the back-propagation algorithm they are Pattern-by-Pattern Mode and Batch Mode. Since the result or output is foreknown, a learning that is guided by knowing what we want to achieve, is known as supervised learning.

Given the topology of the network (number of layers, number of neurons per layer) and the type of activation function used, the synaptic weights (which in general are randomly set at the beginning) are then adjusted so that at the next iteration the output produced by the network are closer to the desired output. The ultimate goal of the training procedure is to minimize the observed error between the desired output and the actual output produced by the network. At the termination of the training process, the neural network has learnt to produce an output that closely matches the desired output. Then the network's structure is frozen and the network becomes operational, ready to be used for prediction of oil quality from the properties of the crude oil. It is to be emphasized that Prediction is made by specifying the properties of the crude oil obtained from laboratory test on the crude oil. The system outputs the density of the petrol expected from the sample crude oil. Based on this, it further classifies the petrol as light, medium or heavy petrol.

2. IMPLEMENTATION

The main interface of this application is shown in figure 2. It has four menu options that provide various functionalities. The first one is the *File Menu***,** it enables the user to save network data, exit application and reset the memory of the Neural Networks. The *Network Menu* enables the user to build his desired neural network, by specifying the number of neurons in the input layer, the number of neurons in the hidden layer, the number of neurons in the output layer. It allows user to specify his Training Method. It also allows the user to load or randomize weights and thresholds that the Neural Network uses initially. Inputs for other Network data like the learning rate, the momentum, number of époques, and the number of data are also taken using this menu. It allows users to analyze the network. The *Parameter–Setup Menu* allows user to change the network parameters. The Help Menu allows the user to view simple instructions about the system. Figure 4 is the platform that allows users to specify the network parameters. The user launches the system, specifies the network topology and creates the neural network as presented in the figure 3. This allows user to specify his choice of network. User then proceeds to the process of making predictions by clicking the Menu item.

This prompts the user to specify the thresholds (biases), weights to be used initially by the neural network as presented in figures 5- 9. In figures 10-14, the threshold for input, hidden and output layer are generated. The training data is then requested to be loaded. Data can be randomly generated or loaded from text files. On presentation of inputs for building the network topology and the initialization of parameters, the training data are then loaded into the built network to be trained. After training ends, the training information is displayed as presented in figure 15- Training data can be loaded from text files or be randomized, but this does not give accurate results. The training is then performed and this yields a Learned Neural Network. The altering page is presented in figure 16.

The network is tested by comparing the output expected with the network output. The output is then presented to user in a readable format for acceptability of the network accuracy. This gives a learned network. With the accuracy of the network ascertained as presented in figure 17, the system is suitable for making prediction of oil quality.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

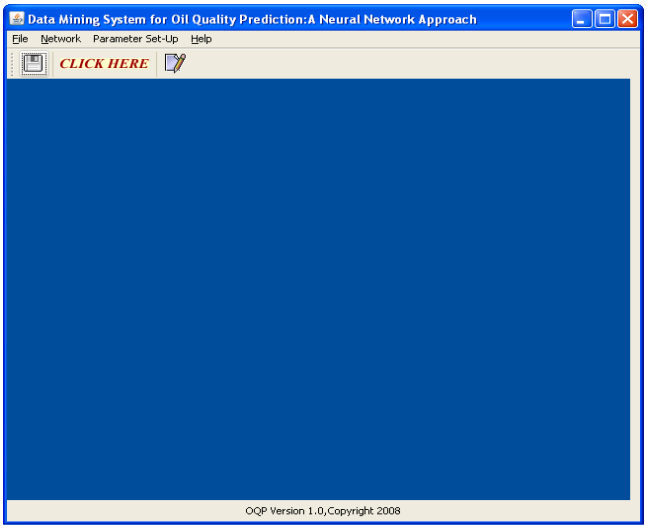


Fig2. Main Interface

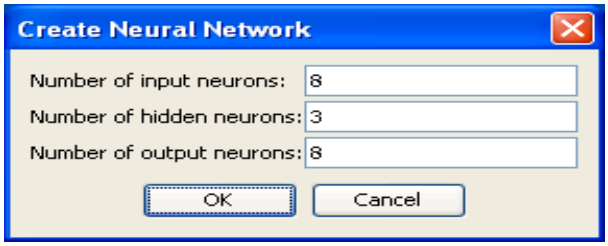


Fig3. Network Topology Design window

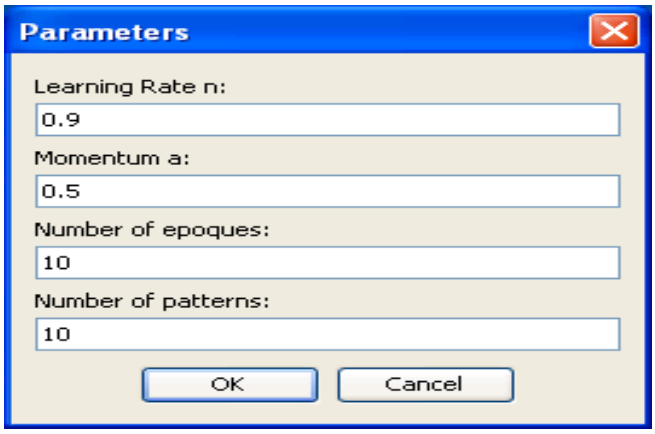


Fig4. Network Parameters Input window

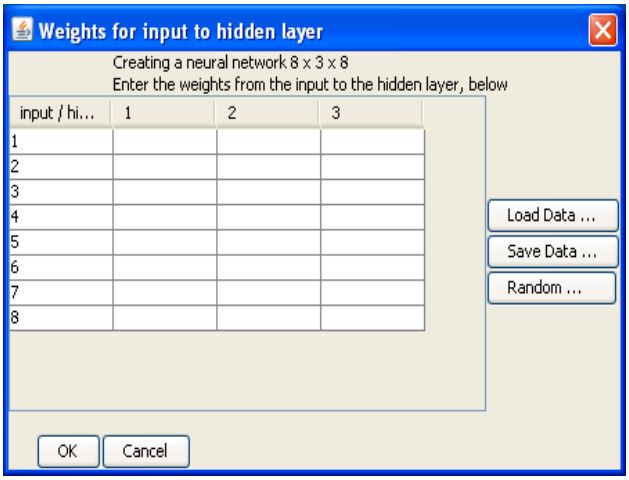


Fig5. Initial Weights Input for the network

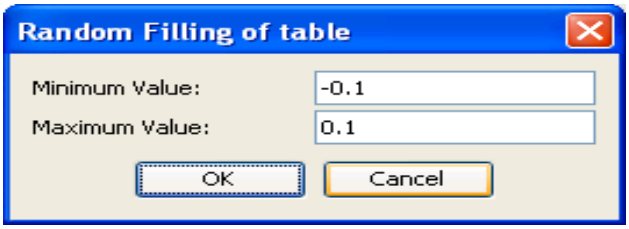


Fig6. Range of Initial Weights (Hidden to Output)

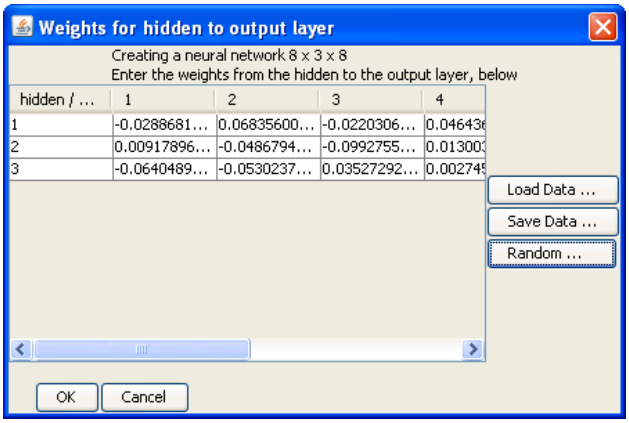


Fig7. Weights are generated

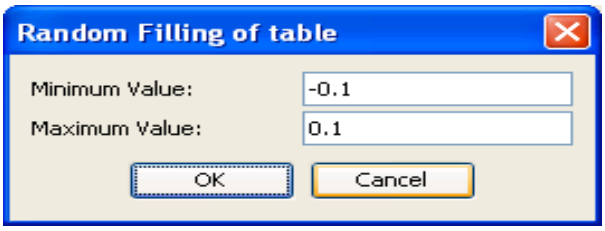


Fig8. Range of Initial Weights (Hidden to Output)

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

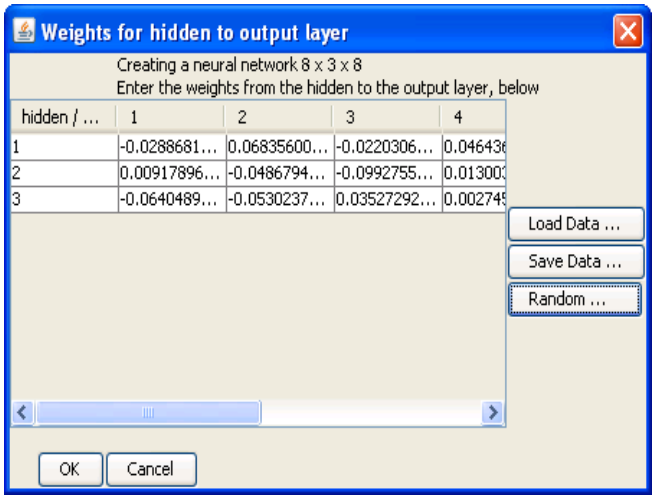


Fig9. Weights are generated

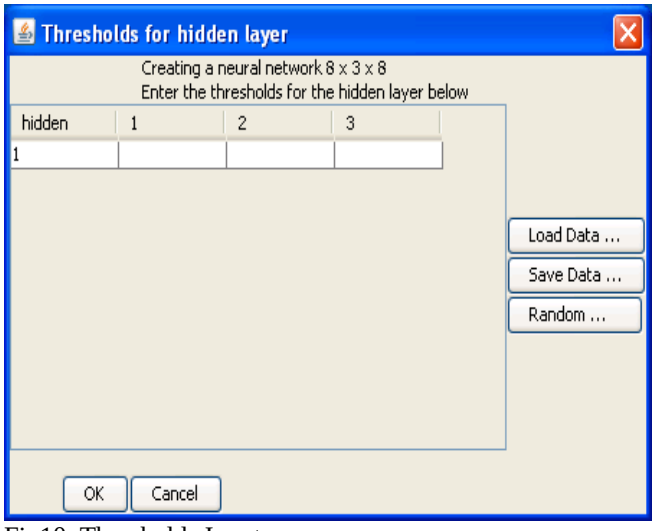


Fig10. Thresholds Input

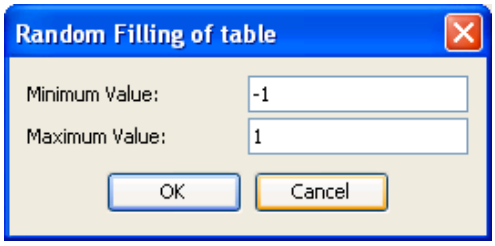


Fig11. Range of Thresholds are specified

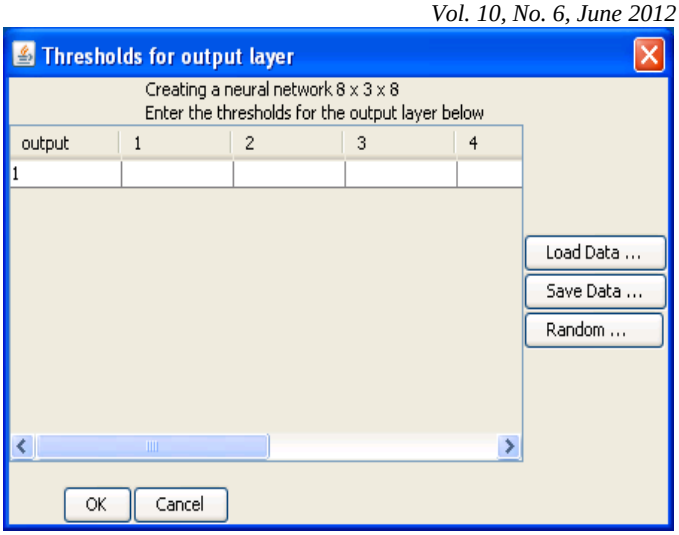


Fig12. Thresholds are generated

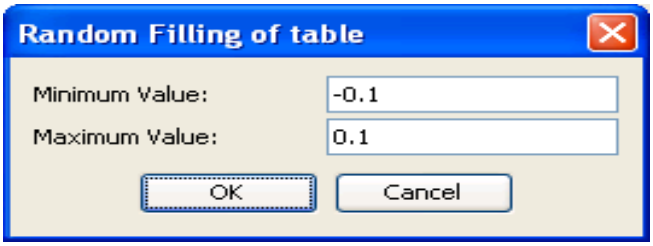


Fig13.Range of Thresholds are generated

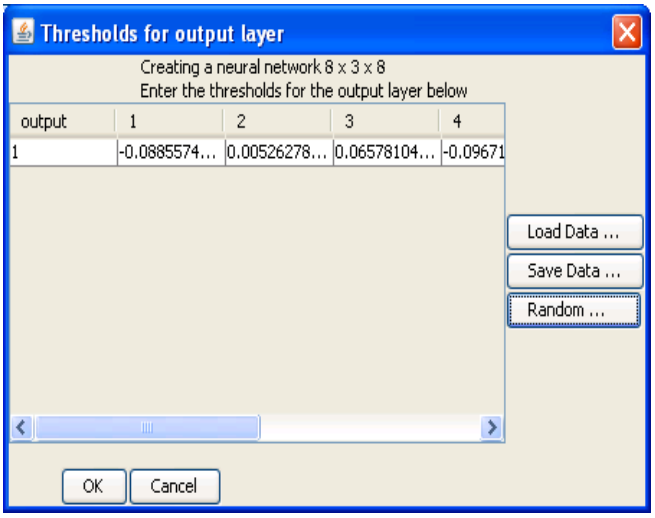


Fig14. Thresholds are generated

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

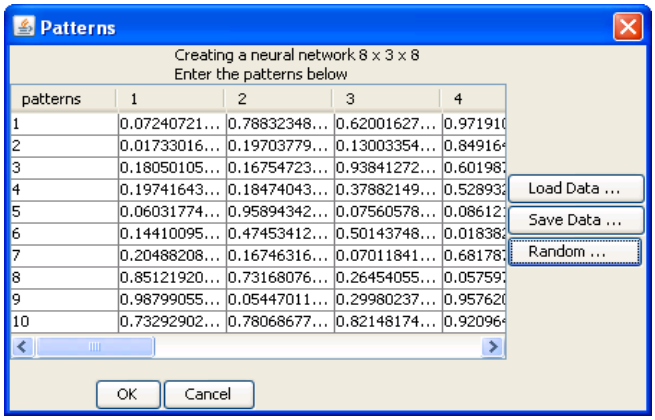


Fig15. Training Data generated

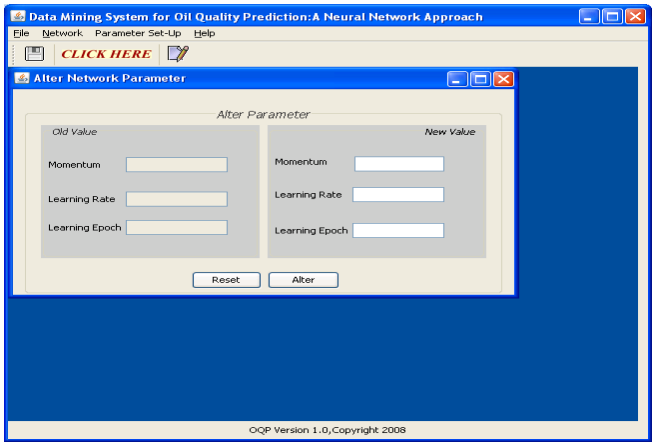


Fig16. Altering the network topology

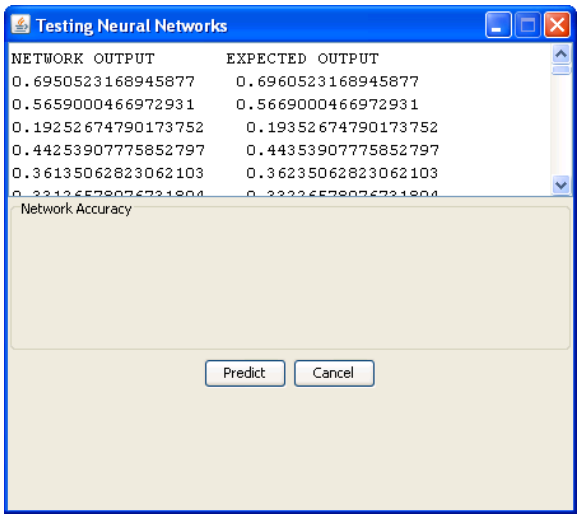


Fig 17. Test Result Displayed

3. CONCLUSION

This work has shown that the strength of Neural Network to mimic the human brain and make accurate predictions cannot be over-emphasized. Its application, as applied in this work has shown that refinery engineers can predict the quality of crude oil expected from a crude oil sample. Not only will such predictions tell the quality of petrol expected from a crude oil sample, it will also prevent the need to refine crude oil that will not yield the desired petrol. It thus enhances a cost-effective refining process.

In future, this work will be extended by comparing multilayer perceptron neural networks with other artificial neural networks to get the best prediction. Also, we will combine neural networks and fuzzy logic to obtain useful information from fuzzy data.

References

[1] Akinyokun O.C., Enikanselu P.A., Adeyemo A.B. and Adesida B. (2009) "Well Log Interpretation Model for the Determination of Lithology and Fluid Contents". *Pacific Journal of Science and Technology*. 507-517.

[2] Linde A., Taveniku M., and Svensson B. (1992). Using Neural Networks for Air-to-Fuel Ratio Estimation in Two-Stroke Combustion Engines.

[3] Baker B. "Forensic Audit and Automated Oversight", Office of Auditor General based on logistic model tree. JBiSE. Vol.2, No.6, 2009, pp. 405-411.

[4] Bansal K., V.adhavkar S, and Gupta A. (1998), Neural networks based forecasting techniques for inventory control applications. *Data Mining and Knowledge Discovery*, 2(1):97–102.

[5] Commuri S., Mai A.T., and Zaman M. (2007), A Novel Neural Network-Based Asphalt Compaction Analyzer, *Int. J. Pavement Engineering.*

[6] She J., Min W., Nakano M. (1999),A Model-Based Expert Control Strategy Using Neural Networks for the Coal Blending Process in an Iron and Steel Plant. *Expert System with Applications*, Vol. 16, No. 3, pp. 271-281.

[7] Zaiane O. R. (1999) Principle of Knowledge Discovery in Databases, University of Alberta. Department of Computer Science. CMPUT690.

[8] Pujar A.K. (2001), Data Mining Techniques, University Press, 1st Edition, 2001.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

IJCSIS REVIEWERS' LIST

Assist Prof (Dr.) M. Emre Celebi, Louisiana State University in Shreveport, USA
Dr. Lam Hong Lee, Universiti Tunku Abdul Rahman, Malaysia
Dr. Shimon K. Modi, Director of Research BSPA Labs, Purdue University, USA
Dr. Jianguo Ding, Norwegian University of Science and Technology (NTNU), Norway
Assoc. Prof. N. Jaisankar, VIT University, Vellore,Tamilnadu, India
Dr. Amogh Kavimandan, The Mathworks Inc., USA
Dr. Ramasamy Mariappan, Vinayaka Missions University, India
Dr. Yong Li, School of Electronic and Information Engineering, Beijing Jiaotong University, P.R. China
Assist. Prof. Sugam Sharma, NIET, India / Iowa State University, USA
Dr. Jorge A. Ruiz-Vanoye, Universidad Autónoma del Estado de Morelos, Mexico
Dr. Neeraj Kumar, SMVD University, Katra (J&K), India
Dr Genge Bela, "Petru Maior" University of Targu Mures, Romania
Dr. Junjie Peng, Shanghai University, P. R. China
Dr. Ilhem LENGLIZ, HANA Group - CRISTAL Laboratory, Tunisia
Prof. Dr. Durgesh Kumar Mishra, Acropolis Institute of Technology and Research, Indore, MP, India
Jorge L. Hernández-Ardieta, University Carlos III of Madrid, Spain
Prof. Dr.C.Suresh Gnana Dhas, Anna University, India
Mrs Li Fang, Nanyang Technological University, Singapore
Prof. Pijush Biswas, RCC Institute of Information Technology, India
Dr. Siddhivinayak Kulkarni, University of Ballarat, Ballarat, Victoria, Australia
Dr. A. Arul Lawrence, Royal College of Engineering & Technology, India
Mr. Wongyos Keardsri, Chulalongkorn University, Bangkok, Thailand
Mr. Somesh Kumar Dewangan, CSVTU Bhilai (C.G.)/ Dimat Raipur, India
Mr. Hayder N. Jasem, University Putra Malaysia, Malaysia
Mr. A.V.Senthil Kumar, C. M. S. College of Science and Commerce, India
Mr. R. S. Karthik, C. M. S. College of Science and Commerce, India
Mr. P. Vasant, University Technology Petronas, Malaysia
Mr. Wong Kok Seng, Soongsil University, Seoul, South Korea
Mr. Praveen Ranjan Srivastava, BITS PILANI, India
Mr. Kong Sang Kelvin, Leong, The Hong Kong Polytechnic University, Hong Kong
Mr. Mohd Nazri Ismail, Universiti Kuala Lumpur, Malaysia
Dr. Rami J. Matarneh, Al-isra Private University, Amman, Jordan
Dr Ojesanmi Olusegun Ayodeji, Ajayi Crowther University, Oyo, Nigeria
Dr. Riktesh Srivastava, Skyline University, UAE
Dr. Oras F. Baker, UCSI University - Kuala Lumpur, Malaysia
Dr. Ahmed S. Ghiduk, Faculty of Science, Beni-Suef University, Egypt
and Department of Computer science, Taif University, Saudi Arabia
Mr. Tirthankar Gayen, IIT Kharagpur, India
Ms. Huei-Ru Tseng, National Chiao Tung University, Taiwan

CALL FOR PAPERS
International Journal of Computer Science and Information Security
January - December
IJCSIS 2012
ISSN: 1947-5500
http://sites.google.com/site/ijcsis/

International Journal Computer Science and Information Security, IJCSIS, is the premier scholarly venue in the areas of computer science and security issues. IJCSIS 2011 will provide a high profile, leading edge platform for researchers and engineers alike to publish state-of-the-art research in the respective fields of information technology and communication security. The journal will feature a diverse mixture of publication articles including core and applied computer science related topics.

Authors are solicited to contribute to the special issue by submitting articles that illustrate research results, projects, surveying works and industrial experiences that describe significant advances in the following areas, but are not limited to. Submissions may span a broad range of topics, e.g.:

Track A: Security

Access control, Anonymity, Audit and audit reduction & Authentication and authorization, Applied cryptography, Cryptanalysis, Digital Signatures, Biometric security, Boundary control devices, Certification and accreditation, Cross-layer design for security, Security & Network Management, Data and system integrity, Database security, Defensive information warfare, Denial of service protection, Intrusion Detection, Anti-malware, Distributed systems security, Electronic commerce, E-mail security, Spam, Phishing, E-mail fraud, Virus, worms, Trojan Protection, Grid security, Information hiding and watermarking & Information survivability, Insider threat protection, Integrity
Intellectual property protection, Internet/Intranet Security, Key management and key recovery, Language-based security, Mobile and wireless security, Mobile, Ad Hoc and Sensor Network Security, Monitoring and surveillance, Multimedia security ,Operating system security, Peer-to-peer security, Performance Evaluations of Protocols & Security Application, Privacy and data protection, Product evaluation criteria and compliance, Risk evaluation and security certification, Risk/vulnerability assessment, Security & Network Management, Security Models & protocols, Security threats & countermeasures (DDoS, MiM, Session Hijacking, Replay attack etc,), Trusted computing, Ubiquitous Computing Security, Virtualization security, VoIP security, Web 2.0 security, Submission Procedures, Active Defense Systems, Adaptive Defense Systems, Benchmark, Analysis and Evaluation of Security Systems, Distributed Access Control and Trust Management, Distributed Attack Systems and Mechanisms, Distributed Intrusion Detection/Prevention Systems, Denial-of-Service Attacks and Countermeasures, High Performance Security Systems, Identity Management and Authentication, Implementation, Deployment and Management of Security Systems, Intelligent Defense Systems, Internet and Network Forensics, Large-scale Attacks and Defense, RFID Security and Privacy, Security Architectures in Distributed Network Systems, Security for Critical Infrastructures, Security for P2P systems and Grid Systems, Security in E-Commerce, Security and Privacy in Wireless Networks, Secure Mobile Agents and Mobile Code, Security Protocols, Security Simulation and Tools, Security Theory and Tools, Standards and Assurance Methods, Trusted Computing, Viruses, Worms, and Other Malicious Code, World Wide Web Security, Novel and emerging secure architecture, Study of attack strategies, attack modeling, Case studies and analysis of actual attacks, Continuity of Operations during an attack, Key management, Trust management, Intrusion detection techniques, Intrusion response, alarm management, and correlation analysis, Study of tradeoffs between security and system performance, Intrusion tolerance systems, Secure protocols, Security in wireless networks (e.g. mesh networks, sensor networks, etc.), Cryptography and Secure Communications, Computer Forensics, Recovery and Healing, Security Visualization, Formal Methods in Security, Principles for Designing a Secure Computing System, Autonomic Security, Internet Security, Security in Health Care Systems, Security Solutions Using Reconfigurable Computing, Adaptive and Intelligent Defense Systems, Authentication and Access control, Denial of service attacks and countermeasures, Identity, Route and

Location Anonymity schemes, Intrusion detection and prevention techniques, Cryptography, encryption algorithms and Key management schemes, Secure routing schemes, Secure neighbor discovery and localization, Trust establishment and maintenance, Confidentiality and data integrity, Security architectures, deployments and solutions, Emerging threats to cloud-based services, Security model for new services, Cloud-aware web service security, Information hiding in Cloud Computing, Securing distributed data storage in cloud, Security, privacy and trust in mobile computing systems and applications, **Middleware security & Security features:** middleware software is an asset on
its own and has to be protected, interaction between security-specific and other middleware features, e.g., context-awareness, **Middleware-level security monitoring and measurement:** metrics and mechanisms for quantification and evaluation of security enforced by the middleware, **Security co-design:** trade-off and co-design between application-based and middleware-based security, **Policy-based management:** innovative support for policy-based definition and enforcement of security concerns, **Identification and authentication mechanisms:** Means to capture application specific constraints in defining and enforcing access control rules, **Middleware-oriented security patterns:** identification of patterns for sound, reusable security, **Security in aspect-based middleware:** mechanisms for isolating and enforcing security aspects, **Security in agent-based platforms:** protection for mobile code and platforms, Smart Devices: Biometrics, National ID cards, Embedded Systems Security and TPMs, RFID Systems Security, Smart Card Security, Pervasive Systems: Digital Rights Management (DRM) in pervasive environments, Intrusion Detection and Information Filtering, Localization Systems Security (Tracking of People and Goods), Mobile Commerce Security, Privacy Enhancing Technologies, Security Protocols (for Identification and Authentication, Confidentiality and Privacy, and Integrity), Ubiquitous Networks: Ad Hoc Networks Security, Delay-Tolerant Network Security, Domestic Network Security, Peer-to-Peer Networks Security, Security Issues in Mobile and Ubiquitous Networks, Security of GSM/GPRS/UMTS Systems, Sensor Networks Security, Vehicular Network Security, Wireless Communication Security: Bluetooth, NFC, WiFi, WiMAX, WiMedia, others

This Track will emphasize the design, implementation, management and applications of computer communications, networks and services. Topics of mostly theoretical nature are also welcome, provided there is clear practical potential in applying the results of such work.

Track B: Computer Science

Broadband wireless technologies: LTE, WiMAX, WiRAN, HSDPA, HSUPA, Resource allocation and interference management, Quality of service and scheduling methods, Capacity planning and dimensioning, Cross-layer design and Physical layer based issue, Interworking architecture and interoperability, Relay assisted and cooperative communications, Location and provisioning and mobility management, Call admission and flow/congestion control, Performance optimization, Channel capacity modeling and analysis, Middleware Issues: Event-based, publish/subscribe, and message-oriented middleware, Reconfigurable, adaptable, and reflective middleware approaches, Middleware solutions for reliability, fault tolerance, and quality-of-service, Scalability of middleware, Context-aware middleware, Autonomic and self-managing middleware, Evaluation techniques for middleware solutions, Formal methods and tools for designing, verifying, and evaluating, middleware, Software engineering techniques for middleware, Service oriented middleware, Agent-based middleware, Security middleware, Network Applications: Network-based automation, Cloud applications, Ubiquitous and pervasive applications, Collaborative applications, RFID and sensor network applications, Mobile applications, Smart home applications, Infrastructure monitoring and control applications, Remote health monitoring, GPS and location-based applications, Networked vehicles applications, Alert applications, Embeded Computer System, Advanced Control Systems, and Intelligent Control : Advanced control and measurement, computer and microprocessor-based control, signal processing, estimation and identification techniques, application specific IC's, nonlinear and adaptive control, optimal and robot control, intelligent control, evolutionary computing, and intelligent systems, instrumentation subject to critical conditions, automotive, marine and aero-space control and all other control applications, Intelligent Control System, Wiring/Wireless Sensor, Signal Control System. Sensors, Actuators and Systems Integration : Intelligent sensors and actuators, multisensor fusion, sensor array and multi-channel processing, micro/nano technology, microsensors and microactuators, instrumentation electronics, MEMS and system integration, wireless sensor, Network Sensor, Hybrid

Sensor, Distributed Sensor Networks. Signal and Image Processing : Digital signal processing theory, methods, DSP implementation, speech processing, image and multidimensional signal processing, Image analysis and processing, Image and Multimedia applications, Real-time multimedia signal processing, Computer vision, Emerging signal processing areas, Remote Sensing, Signal processing in education. Industrial Informatics: Industrial applications of neural networks, fuzzy algorithms, Neuro-Fuzzy application, bioInformatics, real-time computer control, real-time information systems, human-machine interfaces, CAD/CAM/CAT/CIM, virtual reality, industrial communications, flexible manufacturing systems, industrial automated process, Data Storage Management, Harddisk control, Supply Chain Management, Logistics applications, Power plant automation, Drives automation. Information Technology, Management of Information System : Management information systems, Information Management, Nursing information management, Information System, Information Technology and their application, Data retrieval, Data Base Management, Decision analysis methods, Information processing, Operations research, E-Business, E-Commerce, E-Government, Computer Business, Security and risk management, Medical imaging, Biotechnology, Bio-Medicine, Computer-based information systems in health care, Changing Access to Patient Information, Healthcare Management Information Technology. Communication/Computer Network, Transportation Application : On-board diagnostics, Active safety systems, Communication systems, Wireless technology, Communication application, Navigation and Guidance, Vision-based applications, Speech interface, Sensor fusion, Networking theory and technologies, Transportation information, Autonomous vehicle, Vehicle application of affective computing, Advance Computing technology and their application : Broadband and intelligent networks, Data Mining, Data fusion, Computational intelligence, Information and data security, Information indexing and retrieval, Information processing, Information systems and applications, Internet applications and performances, Knowledge based systems, Knowledge management, Software Engineering, Decision making, Mobile networks and services, Network management and services, Neural Network, Fuzzy logics, Neuro-Fuzzy, Expert approaches, Innovation Technology and Management : Innovation and product development, Emerging advances in business and its applications, Creativity in Internet management and retailing, B2B and B2C management, Electronic transceiver device for Retail Marketing Industries, Facilities planning and management, Innovative pervasive computing applications, Programming paradigms for pervasive systems, Software evolution and maintenance in pervasive systems, Middleware services and agent technologies, Adaptive, autonomic and context-aware computing, Mobile/Wireless computing systems and services in pervasive computing, Energy-efficient and green pervasive computing, Communication architectures for pervasive computing, Ad hoc networks for pervasive communications, Pervasive opportunistic communications and applications, Enabling technologies for pervasive systems (e.g., wireless BAN, PAN), Positioning and tracking technologies, Sensors and RFID in pervasive systems, Multimodal sensing and context for pervasive applications, Pervasive sensing, perception and semantic interpretation, Smart devices and intelligent environments, Trust, security and privacy issues in pervasive systems, User interfaces and interaction models, Virtual immersive communications, Wearable computers, Standards and interfaces for pervasive computing environments, Social and economic models for pervasive systems, Active and Programmable Networks, Ad Hoc & Sensor Network, Congestion and/or Flow Control, Content Distribution, Grid Networking, High-speed Network Architectures, Internet Services and Applications, Optical Networks, Mobile and Wireless Networks, Network Modeling and Simulation, Multicast, Multimedia Communications, Network Control and Management, Network Protocols, Network Performance, Network Measurement, Peer to Peer and Overlay Networks, Quality of Service and Quality of Experience, Ubiquitous Networks, Crosscutting Themes – Internet Technologies, Infrastructure, Services and Applications; Open Source Tools, Open Models and Architectures; Security, Privacy and Trust; Navigation Systems, Location Based Services; Social Networks and Online Communities; ICT Convergence, Digital Economy and Digital Divide, Neural Networks, Pattern Recognition, Computer Vision, Advanced Computing Architectures and New Programming Models, Visualization and Virtual Reality as Applied to Computational Science, Computer Architecture and Embedded Systems, Technology in Education, Theoretical Computer Science, Computing Ethics, Computing Practices & Applications

Authors are invited to submit papers through e-mail ijcsiseditor@gmail.com. Submissions must be original and should not have been published previously or be under consideration for publication while being evaluated by IJCSIS. Before submission authors should carefully read over the journal's Author Guidelines, which are located at http://sites.google.com/site/ijcsis/authors-notes .

ISSN 1947 5500