Volume 5 ▪ Issue 1 ▪ March 2011

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND SECURITY (IJCSS)

ISSN : 1985-1553

Publication Frequency: 6 Issues / Year

CSC PUBLISHERS
http://www.cscjournals.org

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND SECURITY (IJCSS)

VOLUME 5, ISSUE 1, 2011

EDITED BY
DR. NABEEL TAHIR

ISSN (Online): 1985-1553
International Journal of Computer Science and Security is published both in traditional paper form and in Internet. This journal is published at the website http://www.cscjournals.org, maintained by Computer Science Journals (CSC Journals), Malaysia.

IJCSS Journal is a part of CSC Publishers
Computer Science Journals
http://www.cscjournals.org

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND SECURITY (IJCSS)

Book: Volume 5, Issue 1, March 2011
Publishing Date: 04-04-2011
ISSN (Online): 1985-1553

IJCSS Journal is a part of CSC Publishers
http://www.cscjournals.org

Published in Malaysia

Typesetting: Camera-ready by author, data conversation by CSC Publishing Services – CSC Journals, Malaysia

CSC Publishers, 2011

EDITORIAL PREFACE

This is first issue of volume five of the International Journal of Computer Science and Security (IJCSS). IJCSS is an International refereed journal for publication of current research in computer science and computer security technologies. IJCSS publishes research papers dealing primarily with the technological aspects of computer science in general and computer security in particular. Publications of IJCSS are beneficial for researchers, academics, scholars, advanced students, practitioners, and those seeking an update on current experience, state of the art research theories and future prospects in relation to computer science in general but specific to computer security studies. Some important topics cover by IJCSS are databases, electronic commerce, multimedia, bioinformatics, signal processing, image processing, access control, computer security, cryptography, communications and data security, etc.

The initial efforts helped to shape the editorial policy and to sharpen the focus of the journal. Starting with volume 5, 2011, IJCSS appears in more focused issues. Besides normal publications, IJCSS intend to organized special issues on more focused topics. Each special issue will have a designated editor (editors) – either member of the editorial board or another recognized specialist in the respective field.

This journal publishes new dissertations and state of the art research to target its readership that not only includes researchers, industrialists and scientist but also advanced students and practitioners. The aim of IJCSS is to publish research which is not only technically proficient, but contains innovation or information for our international readers. In order to position IJCSS as one of the top International journal in computer science and security, a group of highly valuable and senior International scholars are serving its Editorial Board who ensures that each issue must publish qualitative research articles from International research communities relevant to Computer science and security fields.

IJCSS editors understand that how much it is important for authors and researchers to have their work published with a minimum delay after submission of their papers. They also strongly believe that the direct communication between the editors and authors are important for the welfare, quality and wellbeing of the Journal and its readers. Therefore, all activities from paper submission to paper publication are controlled through electronic systems that include electronic submission, editorial panel and review system that ensures rapid decision with least delays in the publication processes.

To build its international reputation, we are disseminating the publication information through Google Books, Google Scholar, Directory of Open Access Journals (DOAJ), Open J Gate, ScientificCommons, Docstoc and many more. Our International Editors are working on establishing ISI listing and a good impact factor for IJCSS. We would like to remind you that the success of our journal depends directly on the number of quality articles submitted for review. Accordingly, we would like to request your participation by submitting quality manuscripts for review and encouraging your colleagues to submit quality manuscripts for review. One of the great benefits we can provide to our prospective authors is the mentoring nature of our review process. IJCSS provides authors with high quality, helpful reviews that are shaped to assist authors in improving their manuscripts.

Editorial Board Members
International Journal of Computer Science and Security (IJCSS)

EDITORIAL BOARD

ASSOCIATE EDITORS (AEiCs)

EDITORIAL BOARD MEMBERS (EBMs)

TABLE OF CONTENTS

Volume 5, Issue 1, April 2011

Pages

1 - 13 Stream Processing Environmental Applications in Jordan Valley
Iyad Ahmad Aldasouqi, Jalal Atoum

14 - 27 Development of Predictor for Sequence Derived Features From Amino Acid Sequence Using Associate Rule Mining
Manpreet Singh, Gurvinder Singh

28 - 38 Car-Following Parameters by Means of Cellular Automata in the Case of Evacuation
Kohei Arai, Tri Harsono, Achmad Basuki

39 - 53 Information Technology (IT) Security Framework for Kenyan Small and Medium Enterprises (SMEs)
Michael Kimwele, Waweru Mwangi, Stephen Kimani

54 – 63 Image Recognition With the Help of Auto-Associative Neural Network
Moumi Pandit, Mousumi Gupta

64-71 A Novel Mathematical Based Method for Generating Virtual Samples from a Frontal 2D Face Image for Single Training Sample Face Recognition
Reza Ebrahimpour, Masoom Nazari, Mehdi Azizi, Mahdieh Rezvan

72-84 Authentication and Authorization Models
More V.N

85-97 Security Model for Hierarchical Clustered Wireless Sensor Networks
Kalpana Sharma, S. K. Ghosh, M.K. Ghose

98-106 Security Architecture for On-Line Mutual Funds Trading With Multiple Mobile Agents
Nirmala C R, V.Ramaswamy

107-117 ID-Based Directed Multi-Proxy Signature Scheme from Bilinear Pairings
B.Umaprasada Rao, P.Vasudeva Reddy

118-131 Systematic Digital Forensic Investigation Model
Ankit Agarwal, Saurabh Gupta, Subhash Chand, Megha Gupta

132-142 Secure E-Commerce Protocol
Khalid Haseeb, Muhammad Arshad, Shoukat Ali, Shazia Yasin

143-155 Diacritic Oriented Arabic Information Retrieval System
Khalid Saleh Aloufi

156-167 An Ant Algorithm for Solving QoS Multicast Routing Problem
Ahmed Younes Hamed

Stream Processing Environmental Applications in Jordan Valley

Iyad Aldasouqi iyad@rss.gov.jo
Information Technology Center
Royal Scientific Society

Jalal Atoum atoum@psut.edu.jo
Princess Sumaya University for Technology
The King Hussein School for Information Technology

Abstract

Database system architectures have been gone through innovative changes, specially the unifications of algorithms and data via the integration of programming languages with the database system. Such an innovative changes is needed in Stream-based applications since they have different requirements for the principal of stream data processing system. For example, the monitoring component requires query processing system to detect user-defined events in a timely manner as in real time monitoring system. Furthermore, stream processing fits a large class of new applications for which conventional DBMSs fall short since many stream-oriented systems are inherently geographically distributed and the distribution offers a scalable load management and higher availability.

This paper presents statistical information about metrological data such as the weather, soil and evapotranspiration as collected by the weather stations distributed in different locations in Jordan Valley. In addition, it shows the importance of Stream Processing in some real life applications, and shows how the database systems can help researcher in building prototypes that can be implemented and used in a continuous monitoring system.

Keywords: Stream Processing, Environment Metrological Data, Sensors.

1. INTRODUCTION

Data is increasingly generated by instruments that monitor the different types of sensors, which can be used to run a machine or represent the core of other machines as in environment monitoring, medical applications and others. Not only that, but web features have become as necessity for many applications in order to support remote access facilities. This has huge implications for how applications would be structured. Also, DBMSs are now considered as object containers, where Queues are the first objects to be added, since they are the basis for transaction processing and workflow applications. Therefore, database systems should consider that new techniques in XML and xQuery will be the main data structure and access pattern as most of programming experts believe [1].

Monitoring applications enable users to continuously observe the current state of a system, and receive alerts when interesting combinations of events occur. Monitoring applications exist in various domains, such as sensor-based environment monitoring (e.g., air quality monitoring, car-traffic monitoring), military applications (e.g., target detection, platoon tracking), network monitoring (e.g., intrusion detection), and computer-system monitoring [2]. Although for a comparison purpose of historical data, stream processing operators are being added to the DBMS; as a result of the size of the database become larger and larger and the increased amount of external data arrival as streams. Since the incoming data is compared against millions of queries rather than queries searching millions of records, the need for huge main memories and sequential disk access have become a necessity. Therefore, Database systems are now expected to be self-managing, self-healing, and always running.

Stream Processing Engines (SPEs) known as Stream-Base [3], stream databases [4] or data stream managers [5], [6] have emerged as new classes of software systems that enable low latency processing of streams of data arriving at high rate. SPEs continuous query processors [7], complex event processing engines, or event stream processors [8] are also software systems that handle data processing requirements of monitoring applications. In these systems, an application-logic takes the form of a dataflow composed of a relatively small set of operators (e.g., filters, aggregates, and correlations). In addition, a new class of data intensive applications may be defined, in which these applications require a continuous and low latency processing of large volumes of information that “stream in” from data sources at high rates. Also, stream processing applications have emerged in several different domains motivated by different needs [9]. Moreover, stream processing run a continuous query processing, in which the Naïve approach uses every new arrival of data item to evaluate all registered continuous queries. If the data satisfies all predicates of the continuous queries, then the result of these queries will be sent to the interested users [10].

Figure 1 illustrates an example of distributed SPEs that performs a computation spread across four nodes. When a stream goes from one node to another, the nodes are called upstream and downstream neighbors respectively [11]. The upstream nodes receive the raw data from sources for a preprocessing stage. Whereas, the downstream nodes process the user queries based on the output the upstream nodes. In Figure 1, Node1 and Node2 are upstream neighbors for the downstream nodes Node3 and Node4. [11]

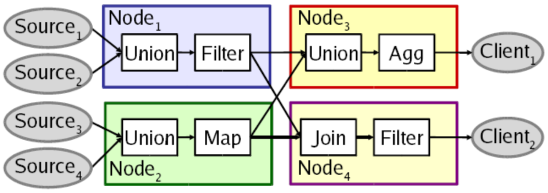


FIGURE 1: An example of distributed SPEs Query diagram.

2. DESIGN CONSIDERATIONS

In every design of SPEs there are some issues that should be considered such as: communication, computation, dynamic adaptation and flexibility. A brief discussion of each of these considerations is presented next.

Communication: This issue is very related to the sensors themselves; since the sensors varies in operation modes, some of them are wireless and battery operated, others are connected directly to the Internet or remotely connected. The operation modes constraints have an affect on the communication resource usage. A key design goal for Task-Cruncher is thus to minimize the redundancy in communication. If data requests from multiple applications have similar temporal characteristics, the sensors should send the minimum amount of data that satisfies all application requests [12].

Computation: This task should be performed at the main servers that are responsible for gathering data from several sensors to do some indexing and calculations in order to make it available for applications and their queries. The large number of sensors and applications to be served imply that the server resource usage per sensor and per task on online data streams cannot be very high. As the number of tasks increases, it is no longer efficient to perform the aggregation required by multiple applications in isolation. For instance, two wireless cameras might be imaging a scene and many applications’ requests this panoramic image that would be generated by stitching the images from these two cameras. Clearly, if the server can detect that more than one application has requested the result of the same computation, then the panoramic image generated from this computation would be stitched only once per frame. Then, the stitched generated image is sent to all the requesting applications.

Dynamic Adaptation: This issue arises when different applications and queries are running using the shared sensors.

Flexibility: This issue arises when different types of computations are occurring at the same time (overlapping). For instance, many primitive operations in sensing tasks can occur concurrently in which both distributive and algebraic operations (such as Sum, Max, Average, etc.) are used. In this case, the final result would be computed from partial results over disjoint partitions of input values.

3. ENVIRONMENT MONITORING

Prototypes for monitoring the health of natural environments [13, 14] have been proposed and developed. Previous work [15] in environmental monitoring has generated efficient protocols and improved the communication between different locations. By combining data from different weather stations (sensor networks) [16, 17] as in Figure 2, and from location-sensing devices [18, 19] can be used to determine the location of each station. Sensor data could come from wireless sources, then stored in a temporary storage device in order to be collected manually or automatically by the network administrator. More complex processing of wide-spread streams could occur at wired, stable nodes (land line telephone and modem), or wireless via GSM line and modem. After the data is collected, a Data Collection Network (DCN) should be constructed as a robust infrastructure for discovery, querying, and delivery of weather station data. In addition, a DCN should be assembled to scale up to a large number of concurrent applications for pulling data from a vast number of weather stations. This process is carried out using an Internet-based overlay network in which the nodes act as both routers and stream processing engines, as in LoggerNet software [16]. LoggerNet is configured to save the data at a certain directory on a PC or on a server. This process can also be called “store-then-process” as in traditional DBMSs (such as Oracle, IBM DB2, and Microsoft SQL Server). This process is designed to support such traditional types of applications; since it is inadequate for high-rate and low-latency stream processing. Furthermore, there is a need to develop some mechanisms to allow streaming applications to interact with databases without introducing significant computational overhead that could affect the performance of the processing of streaming data [20].

FIGURE2: Sample of weather stations in Jordan

Data sources as illustrated in Figure 3 are continuously producing streams of information. These streams are then continuously processed and the results are pushed to client applications [21]. In order to understand any type of application, the properties of that application should be easy to understand. In order to achieve such properties of any application, the following features of a stream processing should be satisfied [22]:

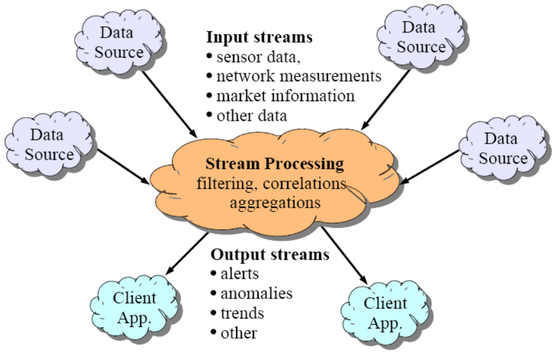


FIGURE 3: High-level view of stream

1. *A continuous-query processing model*: In a traditional DBMS, clients issue one-time queries against stored data (e.g., "Did any source attempt more than 100 connections within a one minute period?"). In a stream processing application, clients submit long duration monitoring queries that must be processed continuously as new input data arrives (e.g., "Alert me if a source attempts more than 100 connections within a one minute period"). Clients submitting continuous queries expect periodic results or alerts when specific combinations of inputs occur.
2. *A push-based processing model*: In a stream processing application, one or more data sources (e.g., sensor networks, ticker feeds, network monitors) continuously produce information and push the data to the system for processing. Client applications passively wait for the system to push them periodic results or alerts. This processing model contrasts with the traditional model, where the DBMS processes locally stored data, and clients actively pull information about the data when they need it.
3. *Low latency processing*: Many stream processing applications monitor ongoing phenomena and require low latency processing of input data. For instance, in a network monitoring, current information about ongoing intrusions is more valuable than stale information about earlier attacks. SPEs strive to provide low-latency processing but do not make any hard guarantees.
4. *High and variable input data rates*: In many stream processing applications, data sources produce large volumes of data. Input data rates may also vary greatly. For instance, a denial of service (DoS) attack may cause large numbers of connections to be initiated. If network monitors produce one data item per connection, the data rates on the streams they produce will increase during the attack. As the data rates vary, the load on an SPE also varies because query operators process data arriving at a higher rate.

In addition, a typical streaming environment has a large number of concurrent overlapping continuous queries. Sharing the query execution is a primary task for query optimizers to address scalability. The current efforts for shared query execution focus on sharing execution at the operator level [21]. Examples of such efforts are covered in the "Monitoring Continuous Queries over Streaming Locations" [23], and in the "Challenges in Dependable Internet-Scale Stream Processing" [24].

4. RELATED WORK

There are some current projects that focus on stream data processing such as the NIAGARA system [25] that proposes architecture for Continuous Queries (CQs) with group optimization techniques. The Fjord [26] project has an architecture which supports both a continuous data stream and a traditional static data set by connecting the push-based operators with the pull-based operators via queues. The STREAM [27] project is trying to build a general data processing architecture that can support the functionalities of both database management system (DBMS) and data stream management system (DSMS). Finally, the Aurora system [28] presents an architecture to process data streams with some Quality of Service (QoS) requirements by decoupling a CQ into a few predefined operators.

5. CURRENT SP APPLICATION IN JORDAN

This section presents the experience of the data stream processing application called the Irrigation Management Information System (IMIS) conducted by the National Center for Agricultural Research and Extension (NCARE) in Jordan [29].

This application is a package that can provide irrigation personnel (farmers) with real time estimates of irrigation requirements and scheduling. In addition, this application helps to initiate and sustain a technology transfer program concerning the issues of when and how much water is needed to irrigate in order to maximize the usage of water efficiently.

In general, the purpose of environmental projects is to evaluate the spatial variability of water consumption of irrigated agriculture under limited water resources conditions.

The objectives of the IMIS project are to: [30]

1- Establish an IMIS based on real time meteorological data, soil characteristics, water quality, crop type, and current irrigation system efficiently.
2- Develop an infrastructure and information management tools for rapid and accurate dissemination of irrigation scheduling information.
3- Adopt state-of-the-art models for predicting crop irrigation requirements.
4- Establish an irrigation scheduling criteria for major crops in the Jordan valley.
5- Establish a data network that can easily be used by other relevant national institutions through improved classification of data entry, retrieval and communications.

5.1. Weather Station Components

Each station of the IMIS project consists of following components as shown in Figure 4:

- Three-meter-long tower.
- Data logger for multiple sensor inputs: This is a data acquisition card that can read analog signals and convert them into digital signals in order to read them by computer (+12, -12, +5 and -5 Volts).
- Cellular phone modem/land line.
- Battery with solar panels.
- Meteorological sensors:
  - Wind speed and direction.
  - Solar radiation.
  - Barometric pressure.
  - Temperature.
  - Relative humidity.
  - Precipitation.
- Soil sensors:
  - Moisture Content.
  - Temperature.

The sensors are designed for long-term installation under adverse environmental conditions. These sensors can be categorized in terms of their functionality as illustrated next:

Air Temperature Sensors: these sensors can be thermostats, thermocouples, or RTDs (as standard sensor models).

Air Temperature and Relative Humidity sensors: These are two separate sensors packaged in the same sensor housing.

Barometric pressure sensors: These sensors measure the fluctuations in the pressure exerted by the atmosphere. Such sensors require protection from condensing humidity, precipitation, and water ingress and they are typically housed within the datalogger (inside an environmental enclosure).

Evaporation Gauges: These sensors are used to determine the evaporation rate by measuring the changing water level in an evaporation pan.

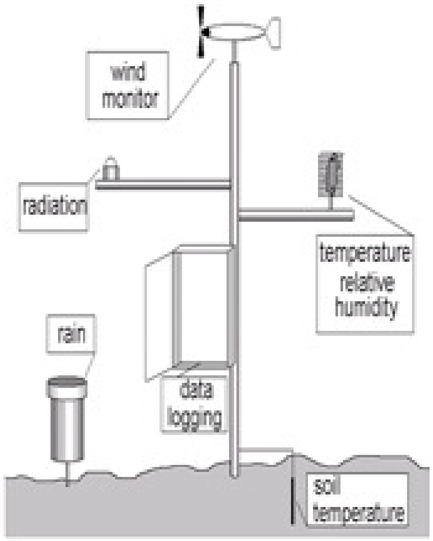


FIGURE 4: A Typical Automated Metrological Station

Leaf wetness sensors: These sensors are used to accomplish the following duties:

- Measuring the electrical resistance of a water film on the leaf surface.
- Detecting a change in a sensor length and weight.
- Appling to mock leaves and to emulate periods of leaf wetness after rainfall, dew, or spray.

Soil Temperature Sensors: These sensors can be either Thermostats, thermocouples, thermocouple wire, or averaging thermocouples.

Solar Radiation Sensors: These sensors can be pyranometers, net radiometers or quantum sensors. Such sensors are designed to measure the various aspects of the energy imparted by the sun on the Earth's surface.

Wind Speed and Wind Direction: The output of these sensors (the wind vanes and the anemometers) can be used in research project, air quality monitoring, and general purpose meteorological applications.

Data loggers and Data Acquisition Systems: These are simply Multiplexers devices that may be added to augment measurement and control capabilities that include:

- Measuring most sensors.
- Providing non-volatile data storage and on-board battery-backed clock.
- On-board data processing.
- Initiating measurement and control functions based on time or event.
- Controlling external devices such as pumps, motors, alarms, freezers, valves, etc.
- Using PC support software or keyboard/display to program.
- Operating independently of AC power, computers, and human interaction.
- Consuming minimal power from a 12 V-DC power source.
- Interfacing with on-site and telecommunication devices such as telephone modems (including cellular and voice-synthesized), short haul modems, radio transceivers, satellite transmitters, and Ethernet interfaces.
- Operating in temperature range of -25° to 50ºC.

5.2. Weather Station Benefits

The IMIS project has the following benefits as results of using automated weather stations [28]:

1. Preconfigured and custom automated weather stations.
2. Stations that can measure most commercially available meteorological sensors.

3. Communications options that do include phone, cell phone, voice-synthesized phone, satellite (DCP), and radio.
4. Stations that can operate reliably in harsh environments.
5. Data loggers that can provide an on-site statistical and mathematical capabilities.
6. Batteries and solar panels that allows long-term and remote operations.
7. Stations are easily expandable in such away that add new sites or add sensors to existing sites.
8. Powerful software that can support programming, data retrieval, and data display.

Furthermore, data are typically viewed and stored in the units of your choice (e.g., wind speed in mph, m/s, and knots). Measurement rates and data recording intervals are independently programmable, allowing calculation of 15-minute, hourly, and/or daily data values, for example, using 1-minute or 1-second measurements. Conditional outputs, such as rainfall intensity and wind gusts, can also be recorded. The program can be modified at any time to accommodate different sensor configurations or new data processing requirements. If needed, channel capacity can be expanded using multiplexers, including a model designed specifically for thermocouples [28].

5.3. System Architecture

The IMIS system architecture as shown in Figure 5 consists of the following modules:

- Weather Stations.
- Data collocation Software.
- DataBase Server.
- Firewall.
- Java application and ASP.net.

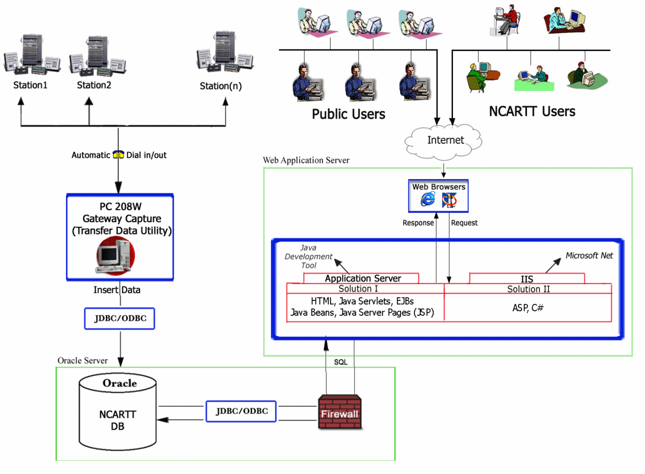


FIGURE 5: System Architecture Modules.

In this architecture, the data will be collected by the sensors (located in the weather stations) in a predefined schedule or when needed (in the data logger). A software called Loggernet, or PC2000 [16] is used to gather the data and merge it in one file (as a text file). Then, this merged data will be imported by a tool into an Oracle database serve to be used by the application server for process manipulation. Users (farmers/ researchers/ others) can access the application website to do certain types of searches (depending on their needs).

The Application server has several functions related to both the normal users and the system administrators as shown in Figure 6. Some of these functions are listed below:

- Manage the user accounts (normal users or system administrator) login process.
- Manage the time and the way of importing data from the stations.
- Manage stations (Add/Delete/Modify).
- Manage countries (Add/Delete/Modify), since many countries may participates in this project (future works).

- Manage parameters (add/delete) new sensors.

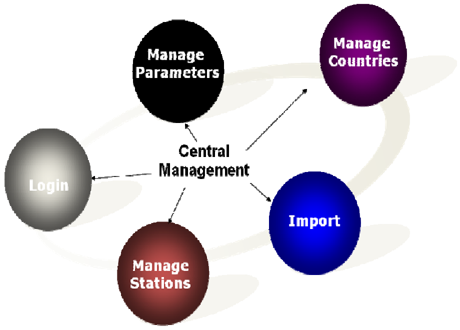


FIGURE 6: Application server functions

Users of the IMIS system would be able to do any of the following functions:

- Display General Information.
- Search and Generate Statistics and reports from the weather stations readings (daily, monthly, yearly .etc).
- Calculate Irrigation Requirements.
- Calculate Chilling Requirements.
- Display Information about weather stations.

Whereas, the administrator would be able to do any of the above function in addition to the following:

- Admin Users Management.
- Stations Management.
- Crops Management.
- Raw Data Management.
- Web Site Statistics.
- Weather station Management.

5.4. IMIS Generated information

The IMIS system would be able to generate various useful information needed by end users. For example, the Irrigation water requirements are based on real metrological data form automated weather stations that are distributed all over Jordan. Data are being collected on a hourly basis; results are submitted on a daily basis. To calculate the EvaporTanspiration (ET), the Modified Penman-Monthieth equation (eq. 1) is used [30]. For more details on the derivation of this equation refer to Monteith and Unsworth [31] and to Campbell [32].

$$ET_O = \frac{\Delta(R_n - G)}{\lambda(\Delta + \gamma^*)} + \frac{\gamma^* M_W (e_a - e_d)}{R\Theta r_v (\Delta + \gamma^*)} \qquad \text{Eq. 1}$$

Where:

ETo: Potential evaporation (kg m-2 s-1 or mm s-1).
Rn: Net Radiation (kW m-2).
G: Soil heat flux density (k W m-2).
Mw: Molecular mass of water (0.018kg mol-1).
R: Gas constant (8.13 X 10-3 kJ mol-1 K-1).
Θ: Kelvin temperature (293K).
ea-ed: Vapor pressure deficit of the air (kPa).
λ: Latent heat of vaporization of water (2450 kJ kg-1).
rv: Canopy plus boundary layers resistance for vapor (s m-1).
Δ: Slope of the saturation vapor pressure function (Pa oC-1).
γ*: Apparent psychrometer constant (Pa oC-1).

Furthermore, users of the IMIS system can get more benefits from the data generated from the stations in computing other useful information such as (Pipes Pressure and Smooth Flow in Pipes) using the formulas presented in equations eq. 2 through 5 respectively [33, 34, 35].
For example, the Darcy-Weisbach Formula (as illustrated in equation eq.2) is used for the analysis of pressure in pipe systems and it can be applied readily to open channel flow systems:

$$h_f = f\left(\frac{L}{D}\right)\frac{V^2}{2g} \qquad \text{Eq. 2}$$

Directly used Formula:

$$h_f = 1.21x10^{10}\left(\frac{Q}{C}\right)^{1.852}\left(D^{-4.871}\right)L \qquad \text{Eq. 3}$$

The smooth flow in pipes is measured by the Hazen Williams Formula (equations eq. 4 and eq.5) in SI units:

$$V = 0.85C_{HW}R_H^{0.63}S^{0.54} \qquad \text{Eq. 4}$$

Manning Formula:

$$V = \frac{1}{n}R_H^{2/3}S^{1/2} \qquad \text{Eq. 5}$$

Hence, IMIS system can be considered as a source of knowledge for users since the results can be customized depending on their needs. Furthermore, the Short Message Services (SMSs) of Mobile phones have recently been added to the IMIS to enable the farmers/users to send requests via an SMS messages to ask for a certain type of information. As a result the IMIS system helps the researchers, the farmers, the experts and even the students in both the research and a real work fields.

5.5 Development Stages

The IMIS system development is done via several stages. The first stage is the understanding of the type of data generated from the weather stations. In the second stage a site visit is required to understand the communications between the stations and the application server. In the third stage a meeting with system owners should be carried out in order to understand their requirements and to get more information about what types of information is needed. In the fourth stage the application developer will build use cases depending on collected information to be discussed with the customers in order to get their feedback. After the application is being developed the users can start requesting information/data as explained in section 5.4.

6. CONCLUSION AND FUTURE WORK

The restructuring of database systems to be used as web services and to integrate them with language runtimes have guided the researchers to establish what is known as Stream Processing. Stream Processing allows researchers and entrepreneurs to add new algorithms and other subsystems to the DBMS. Databases are evolving from SQL-engines to data integrators and mediators that provide a transactional and non-procedural access to data in various forms.

Fortunately, most innovations in database systems are traced back to the research prototypes that had been implemented after being published in research papers. Stream Processing of a continuous monitoring system is an example of such innovations. In such a system, we get the benefits and challenges of integrating history into this continuous monitoring system. IMIS idea came after long years of research and several experiments done by collaborative efforts of local and international researchers.

There are many beneficiaries from this IMIS project:

- Planners: Water allocation will be done on more robotic bases, and supply demand policy will be formulated.
- Water Sector: Increase water use efficiency in agriculture which will allow releasing water to other pressing needs.
- Agricultural Sector: Increase crop production by increasing the water use efficiently.
- Farmers: Reduction of cost which is translated to a higher return.
- National Economy:
  - Increase national income by increasing the irrigated area as a result of improving irrigation management efficiently.
  - Improve and sustain the agricultural system which will stabilize the social life of farmers in the Jordan Valley.
- Environment:
  - Minimizing hazard pollution through good irrigation management practices, and minimum use of fertilizers.
  - Expansion of irrigated areas through saving water.
  - Improvement of water quality (surface, drainage, and ground water) by implementing fertilization and other appropriate agriculture practices.

As a future work, the system can be used as an early warning system for farmers, especially during the winter when temperature goes down below zero. Also other related sensors can be added into these stations such as sensors to monitor the amount of chemical materials in the air or the soil, and other sensors may be added such as radio logical sensors to measure the radiation around the areas of the stations.

7. ACKNOWLEDGMENT

Thanks for the Information Technology Center at the Royal Scientific Society and to the National Center for Agricultural Research and Extension at Ministry of Agriculture-Jordan for their support and cooperation.

8. REFERENCES

1. **FOR WEBSITE:** *Next The Database Revolution Jim Gray Microsoft 455 Market St. #1650 San Francisco, CA, 94105 USA http://research.microsoft.com/~Gray Gray@Microsoft.com*

2. **FOR JOURNALS:** *Magdalena Balazinska, YongChul Kwon, Nathan Kuchta, and Dennis Lee, Moirae: History-Enhanced Monitoring, Third Biennial Conference on Innovative Data Systems Research CA, USA, January 7-10, 2007, pp 375-386, Online Proceedings 2007 (CIDR 2007).*

3. **FOR CONFERENCES:** *Abadi, D. J., Ahmad, Y., Balazinska, M., C¸ etintemel, U., Cherniack, M., Hwang, J.-H., Lindner, W., Maskey, A. S., Rasin, A., Ryvkina, E., Tatbul, N., Xing, Y., and Zdonik, S. The design of the Borealis stream processing engine. In 2nd Biennial Conference on Innovative Data Systems Research (CIDR'05) (2005), pp. 277-289. Key: citeulike:1681216.*

4. **FOR CONFERENCES:** *Cranor, C., Johnson, T., Shkapenyuk, V., and Spatscheck, O. 2003. Gigascope: A stream database for network applications. In ACM, SIGMOD (2003), pp. 647-651. Key: citeulike:4014029*

5. **FOR JOURNALS:** *Abadi, D. J., Carney, D., C¸ etintemel, U., Cherniack, M., Convey, C., Lee, S., Stonebraker, M., Tatbul, N., and Zdonik, S. Aurora: A new model and architecture for data stream management. VLDB Journal, Volume 12 Issue 2, August 2003.*

6. **FOR JOURNALS:** *Rajeev Motwani, Jennifer Widom, Arvind Arasu, Brian Babcock, Shivnath Babu, Mayur Datar, Gurmeet Singh Manku, Chris Olston, Justin Rosenstein, and Rohit Varma. Query processing, approximation, and resource management in a data stream management system. In Proc. of First Biennial Conference on Innovative Data Systems Research, January 5-8, 2003, Asilomar, CA, USA, 2003.*

7. **FOR CONFERENCES:** *Chandrasekaran, S., Cooper, O., Deshpande, A., Franklin, M. J., Hellerstein, J. M.,Hong, W., Krishnamurthy, S., Madden, S., Raman, V., Reiss, F., and Shah, M. . TelegraphCQ: Continuous dataflow processing for an uncertain world. The First Biennial Conference on Innovative Data Systems Research (CIDR), Asilomar, USA, 2003.*

8. **FOR WORKSHOP:** *C. Koulamas, A. Prayati, G. Papadopoulos, A Framework for the Implementation of Adaptive Streaming Systems, Proceedings of the 3rd ACM workshop on Wireless multimedia networking and performance modeling , WMuNeP'2007. pp.23-26 ,2007*

9. **FOR THESIS:** *Magdalena Balazinska, Fault-Tolerance and Load Management in a Distributed Stream Processing System, Doctoral Dissertation, ACM, (p. 187-199), December 2005*

10. **FOR CONFERENCES:** *Yongxu Piao, Wooseok Ryu, Haipeng Zhang, Bonghee Hong, Optimization of Continuous Query Processing for RFID Sensor Tag Data Stream, Proceeding ICIS '09 Proceedings of the 2nd International Conference on Interaction Sciences: Information Technology, Culture and Human, ISBN: 978-1-60558-710-3, pages 586-591, 2009.*

11. **FOR JOURNALS:** *Magdalena Balazinska, Hari Balakrishnan, Samuel R. Madden, And Michael Stonebraker, Fault-Tolerance in the Borealis Distributed Stream Processing System, Journal, ACM Transactions on Database Systems (TODS), Volume 33 Issue 1, pp. 3:1--3:44, March 2008.*

12. **FOR CONFERENCES:** *Arsalan Tavakoli, Aman Kansal and Suman Nath, On-line Sensing Task Optimization for Shared Sensors, IPSN '10 Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks, pages 47-57, ISBN: 978-1-60558-988-6, 2010.*

13. **FOR CONFERENCES:** *Hailiang Mei, Smart Distribution of Bio-signal Processing Tasks in M-Health, In: On the Move to Meaningful Internet Systems 2007: OTM 2007 Workshops, pp 284-293, 25-30 Nov 2007, Vilamoura, Portugal.*

14. **FOR WORKSHOP:** *A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler, and J.Anderson.Wireless Sensor Networks for Habitat Monitoring. In ACM International Workshop on Wireless Sensor Networks and Applications (WSNA'02), Atlanta, GA, pages 88 – 97, ISBN: 1-58113-589-0, Sept. 2002.*

15. **FOR UNIVERSITY:** *Wisconsin K-12 Forestry Education Program, Wisconsin Center for Environmental Education, College of Natural Resources, University of Wisconsin Stevens Point*
http://www.uwsp.edu/cnr/wcee/programs.htm

16. **FOR WEBSITE:** *http://www.campbellsci.com/weather-climate*

17. **FOR WEBSITE:** *Crossbow Technology. Products: Wireless sensor networks. http://www.xbow.com/Products/Wireless_Sensor_Networks.htm.*

18. **FOR JOURNALS:** *Quinn Hart, Michael Gertz, Optimization of Multiple Continuous Queries over Streaming Satellite Data, GIS '06 Proceedings of the 14th annual ACM international symposium on Advances in geographic information systems, pages 243 – 250, ISBN: 1-59593-529-0, 2006.*

19. **FOR WEBSITE:***M. Hapner, R. Burridge, R. Sharma, J. Fialli, and K. Stout. Java Message Service Specification Version 1.1. Sun Microsystems, Inc., April 2002. http://java.sun.com/products/jms/.*

20. **FOR CONFERENCES:** *Daby Sow, Alain Biem, Marion Blount, Maria Ebling, Olivier Verscheure, Body Sensor Data Processing using Stream Computing, MIR '10 Proceedings of the international conference on Multimedia information retrieval, pages 449-458, ISBN: 978-1-60558-815-5, 2010.*

21. **FOR JOURNALS:** *Thanaa M. Ghanem, Ahmed K. Elmagarmid, Perake Larson Walid G. Aref, Supporting Views in Data Stream Management Systems, Journal, ACM Transactions on Database Systems (TODS),Volume 35 Issue 1, Article No.1, pp 1:1--1:47, February 2010.*

22. **FOR JOURNALS:** *Hari Balakrishnan, Magdalena Balazinska, Don Carney, U˘gur C¸ etintemel, Mitch Cherniack, Christian Convey, Eddie Galvez, Jon Salz, Michael Stonebraker, Nesime Tatbul, Richard Tibbets, and Stan Zdonik. Retrospective on Aurora. VLDB Journal, 13(4), pp. 370-383, December 2004.*

23. **FOR CONFERENCES:** *Kostas Patroumpas, Evi Kefallinou, Timos Sellis, Monitoring Continuous Queries over Streaming Locations, GIS '08 Proceedings of the 16th ACM SIGSPATIAL international conference on Advances in geographic information systems, Article No.81, pp. 1-2, ISBN: 978-1-60558-323-5, 2008.*

24. **FOR CONFERENCES:** *Peter Pietzuch, Challenges in Dependable Internet-Scale Stream Processing, SDDDM '08 Proceedings of the 2nd workshop on Dependable distributed data management, pages 25-28, ISBN: 978-1-60558-121-7, 2008.*

25. **FOR CONFERENCES:** *J. Chen, D. Dewitt, F. Tian, and Y. Wang. Niagaracq: A scalable continuous query system for internet databases. ACM SIGMOD international conference on Management of data, pages 379 – 390, ISBN: 1-58113-217-4, 2000.*

26. **FOR CONFERENCES:** *S. Madden and M. J. Franklin. Fjording the stream: An architecture for queries over streaming sensor data. ICDE Proceedings of the 18th International Conference on Data Engineering, page 555, 2002.*

27. **FOR CONFERENCES:** *S. Babu and J. Widom. Continuous queries over data streams. Newsletter, ACM SIGMOD Record, Volume 30 Issue 3, September 2001.(Pages 109-120).*

28. **FOR CONFERENCES:** *D. Carney, U. Cetintemel, et al. Monitoring streams - a new class of data management applications. VLDB '02 Proceedings of the 28th international conference on Very Large Data Bases, pages 215 - 226 Sept. 2002.*

29. **FOR WEBSITE:** *http://www.ncare.gov.jo/*

30. **FOR WEBSITE:** *http://imis.ncare.gov.jo/ncartt/index.html*

31. **FOR BOOKS:** *Monteith, J.L., and M.H. Unsworth, 1990. Principles of environmental physics, 2nd ed. Edward Arnold, London, United Kingdom.*

32. **FOR BOOKS:** *Campbell, G. S. 1977, A Introduction to Environmental Biophysics. Springer-Verlag, New York, New York, pp 159.*

33. **FOR BOOKS:** *Crane Technical Paper No. 410, Flow of Fluids Through Valves, Fittings, and Pipe. Crane Co., Signal Hill CA, 1988.*

34. **FOR BOOKS:** *Hickey Harry E., Hydraulics for Fire Protection, National Fire Protection Association, Quincy MA, 1980.*

35. **FOR BOOKS:** *Wass Harold S., Sprinkler Hydraulics and What it's all about, 2nd edition, Society of Fire Protection Engineers, Bethesda MD, April 2000.*

Development of Predictor for Sequence Derived Features from Amino Acid Sequence using Associate Rule Mining

Manpreet Singh mpreet78@yahoo.com
Department of Information Technology
Guru Nanak Dev Engineering College
Ludhiana, Punjab, India - 141006

Gurvinder Singh gsbawa71@yahoo.com
Department of Computer Science and Engineering
Guru Nanak Dev University
Amritsar, Punjab, India

Abstract

Drug Discovery process include target identification i.e. to identify a target protein whose inhibition can destroy the pathogen. In testing phase, clinical and pre-clinical trials are done on the animals and then on humans. After the discovery process, the drug or medicine is made available for public use. But if the testing of the drug is ineffective or unable to yield the appropriate results, then the whole process need to be repeated. This makes the first stage of drug discovery the most important than the other stages. The present work will assist in the process of drug discovery.

The present work involves the development of a model that extracts the sequence derived features from the given amino acid sequence using associative rule mining. Associative rule mining is a data mining technique useful to identify related items and to develop rules. In the present work, various parameters of the amino acid sequence are studied that affect the sequence-derived features and some of the equations and algorithms are implemented. Input is given through text file and collective results are obtained. MATLAB environment is used for the implementation. The results are compared with the previous bioinformatics tools. The model developed assists in protein class prediction process which assists drug discoverers in the drug discovery process.

Keywords: Drug Discovery, Associative Rule Mining, Amino Acid, Sequence Derived Features.

1. ASSOCIATIVE RULE MINING

Association rule mining is a common data mining technique, which can be used to produce interesting patterns or rules [2]. Association rule mining involves counting frequent patterns (or associations) in large databases, reporting all that exist above a minimum frequency threshold known as the ‘support’ e.g. analyzing supermarket basket data, where a supermarket would want to see which products are frequently bought together. Such an association might be “if a customer buys biscuits and patty then they are 80% likely to buy coffee”. Rule support and confidence are two measures of rule interestingness. Association rules are considered interesting if they satisfy both a minimum support threshold and a minimum confidence threshold [5].

1.1 Association Rules

Association rules are required to satisfy a user-specified minimum support and a user-specified minimum confidence at the same time. To achieve this, association rule generation is a two-step process. First, minimum support is applied to find all frequent itemsets in a database. In a second step, these frequent itemsets and the minimum confidence constraint are used to form rules. While the second step is straight forward, the first step needs more attention. The problem is defined as: Let I be a set of n binary attributes called items. Let D be a set of transactions called the database. Each transaction in D has a unique transaction ID and contains a subset of the items in I. A rule is defined as an implication of the form where X, Y C I and X ∩Y= θ. The sets of items (for short item sets) X and Y are called antecedent (left-hand-side or LHS) and consequent (right-hand-side or RHS) of the rule.

Finding all frequent itemsets in a database is difficult since it involves searching all possible itemsets (item combinations). The set of possible itemsets is the power set over I and has size 2n – 1 (excluding the empty set which is not a valid itemset). Although the size of the powerset grows exponentially in the number of items n in I, efficient search is possible using the downward-closure property of support (also called anti-monotonicity) which guarantees that for a frequent itemset also all its subsets are frequent and thus for an infrequent itemset, all its supersets must be infrequent [13][16].

2. PROTEIN AND PROTEIN FUNCTIONS

Proteins are large, complex molecules that play many critical roles in the body. They do most of the work in cells and are required for the structure, function and regulation of the body's tissues and organs.

Proteins are made up of hundreds or thousands of smaller units called amino acids, which are attached to one another in long chains. There are 20 different types of amino acids that can be combined to make a protein. The sequence of amino acids determines each protein's unique 3-dimensional structure and its specific function [6-8].

As amino acids band together in chains to form the stuff from which our life is born. It's a two-step process: Amino acids get together and form peptides or polypeptides. It is from these groupings that proteins are made. Commonly recognized amino acids include glutamine, glycine, phenylalanine, tryptophan, and valine. Three of those — phenylalanine, tryptophan, and valine — are essential amino acids for humans; the others are isoleucine, leucine, lysine, methionine, and threonine. The essential amino acids cannot be synthesized by the body; instead, they must be ingested through food.

They serve as enzymatic catalysts, are used as transport molecules (hemoglobin transports oxygen) and storage molecules (iron is stored in the liver as a complex with the protein ferritin), they are used in movement (proteins are the major component of muscles), they are needed for mechanical support (skin and bone contain collagen-a fibrous protein), they mediate cell responses (rhodopsin is a protein in the eye which is used for vision), antibody proteins are needed for immune protection; control of growth and cell differentiation uses proteins (hormones) [4].

3. SEQUENCE DERIVED FEATURES

Sequence derived features are the various features of protein which are used to predict protein class. Sequence derived features are very important in protein class prediction as these are the input to the HPF predictor. SDF's can be derived from a given set of amino-acid (protein) sequences using various web-based bioinformatics tools [12]. The various sequence derived features are as given below:

3.1 Extinction Coefficient (Eprotein)

Extinction Coefficient is a protein parameter that is commonly used in the laboratory for determining the protein concentration in a solution by spectrophotometry. It describes to what extent light is absorbed by the protein and depends upon the protein size and composition as well as the wavelength of the light. For proteins measured in water at wavelength of 280nm, the value of the Extinction coefficient can be determined from the composition of Tyrosine, Tryptophan and Cystine.

Mathematically:

$$Eprotein = Ntyr * Etyr + Ntrp * Etrp + Ncys * Ecys \qquad (1)$$

Where Etyr=1490, Etrp =5500, Ecys =125 are the Extinction coefficients of the individual amino acid residues.

3.2 Absorbance (Optical Density)

For proteins measured in water at wavelength of 280nm the absorbance can be determined by the ratio of Extinction coefficient and the molecular weight of the protein. It is a representation of a material's light blocking ability.

Mathematically:

$$\text{Absorbance} = \text{Eprotein} / \text{Molecular Weight} \qquad (2)$$

3.3 Number of Negatively Charged Residues (Nneg)

This can be calculated from the composition of Aspartic acid and Glutamic acid.

3.4 Number of Positively Charged Residues (Npos)

This can be calculated from the composition of ARginine and Lysine.

3.5 Aliphatic Index (AI)

The aliphatic index of a protein is defined as the relative volume occupied by aliphatic side chains (alanine, valine, isoleucine, and leucine). It may be regarded as a positive factor for the increase of thermostability of globular.

Mathematically:

$$AI = Xala + a * Xval + b * (Xile + Xleu) \qquad (3)$$

Where Xala , Xval , Xile and Xleu are the mole percentages of alanine, valine, isoleucine and leucine respectively. Coefficients a and b are the relative volume of valine side chain and of leu/ile side chains to the side chain of alanine i.e. a = 2.9 and b = 3.9.

3.6 Compute IP/mol weight

It calculates the isoelectric point by molecular weight of the input amino acid sequence. IP stands for isoelectric point of the input amino acid sequence. Mol weight stands for molecular weight of the input amio acid sequence.

4. LITERATURE SURVEY

Jensen et al. (2002) proposed the human protein function from post-translational modifications and localization features. The prediction method involved the use of sequence derived features for human protein function prediction. The posttranslational modifications (PTMs) are the changes that occur to the protein after its production by the process of translation. They extracted the sequence derived features from the different servers like Expasy, PSORT as discussed in section 5. Fourteen features were extracted from the amino acid sequences [6].

Al-Shahib et al. (2007)

Calculated the frequency, total number of each amino acid and the set of amino acids for the input protein seqnence. To encode distributional features, they also determined the number and size of continuous stretches of each amino acid or amino acid set. They subdivided every protein into four equally sized fragments and calculated the same feature values for each fragment and combination of fragments. In addition, the other features like the secondary structure was predicted using Prof [10], the position of putative transmembrane helices using TMHMM [21] and of disordered regions using DisEMBL [15]. The features were used for protein function prediction [1].

Kanakubo et al. (2007)

Stated that association rule mining was one of the most important issues in data mining. With Apriori methods, the problem becomes incomputable when the total number of items are large. On the other hand, bottom-up approaches such as artificial life approaches were opposite of the top-down approaches of searches covering all transactions and may provide new methods of breaking away from the completeness of searches in conventional algorithms. Here, an artificial life data mining technique was proposed in which one transaction was considered as one individual and association rules were accumulated by the interaction of randomly selected individuals. The proposed algorithm was compared to other methods in application to a large scale actual dataset and it was verified that its performance was greatly superior to that of the method using transaction data virtually divided and that of apriori method by sampling approach, thus demonstrating its usefulness [9].

Gupta et al. (2008)
Proposed a novel feature vector based on physicochemical property of amino acids for prediction protein structural classes. They presented a wavelet-based time-series technique for extracting features from mapped amino acid sequence and a fixed length feature vector for classification is constructed. Wavelet transform is a technique that decomposes a signal into several groups (vectors) of coefficients. Different coefficient vectors contain information about characteristics of the sequence at different scales. The proposed feature vector contains information about the variability of ten physiochemical properties of protein sequences over different scales. The variability of physiochemical properties was represented in terms of wavelet variance [14].

Jaiswal et al. (2011)
Studied that the identification of specific target proteins for any diseased condition involves extensive characterization of the potentially involved proteins. Members of a protein family demonstrating comparable features may show certain unusual features when implicated in a pathological condition. They studied the Human matrix metalloproteinase (MMP) family of endopeptidases and discovered their role in various pathological conditions such as arthritis, atherosclerosis, cancer, liver fibrosis, cardio-vascular and neurodegenerative disorders, little is known about the specific involvement of members of the large MMP family in diseases. They hypothesized that cysteine rich and highly thermostable MMPs might be key players in diseased conditions and hence signify the importance of sequence derived features [3].

5. FEATURE EXTRACTION TOOLS

There are various Bioinformatics Tools for obtaining Sequence derived features (SDFs) [11]. These are as follows:

5.1 NetNGlyc 1.0 Server

It predicts N-Glycosylation sites in human proteins using artificial neural networks that examine the sequence context of Asn-Xaa-ser/Thr sequins [18].

5.2 PSORT Server

It is a computer program for the prediction of protein localization sites in cells. It receives the information of an amino acid sequence and its source origin e.g. Gram-negative bacteria, as inputs. Then, it analyzes the input sequence by applying the stored rules for various sequence features of known protein sorting signals. Finally, it reports the possibility for the input protein to be localized at each candidate site with additional information [23].

5.3 TMHMM Server

It is a program for predicting transmembrane helices based on a hidden Markov model. It reads a FASTA formatted protein sequence and predicts locations of transmembrane, intracellular and extracellular regions. (http://www.cbs.dtu.dk/services/TMHMM/) [21].

5.4 NetOGlyc Server

It produces neural network predictions of mucin type GalNAc O-Glycosylation sites in mammalian proteins [19].

5.5 Signal-P server

It predicts the presence and location of signal peptide cleavage sites in amino acid sequences from different organisms: Gram-positive prokaryotes, Gram-negative prokaryotes, and eukaryotes. The method incorporates a prediction of cleavage sites and a signal peptide/non-signal peptide prediction based on a combination of several artificial neural networks and hidden Markov models [20].

5.6 Expasy Server

It computes various physico-chemical properties of protein like iso-electric point, extinction coefficient, optical density etc [22].

5.7 PROFEAT

It is a web server for computing commonly-used structural and physicochemical features of proteins and peptides from amino acid sequence. It includes amino acid composition and dipeptide composition, normalized Moreau–Broto autocorrelation, Moran autocorrelation and Geary autocorrelation, composition, transition and distribution, sequence-order-coupling number, quasi-sequence-order [17].

6. ALGORITHM FOR PREDICTING SEQUENCE DERIVED FEATURES

Among various Sequence derived features are Extinction Coefficient, Aliphatic Index, Absorbance, No. of negatively charged residues, No. of positively charged residues, Compute Iso-electric point/molecular weight. These SDF's are integrated and computed in one platform using Associative rule mining.

In the existing techniques the various categories of features were not computed for the same input by any single tool rather different tools are available for different categories as discussed in section 5. The methods for extracting multiple features of relevant to the density of the amino acids were also developed [1][14]. The present work focuses on developing the single tool for extracting the features of multiple categories from the single input file. The algorithm predicts the Extinction Coefficient, Aliphatic Index, Absorbance, No. of negatively charged residues, No. of positively charged residues, Compute Iso-electric point/molecular weight from the input amino acid sequence. All these features are computed by giving single input sequence file which is type of string made from possible combinations of 20 characters representing the 20 amino acids. It is possible by integrating all these computations by using associative rule mining. The amino acid sequences may contain thousands of amino acid i.e characters in a string. Thus extracting any sequence derived feature from the sequence is a compute intensive problem. Computing multiple features from single sequence is even more herculean task. Each computation has some common part that is called the intersection. The intersection and union operations are utilized to give the integrated results from the single input file.

The different algorithms for individual feature prediction are shown here for clear interpretation. Fig. 1 shows the steps involved in Extinction Coefficient Prediction. Fig. 2 and Fig. 3 shows the algorithm for prediction of negatively charged and positively charged residues respectively. Fig. 4 shows the predictor for Iso-electric point and molecular weight for the amino acid chain. Fig. 5 shows the Aliphatic Index prediction and Fig. 6 shows the Absorbance prediction for the input file.

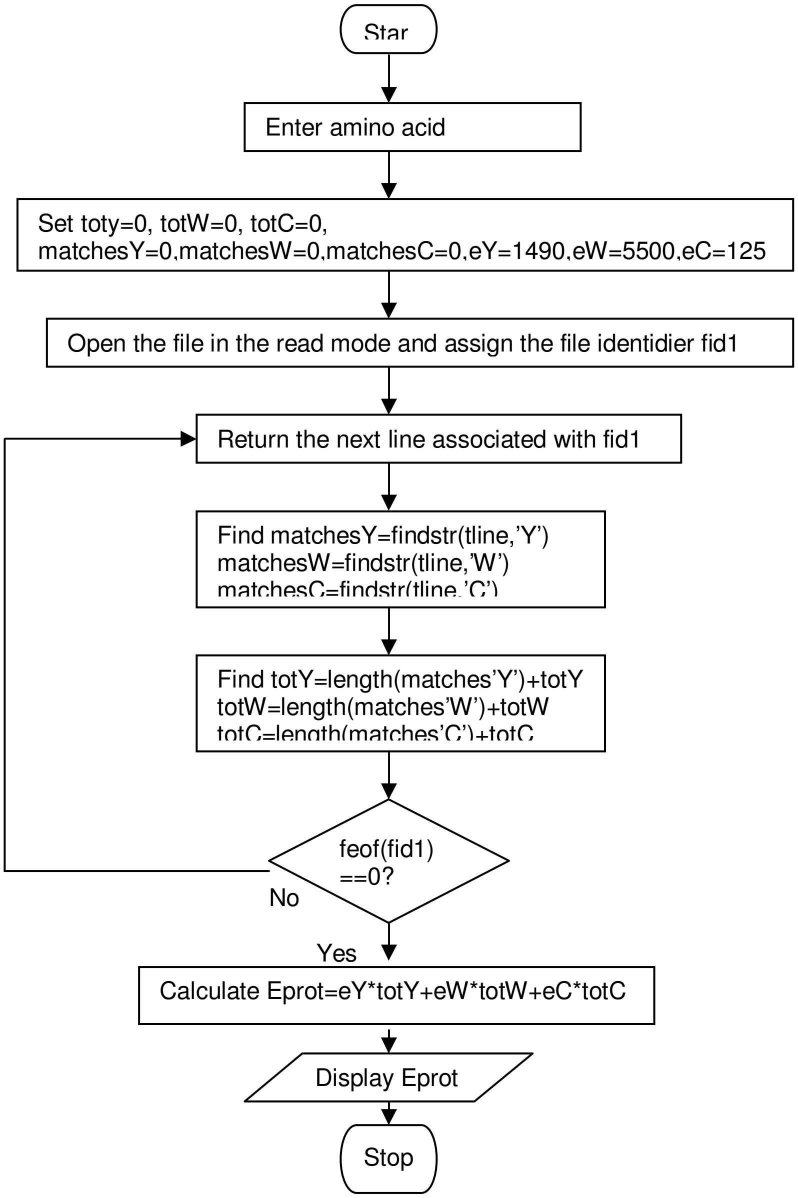

Star
Enter amino acid
Set toty=0, totW=0, totC=0,
matchesY=0,matchesW=0,matchesC=0,eY=1490,eW=5500,eC=125
Open the file in the read mode and assign the file identidier fid1
Return the next line associated with fid1
Find matchesY=findstr(tline,'Y')
matchesW=findstr(tline,'W')
matchesC=findstr(tline,'C')
Find totY=length(matches'Y')+totY
totW=length(matches'W')+totW
totC=length(matches'C')+totC
feof(fid1)
==0?
No
Yes
Calculate Eprot=eY*totY+eW*totW+eC*totC
Display Eprot
Stop

FIGURE 1: Prediction of Extinction Coefficient.

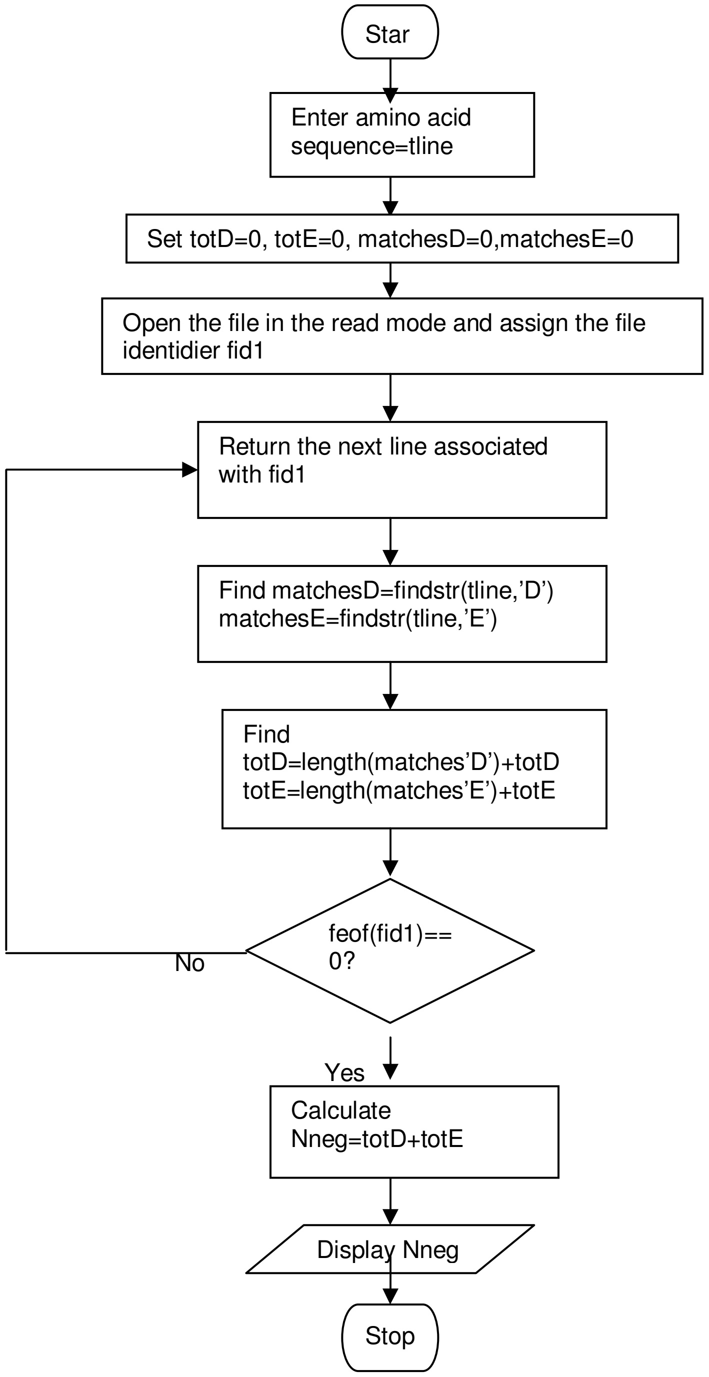

Star
Enter amino acid sequence=tline
Set totD=0, totE=0, matchesD=0,matchesE=0
Open the file in the read mode and assign the file identidier fid1
Return the next line associated with fid1
Find matchesD=findstr(tline,'D')
matchesE=findstr(tline,'E')
Find
totD=length(matches'D')+totD
totE=length(matches'E')+totE
feof(fid1)== 0?
No
Yes
Calculate Nneg=totD+totE
Display Nneg
Stop

FIGURE 2: Prediction of Negatively charged residues

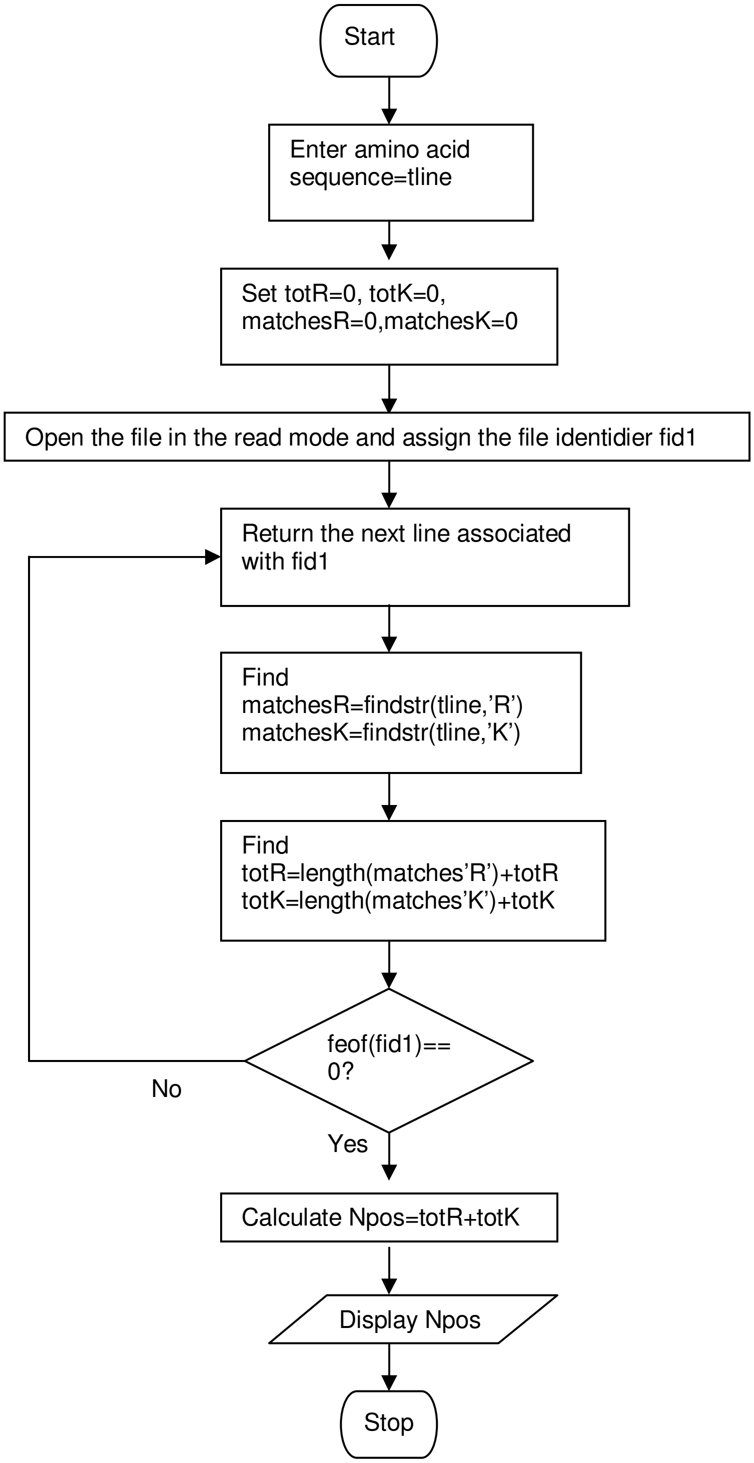

Start
Enter amino acid sequence=tline
Set totR=0, totK=0, matchesR=0,matchesK=0
Open the file in the read mode and assign the file identidier fid1
Return the next line associated with fid1
Find matchesR=findstr(tline,’R’) matchesK=findstr(tline,’K’)
Find totR=length(matches’R’)+totR totK=length(matches’K’)+totK
feof(fid1)== 0?
No
Yes
Calculate Npos=totR+totK
Display Npos
Stop

FIGURE 3: Prediction of Positively charged residues

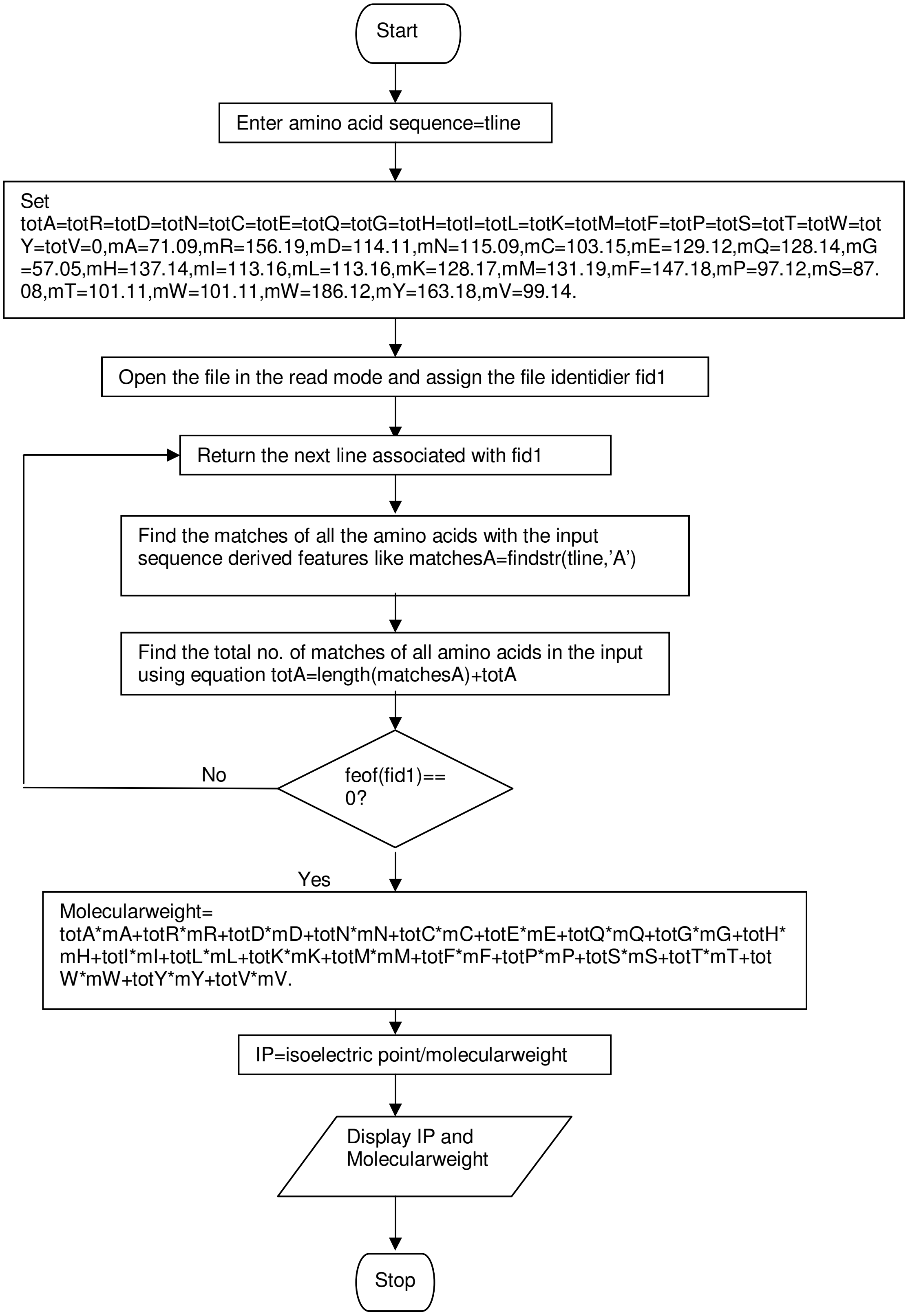

Start
Enter amino acid sequence=tline
Set
totA=totR=totD=totN=totC=totE=totQ=totG=totH=totI=totL=totK=totM=totF=totP=totS=totT=totW=totY=totV=0,mA=71.09,mR=156.19,mD=114.11,mN=115.09,mC=103.15,mE=129.12,mQ=128.14,mG=57.05,mH=137.14,mI=113.16,mL=113.16,mK=128.17,mM=131.19,mF=147.18,mP=97.12,mS=87.08,mT=101.11,mW=101.11,mW=186.12,mY=163.18,mV=99.14.
Open the file in the read mode and assign the file identidier fid1
Return the next line associated with fid1
Find the matches of all the amino acids with the input sequence derived features like matchesA=findstr(tline,'A')
Find the total no. of matches of all amino acids in the input using equation totA=length(matchesA)+totA
No
feof(fid1)== 0?
Yes
Molecularweight=
totA*mA+totR*mR+totD*mD+totN*mN+totC*mC+totE*mE+totQ*mQ+totG*mG+totH*mH+totI*mI+totL*mL+totK*mK+totM*mM+totF*mF+totP*mP+totS*mS+totT*mT+totW*mW+totY*mY+totV*mV.
IP=isoelectric point/molecularweight
Display IP and Molecularweight
Stop

FIGURE 4: Prediction of Iso-electric point/Mol weight

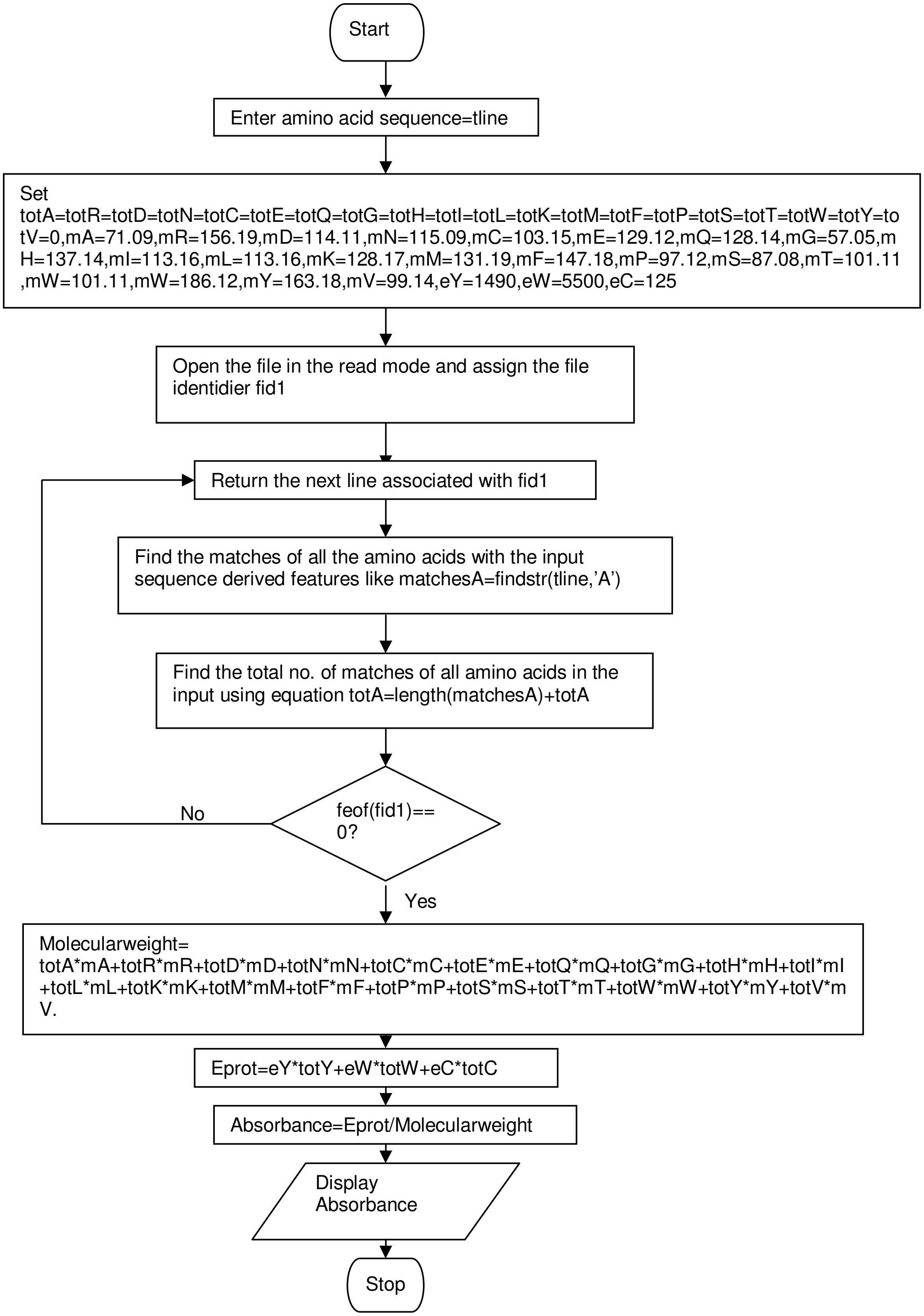

Start
Enter amino acid sequence=tline
Set
totA=totR=totD=totN=totC=totE=totQ=totG=totH=totI=totL=totK=totM=totF=totP=totS=totT=totW=totY=totV=0,mA=71.09,mR=156.19,mD=114.11,mN=115.09,mC=103.15,mE=129.12,mQ=128.14,mG=57.05,mH=137.14,mI=113.16,mL=113.16,mK=128.17,mM=131.19,mF=147.18,mP=97.12,mS=87.08,mT=101.11,mW=101.11,mW=186.12,mY=163.18,mV=99.14,eY=1490,eW=5500,eC=125
Open the file in the read mode and assign the file identidier fid1
Return the next line associated with fid1
Find the matches of all the amino acids with the input sequence derived features like matchesA=findstr(tline,'A')
Find the total no. of matches of all amino acids in the input using equation totA=length(matchesA)+totA
No
feof(fid1)== 0?
Yes
Molecularweight= totA*mA+totR*mR+totD*mD+totN*mN+totC*mC+totE*mE+totQ*mQ+totG*mG+totH*mH+totI*mI+totL*mL+totK*mK+totM*mM+totF*mF+totP*mP+totS*mS+totT*mT+totW*mW+totY*mY+totV*mV.
Eprot=eY*totY+eW*totW+eC*totC
Absorbance=Eprot/Molecularweight
Display Absorbance
Stop

FIGURE 5: Prediction of Absorbance

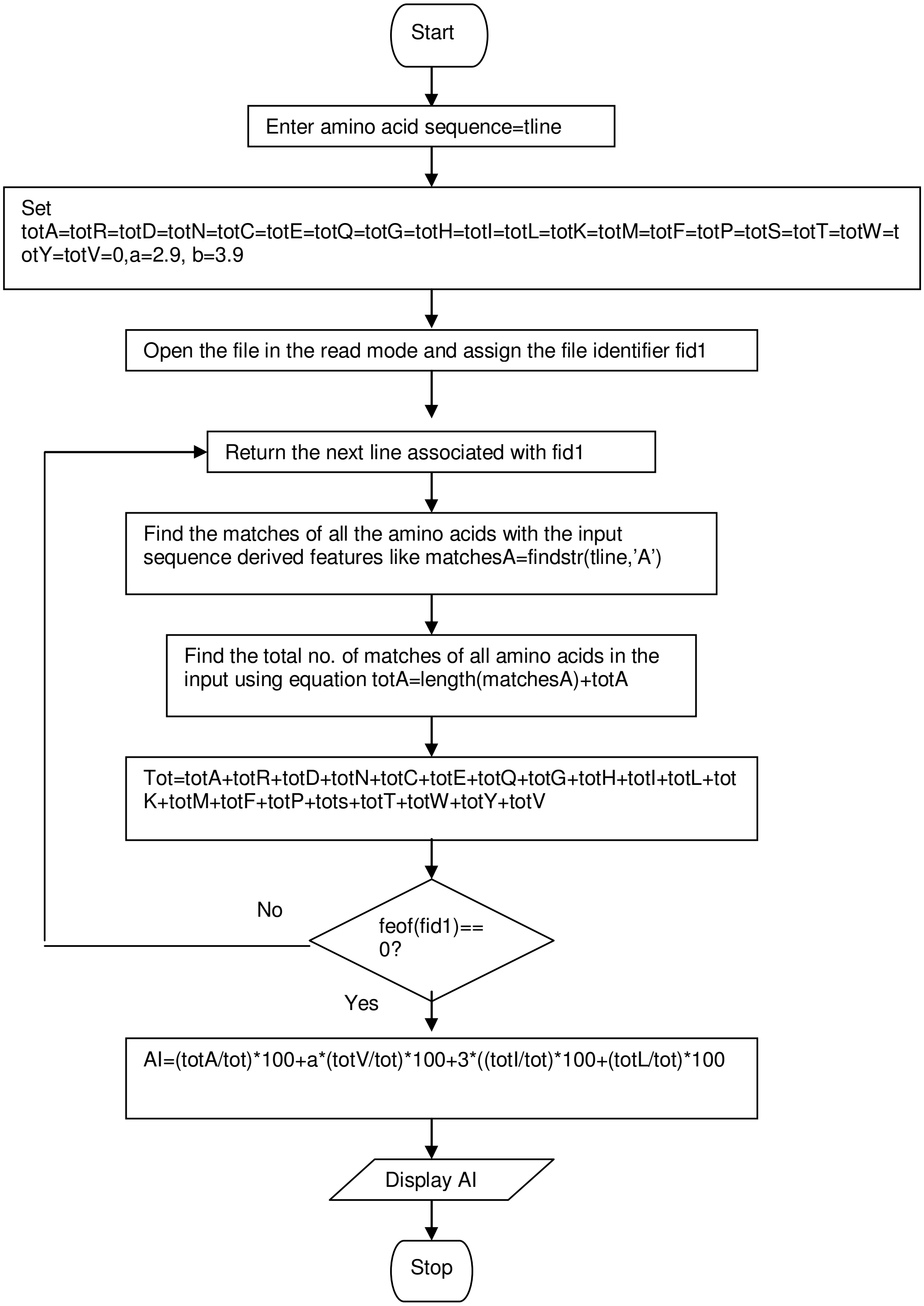

Start
Enter amino acid sequence=tline
Set
totA=totR=totD=totN=totC=totE=totQ=totG=totH=totI=totL=totK=totM=totF=totP=totS=totT=totW=totY=totV=0,a=2.9, b=3.9
Open the file in the read mode and assign the file identifier fid1
Return the next line associated with fid1
Find the matches of all the amino acids with the input sequence derived features like matchesA=findstr(tline,'A')
Find the total no. of matches of all amino acids in the input using equation totA=length(matchesA)+totA
Tot=totA+totR+totD+totN+totC+totE+totQ+totG+totH+totI+totL+totK+totM+totF+totP+tots+totT+totW+totY+totV
No
feof(fid1)== 0?
Yes
AI=(totA/tot)*100+a*(totV/tot)*100+3*((totI/tot)*100+(totL/tot)*100
Display AI
Stop

FIGURE 6: Prediction of Aliphatic Index

7. RESULTS AND DISCUSSION

In the present work, the amino acid sequence is used as input to predict the sequence derived features. Some of these sequence derived features are produced from amino acid sequence by exploring different parameters. In this present work, output will be displayed if the blank spaces are included in the input sequence and output will not be displayed if lowercase alphabets of amino acid sequence are given as input. The respective results are shown in table 1.
The input of amino acid sequence in ex1.txt file is given below:

LCLYTHIGRNIYYGSYLYSETWNTGIMLLLITMATAFMGYVLPWGQMSFWGATVITNLFSAIPYIGT
NLVEWIWGGFSVDKATLNRFFAFHFILPFTMVALAGVHLTFLHETGSNNPLGLTSDSDKIPFHPYY
TIKDFLGLLILILLLLLLALLSPDMLGDPDNHMPADPLNTPLHIKPEWYFLFAYAILRSVPNKLGGVL
ALFLSIVILGLMPFLHTSKHRSMMLRPLSQALFWTLTMDLLTLTWIGSQPVEYPYTIIGQMASILYF
SIILAFLPIAGXIENY

Sr. No.	Sequence Derived Features obtained	Values
1.	No. of Amino Acids	283
2.	Molecular weight	3.1955e+504
3.	Number of Negatively charged residues	15
4.	Number of positively charged residues	11
5.	Extinction Coefficient	66475
6.	Absorbance	2.0803
7.	Aliphatic Index	119.6113
8.	Compute IP/Mw	1.2048e-004

TABLE 1: Sequence Derived Features Produced

Calculations on ex1.txt file:
Number of Negatively charged residues:
Composition of Aspartic acid (D) and Glutamic acid (E) for ex1.txt:
No. of Aspartic acid in ex1=9
No. of Glutamic acid in ex1=6
Number of Negatively charged residues for ex1 =9+6=15
Number of positively charged residues:
Composition of Arginine (R) and Lysine (K) for ex1.txt:
No. of Arginine in ex1=5
No. of Lysine in ex1=6
Number of Positively charged residues for ex1 =5+6=11
Extinction Coefficient:
The equation to calculate Extinction Coefficient is as given below:
Eprotein = Ntyr * Etyr + Ntrp * Etrp+ Ncys * Ecys
Where Etyr =1490, Etrp =5500, Ecys = 125
No. of Tyrosine (Y) in ex1=Ntyr= 15

No. of Tryptophan (W) in ex1=Ntrp = 8
No. of Cystine (C) in ex1=Ncys= 1
Putting these values in the above equation:
Eprotein=15*1490+8*5500+1*125 = 66475
Aliphatic Index:
The equation to calculate the Aliphatic Index as given below:
AI = Xala + a * Xval + b * (Xile + Xleu)
Where a = 2.9, b = 3.9
Mole Percentage of Alanine(A) in ex1= Xala =(17/283)*100=6.007
Mole Percentage of Valine (V) in ex1= Xval = (10/283)*100=3.533
Mole Percentage of Isoleucine(I) in ex1= Xile =(25/283)*100=8.834
Mole Percentage of Leucine (L) in ex1= Xleu = (50/283)*100=17.666
Putting these values in the above equation:
AI= 6.007+2.9*3.533+3.9(8.834+17.666) =0.9542
Absorbance/Optical Density:
The equation to calculate the Absorbance is as given below:
Absorbance = Eprotein / Molecular Weight
Eprotein for ex1 (as calculated above) =66475
Molecular weight for ex1=3.1955e+504
Putting these values in the above equation:
Absorbance =66475/3.1955e+504=2.0803
Compute IP/Mw:
Calculate Isoelectric of the amino acid sequence/Molecular weight
Isoelectric point of ex1=24.742e
Molecular weight of ex1=3.1955e+504
Compute IP/Mw=1.2048e-004

8. CONCLUSION AND FUTURE SCOPE

This present work is designed and implemented for prediction of sequence derived features which are used for protein class prediction that is further useful in drug discovery process. In this various sequence derived features are studied and integrated using Associative rule mining. The model is very simple to use and no manual work is involved. The results have been verified by comparing their output with the previously available tools. The future scope for further work is listed below:
a) Other 2-D and 3-D protein structure prediction algorithms can be included to predict the protein function.
b) Protein Class Prediction can be done from the input sequence itself.

9. REFERENCES

1. A. Al-Shahib, R. Breitling, and D. R. Gilbert "*Predicting protein function by machine learning on amino acid sequences – a critical evaluation*" BMC Genomics, 8:1-10, 2007

2. A. Clare. "*Machine learning and data mining for yeast functional genomics*", Ph.D. thesis, University of Wales, February 2003

3. A. Jaiswal, A. Chhabra, U. Malhotra, S. Kohli, V. Rani "*Comparative analysis of human matrix metalloproteinases: Emerging therapeutic targets in diseases*" Bioinformation 6(1): 23-30, 2011

4. D. Krane and M. Raymer. "*Fundamental Concepts of Bioinformatics*", Pearson Education, New Delhi, pp.1-314 (2006)

5. J. Han and M. Kamber. "*Data Mining: Concepts and Techniques*", Morgan Kaufmann Publishers, pp. 226-229 (2004)

6. L. Jensen. “*Prediction of Protein Function from Sequence Derived Protein Features*”, Ph.D. thesis, Technical University of Denmark, 2002

7. L. Jensen, M. Skovgaard and S. Brunak. “*Prediction of Novel Archaeal Enzymes from Sequence Derived Features*”, Protein Science, 11: 2894-2898, 2002

8. L.J. Jensen, R. Gupta, N. Blom, D. Devos, J. Tamames, C. Kesmir, H. Nielsen, H.H. Starfeldt, K. Rapacki, C. Workman, C.A.F. Andersen, S. Knudsen, A. Krogh, A. Valencia and S. Brunak “*Prediction of Human Protein Function from Post-Translational Modifications and Localization Features*” Journal of Molecular Biology, 319(5): 1257-1265, 2002

9. M. Kanakubo and M. Hagiwara. “*Speed up technique for Associative rule mining based on an Artificial Algorithm*”, GRC book on granular computing, 38(12):318-323, 2007

10. M. Ouali, R.D. King “*Cascaded multiple classifiers for secondary structure prediction*” Prot Sci., 9:1162–1176, 2000

11. M. Singh, P. Singh and P.K, Wadhwa “*Human Protein Function Prediction using Decision Tree Induction*” International Journal of Computer Science and Network Security, USA, 7(4):92-98, 2007

12. M. Singh, Wadhwa P.K., Surinder Kaur “*Predicting Protein Function using Decision Tree*” World Academy of Science, Engineering and Technology, 39:350-353, 2008

13. R. Agrawal, T. Imielinski and A. Swami. “*Mining Association Rules Between Sets of Items in Large Databases*", SIGMOD ACM Conference, 22(2):207-216, 1993

14. R. Gupta, A. Mittal, and K. Singh. “*Time series based feature extraction approach for prediction of protein structural class*”, EURASIP Journal, 8(1): 1-7, 2008

15. R. Linding, L. J. Jensen, F. Diella, P. Bork, T.J. Gibson, R.B. Russell “*Protein disorder prediction: implications for structural proteomics*” Structure, 11:1453-1459, 2003

16. Veenu Mangat "*Swarm Intelligence Based Technique for Rule Mining in the Medical Domain*" International Journal of Computer Applications, 4(1):19-24, July 2010

17. Z.R. Li, H.H. Lin, L.Y. Han, L. Jiang, X. Chen, Y.Z. Chen. “*PROFEAT: a web server for computing structural and physicochemical features of proteins and peptides from amino acid sequence*” Nucleic Acids Res, 34:W32-W37, 2008

18. http://www.cbs.dtu.dk/services/NetNGlyc/

19. http://www.cbs.dtu.dk/services/NetOGlyc/

20. http://www.cbs.dtu.dk/services/SignalP/

21. http://www.cbs.dtu.dk/services/TMHMM/

22. http://expasy.org/

23. http://psort.hgc.jp/

Car-Following Parameters by Means of Cellular Automata in the Case of Evacuation

Kohei Arai arai@is.saga-u.ac.jp
Faculty of Science and Engineering/Department of Information Science
Saga University
1 Honjo-machi, Saga, 840-8502, Japan

Tri Harsono triharsono69@yahoo.com
Faculty of Science and Engineering/
Department of Information Science
Saga University
1 Honjo-machi, Saga, 840-8502, Japan
Electronics Engineering Polytechnic Institute of Surabaya (EEPIS)
Jalan Raya ITS, Keputih Sukolilo, Surabaya, 60111, Indonesia

Achmad Basuki basukieepis2008@yahoo.com
Faculty of Science and Engineering/Department of Information Science
Saga University
1 Honjo-machi, Saga, 840-8502, Japan
Electronics Engineering Polytechnic Institute of Surabaya (EEPIS)
Jalan Raya ITS, Keputih Sukolilo, Surabaya, 60111, Indonesia

Abstract

This study is attention to the car-following model, an important part in the micro traffic flow. Different from Nagel–Schreckenberg's studies in which car-following model without agent drivers and diligent ones, agent drivers and diligent ones are proposed in the car-following part in this work and lane-changing is also presented in the model. The impact of agent drivers and diligent ones under certain circumstances such as in the case of evacuation is considered. Based on simulation results, the relations between evacuation time and diligent drivers are obtained by using different amounts of agent drivers; comparison between previous (Nagel–Schreckenberg) and proposed model is also found in order to find the evacuation time. Besides, the effectiveness of reduction the evacuation time is presented for various agent drivers and diligent ones.

Keywords: Car-Following, Agent Drivers, Diligent Drivers, Evacuation Time, Effectiveness

1. INTRODUCTION

Car-following model has an important role in the micro traffic flow. Maerivoet et al. [1] have expressed that car-following behavior influences the activities of traffic on the roadway. The smoothness of traffic activities on the roadway is determined by the speed of vehicles on the aforementioned road. The flexibility of vehicles speed in the sense that they can adjust the acceleration and deceleration has been considered by Brilon et al. [2] with insert a parameter based on the temporal variables into the car-following model. Besides, the smoothness of traffic activities is also determined by the cooperation model between the drivers and it is associated by car-following model such as presented by [3-5]. Car-following model is also very influential in creating the stability of traffic flow such as investigated by [2-7].

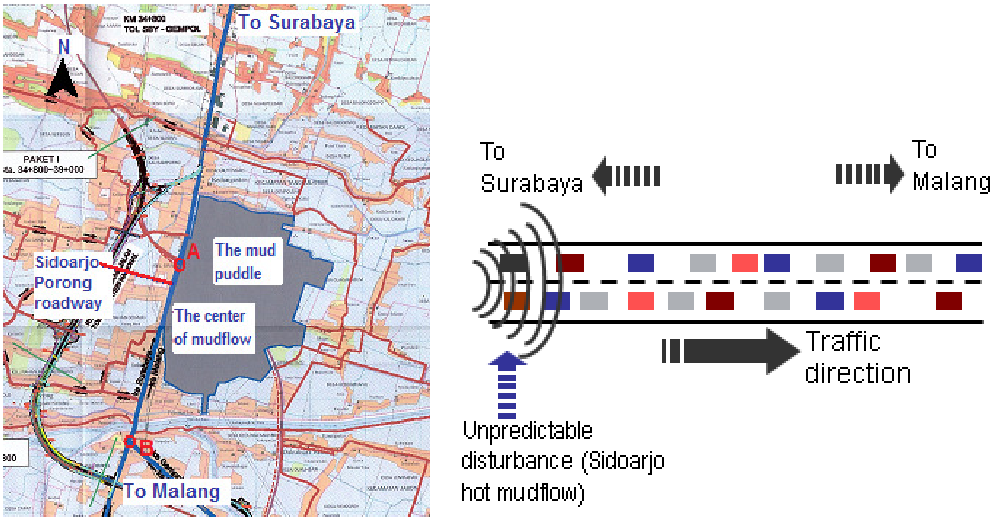
In this work, in the case of evacuation, car-following model has the proposed parameters, they are agent drivers and diligent ones. They have a good response to the surrounding environment and also recognize speed changes so that allowing traffic to be controlled by the best way to minimize the evacuation time. Agent drivers have capability to lead the other cars and they also have information that can be derived from the evacuation control centre and transferred to the other drivers through wireless network connection. Besides, agent drivers can lead the other cars to the safe area in a fastest way. Not only agent drivers but also diligent ones have a concern to the distance between their vehicle and the vehicle ahead.

Car-following model used in this study is reflected in the case of vehicles evacuation on Sidoarjo Porong roadway. The location of this road is in Sidoarjo, East Java, Indonesia. The structure of Sidoarjo Porong roadway and surrounding areas is shown in Fig. 1. The road is very close to the hot mudflow disaster and as a main artery road connects between Surabaya, the capital city of the province and the cities inside the province. Besides, the mud volcano remains have high flow rates until now [8]. One of the important things when the dike of hot mudflow is damaged and the mud overflows from the damaged dike to the nearby road spontaneously is how to evacuate the vehicles from disaster area to the safe area. At the time of the vehicles evacuation is carried out, the best way to get the minimum evacuation time is a condition that is highly desirable.

This study presents the impact of agent drivers and diligent ones toward the evacuation time and also describes the effectiveness of reduction the evacuation time for various agent drivers and diligent ones.

2. THE ROAD STRUCTURE AND ITS CONDITIONS

The map of Sidoarjo Porong roadway and surrounding areas is shown in Fig. 1(a). Sidoarjo Porong roadway is located in the middle part of this map (the blue color, straight line). There is center of hot mudflow (the gray color) very close to this road. The road has two directional, from Surabaya to Malang and from Malang to Surabaya. In this work, we investigate one directional, i.e. from Surabaya to Malang, this part is adjacent to the center of mudflow. The visualization of this part is shown in Fig. 1(b) in which there are two lanes formally.



(a) (b)

FIGURE 1: (a) Sidoarjo Porong roadway and surrounding areas; (b) Structure of Sidoarjo Porong roadway, direction: from Surabaya to Malang.

In the context that mud overflows into the road, we assume that it comes from one end of the road and has the same direction as the vehicles direction. In another sense, when we see in Fig. 1(b), we can say that mud will flows from left to right in accordance with the vehicles movement. The speed of the mudflow is assumed to be constant. It is set as smaller than maximum speed of vehicle. The other condition on this road is that there is no traffic light at all.

3. THE PROPOSED MODEL IN THE CASE OF EVACUATION

There are two major methods of car-following in the micro traffic flow models, continuous models and discrete ones. Several kinds of the continuous models are Optimal Velocity Model (OVM), Generalized Force Model (GFM), Full Velocity Difference Model (FVDM), and Two Velocity Difference Model (TVDM) explained in [9]; [10]; [11]; and [5], respectively. In the continuous models, a driver is stimulated by his own velocity v_n, n is the position of his car; the distance between the car and the car ahead s_n; and the velocity of the vehicle in front v_{n+1}. The equation of the vehicles motion is characterized by the acceleration function $\ddot{s}_n(t) = \dot{v}_n(t)$ in which depends on the input stimuli. The equation of the acceleration function is $\ddot{s}_n(t) = \dot{v}_n(t) = F\big(v_n(t), s_n(t), v_{n+1}(t)\big)$, t is the time variable.

The discrete model of car-following has been developed by using Cellular Automata (CA). CA is model that has discrete in space, time and state variables. Due to the discreteness, CA is extremely efficient in implementations on a computer. CA for traffic has been called by Traffic Cellular Automata (TCA) [1]. Maerivoet et al. [1] have also expressed that there are some kinds of stochastic models of CA for micro traffic flow, one of them is Nagel-Schreckenberg model. They stated that in 1992, Nagel and Schreckenberg proposed a TCA model that was able to reproduce several characteristics of real-life traffic flows, e.g., the spontaneous emergence of traffic jams. Their model has been called the Nagel-Schreckenberg TCA and it has been explained in the [12]. Hereinafter, the Nagel-Schreckenberg TCA is referred as the NaSch. Maerivoet et al. [1] have also stated that the NaSch model has been called as a minimal model, in the sense that all the rules are a necessity for mimicking the basic features of real-life traffic flows.

In this study, we propose the driver behavior parameters and inserted into the car-following part of micro traffic flow. They are agent drivers and diligent ones. The characteristics of agent drivers and diligent ones are explained in the section one. We can summarize that agent drivers and diligent ones have the ability to expand their chance increasing their speed in accordance with the information they get from the surrounding environment. Their ability can be reflected by the addition of the speed parameter on those, for each agent driver is $c' = [0 : v_{\max}]$ while for each diligent one is $c = [0 : \min(\bar{v}, v)]$. These parameters have the sense that for agent drivers can expand the chance to increase the speed start from zero to maximum speed $v_{\max}$, while for diligent drivers start from zero to minimum value between mean speed $\bar{v}$ and current speed v. With regard to the addition of the speed parameters, the velocity of agent drivers and diligent ones are respectively defined by the equations $v'_{i,j,t} = v_{i,j}(t) + [0 : v_{\max}]$ and $v_{i,j,t} = v_{i,j}(t) + [0 : \min(\bar{v}, v)]$. $v_{i,j}(t)$ is the velocity of the *ith* lane-*jth* site car by the time *t*. $v'_{i,j,t}$ and $v_{i,j,t}$ are consecutive the velocity of an agent driver and a diligent one by the time *t* in the position *ith* lane-*jth* site.

In the model, the road consists of two lanes (as be mentioned in section two) and each lane is comprised of *L* sites of equal size. Each site can either be occupied by a vehicle or it can be empty. The amounts of agent drivers *A* are determined by the integer number, while diligent drivers are determined by using probability *dd*. The velocity for each vehicle is an integer value between zero and $v_{\max}$. The initial velocity for each vehicle is determined by using normal random in which mean speed $\bar{v}$ and standard deviation *sd* as parameters inserted in the system. The total number of vehicles on the road is determined by the initial conditions using probability of vehicle density *k*, and with open boundary conditions. Due to the fact that the vehicles evacuation must be performed in the best way to minimize evacuation time *T*, the specific rules of the Nagel-Schreckenberg traffic cellular automata (NaSch) [12] is modified in the following for the car-following model. At each discrete time step $t \to t+1$, all the vehicles simultaneously update their states according to four consecutive steps:

1) Acceleration: if $v_{i,j}(t) < v_{\max}$ and $gs_{i,j}(t) > v_{i,j}(t)+1$, $v_{i,j}(t+1) \rightarrow v_{i,j}(t)+1$. $gs_{(i,j)}(t)$ is the distance between the *ith* lane-*jth* site car and the next car ahead.
2) Braking: if $gs_{i,j}(t) \leq v_{i,j}(t)$, $v_{i,j}(t+1) \rightarrow gs_{i,j}(t)-1$
3) Randomization: with probability *h* and random number $\xi(t)$, if $\xi(t) < h$; $v_{i,j}(t+1) \rightarrow v_{i,j}(t)-1$
4) Vehicle movement: in accordance with the proposed parameters in the car-following part, agent drivers and diligent ones; vehicle movement is divided into three kinds,

   (*a*) $x_{i,j}(t+1) \rightarrow x_{i,j}(t)+v_{i,j}(t+1)+[0:v_{\max}]$ for an agent driver,

   (*b*) $x_{i,j}(t+1) \rightarrow x_{i,j}(t)+v_{i,j}(t+1)+[0:\min(\bar{v},v)]$ for a diligent driver,

   (*c*) $x_{i,j}(t+1) \rightarrow x_{i,j}(t)+v_{i,j}(t+1)$ for an usual driver.

   $x_{i,j}(t)$ is the position of the *ith* lane-*jth* site vehicle by the time *t*.

By referring [1], the modified implementation of lane-changing model is conducted by the following two rules consecutively executed at each time step: (*i*) the lane-changing model, exchanging vehicles between laterally adjacent lanes. By using two lanes; probability of lane-changing *lc*; and integer value $a=[0:v]$, the rules are: if $gs_{i=1,j}(t) < v_{i=1,j}(t)$ and $x_{i=2,j,j+v}(t)=0$, $x_{i=2,j+a}(t+1) \rightarrow x_{i=1,j}(t)$; and if $gs_{i=2,j}(t) < v_{i=2,j}(t)$ and $x_{i=1,j,j+v}(t)=0$, $x_{i=1,j+a}(t+1) \rightarrow x_{i=2,j}(t)$. (*ii*) vehicle movement, all the vehicles are moved forward by applying three kinds of the vehicle movement in the step 4.

The lane-changing model describes that if in a lane, a driver is not possible to move his car forward (there is a car ahead) and he sees the empty sites in other lane with the number of sites up to the speed *v* then he drives his car into the aforementioned lane. When a car is on a new lane, it has a speed less than or equal to the current speed *v*. It implies a deceleration that experienced by a car when it is moving to the other lane.

4. SIMULATION RESULTS

Regarding with the real situation on Sidoarjo Porong roadway, the start position of the evacuation is point A and the destination area (safe area) is point B (Fig. 1a), the distance is 3500 m, it is as a road length *L*. In this work, *L* is assumed to be 500, so that the length of one site is set to 7 m. By referring to [12], one time step approximately corresponds to 1 second in real time. The initial velocity for each vehicle is determined by using normal random with the value of parameters ($\bar{v}$ and *sd*) is depends on the vehicle density (probability of vehicle density *k*). In the term of the low vehicle density, we use $\bar{v}$ and *sd* is 4 and 1, respectively; in the intermediate one, $\bar{v}$ and *sd* is consecutively set by 3 and 1; while in the high one, we use $\bar{v}$ and *sd* is 2 and 1, respectively.

The following section, we show relations between *T* and *dd* using different amounts of agent drivers *A*, after that comparison between previous (NaSch) and proposed model is performed in order to find the evacuation time, and followed by description of the effectiveness of reduction the evacuation time for various *A* and *dd*.

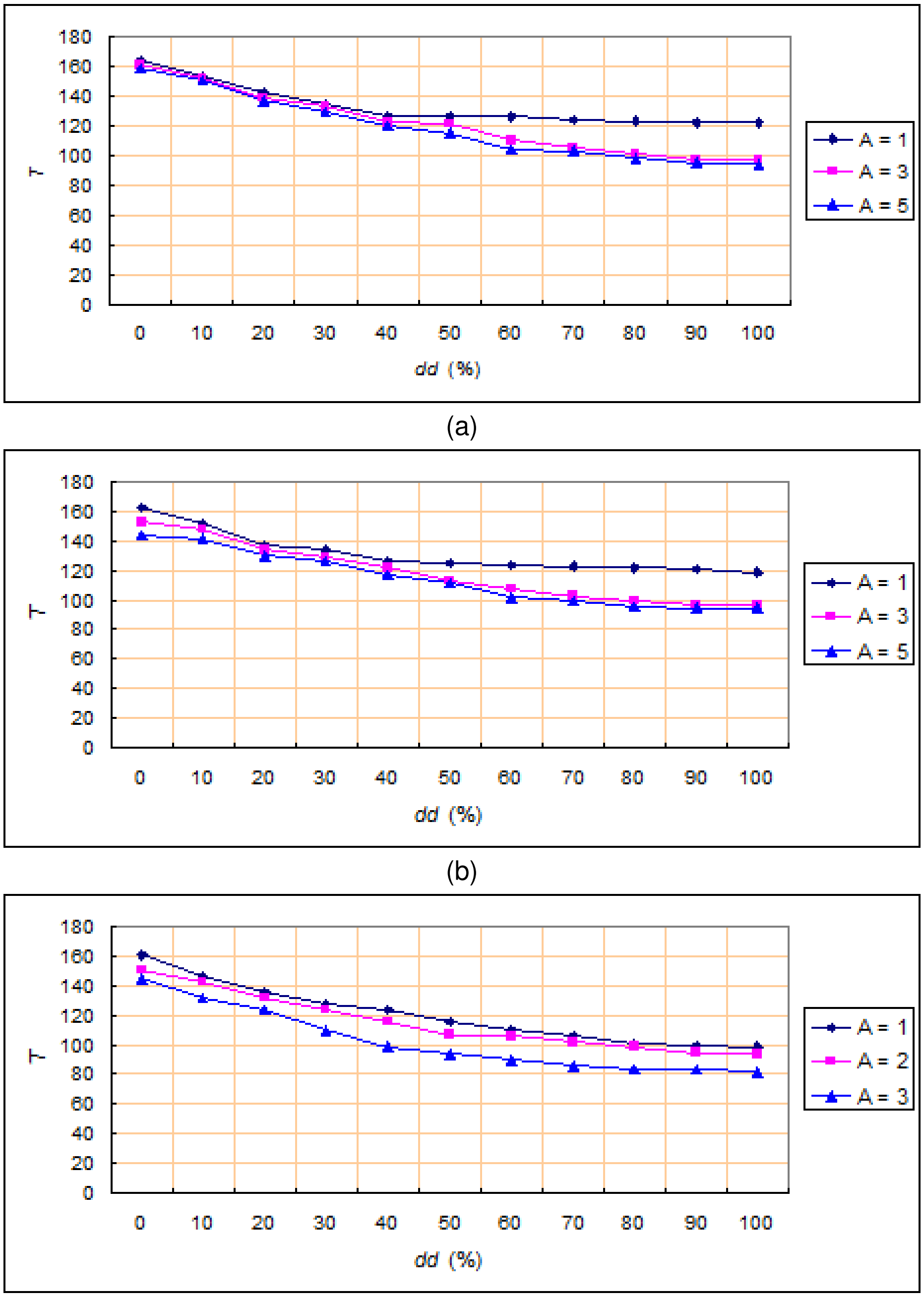
4.1 Relations between the Evacuation Time *T* and Diligent Driver *dd*

In these relations, we present the evacuation time *T* for unequal vehicle densities *k*. For each of the selected *k*, the evacuation time *T* is obtained in various *A*.

A. The Case of the Low Vehicle Density

For the low vehicle density *k* = 0.2; parameters $\bar{v}$ and *sd* for the initial velocity of each vehicle are 4 and 1, respectively. In Fig. 2(a), for *lc* = 0.3; and successively *A* = 1, 3, and 5; we obtain that by the increase of *dd* from 0% to 100%, *T* decreases either for *A* = 1, 3 or 5. By the value of

A = 1, *T* decreases significantly from *dd* = 0% to 40%, but the decrease of *T* gradually occurred from *dd* = 40% to 100%. While, *T* decreases significantly for *A* = 3 and 5 start from *dd* = 0% to 100%.



(a)

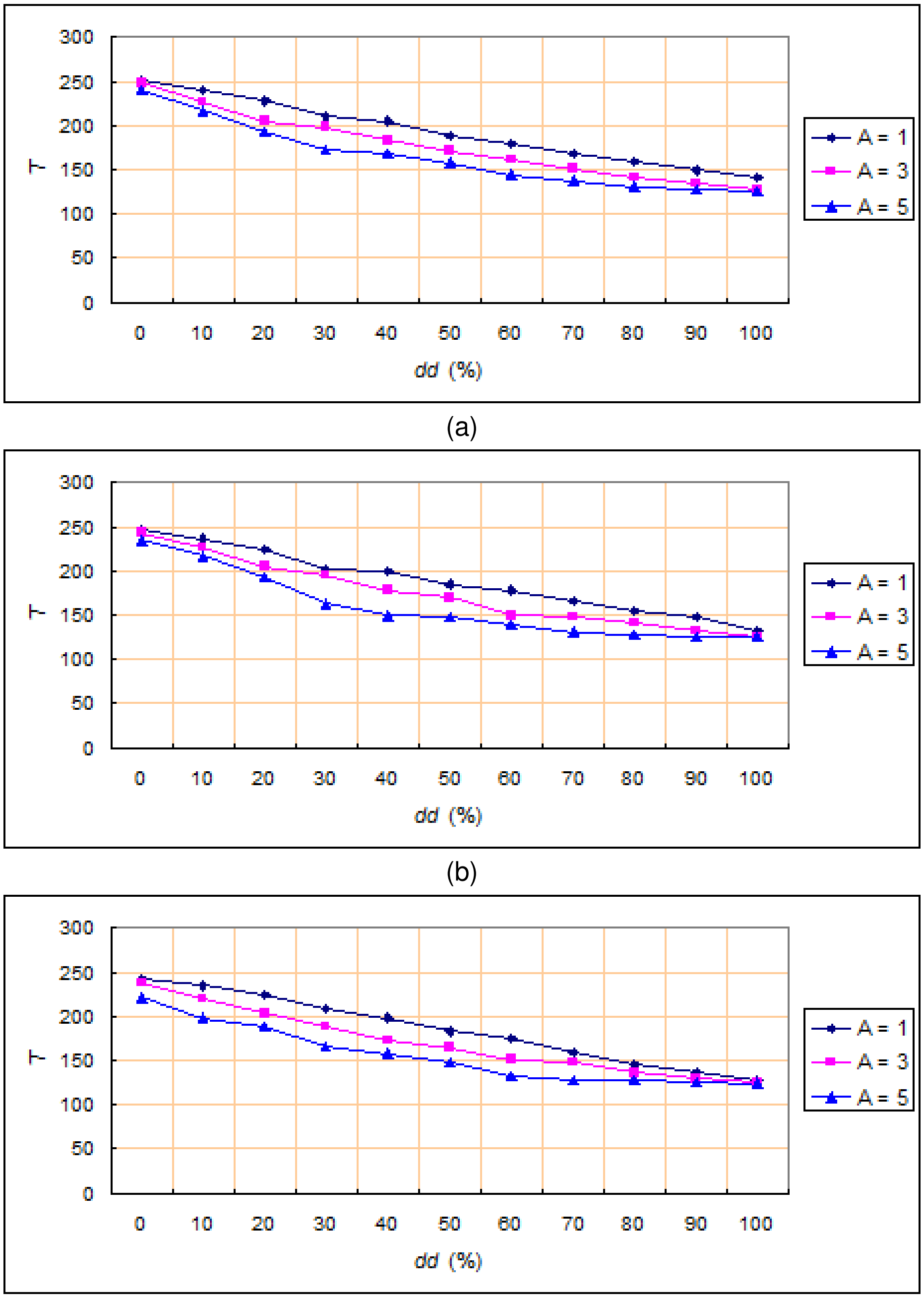
(b)

(c)

FIGURE 2: *T* vs. *dd* for different *lc* at (a) *lc* = 0.3, (b) *lc* = 0.5, (c) *lc* = 0.8; *k* = 0.2.

The condition is also experienced for *lc* = 0.5 and successively *A* = 1, 3, and 5; when *dd* increases, we find *T* decreases either for *A* = 1, 3, or 5 (Fig. 2(b)). When *A* = 1, the decrease of *T* significantly occurred from *dd* = 0% to 40%, while *T* gradually decreases from *dd* = 40% to 100%. The decrease of the evacuation time *T* also significantly occurs when we use *A* = 3 or 5, it happens for each *dd* that increases from 0% to 100%.

In Fig. 2(c), for *lc* = 0.8 and successively *A* = 1, 3, and 5; the decrease of the evacuation time *T* is obtained as *dd* increases. By using the value of *A* = 1, 3, or 5; all of the evacuation time *T* significantly decrease. Those conditions happen on the value of *dd* from 0% to 100%. We also find that for all the value of *lc* (0.3, 0.5, and 0.8); by the increase of *A*, the evacuation time *T* decreases as *dd* increases from 0% to 100%.



(a)

(b)

(c)

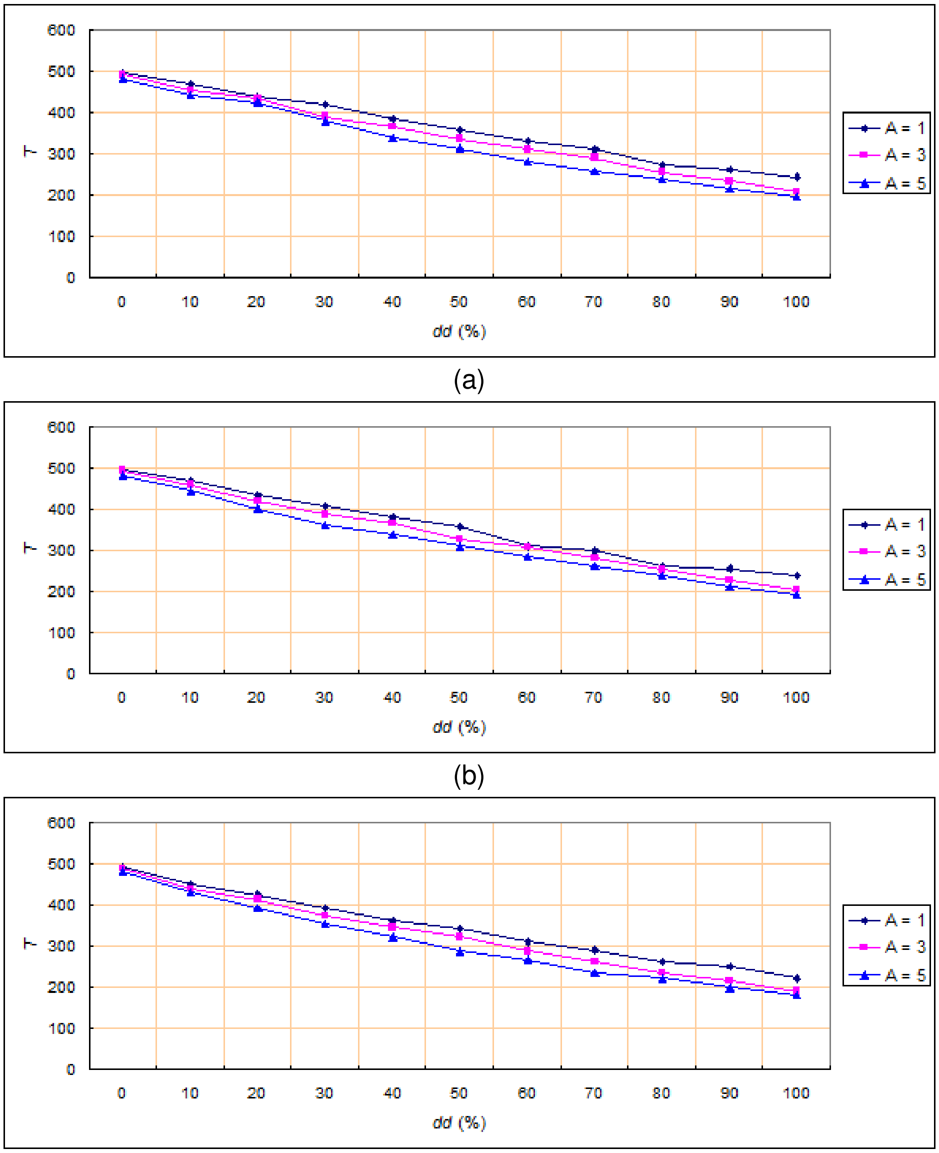
FIGURE 3: *T* vs. *dd* for different *lc* at (a) *lc* = 0.3, (b) *lc* = 0.5, (c) *lc* = 0.8; *k* = 0.5.

B. The Case of the Intermediate Vehicle Density

For the intermediate vehicle density *k* = 0.5; parameters $\overline{v}$ and *sd* for the initial velocity of each vehicle are 3 and 1, respectively. In Fig. 3(a), by using *lc* = 0.3 and successively *A* = 1, 3, and 5;

we obtain that with the increase of *dd* from 0% to 100%, *T* significantly decreases, it happens either for *A* = 1, 3 or 5.

The condition is also experienced for *lc* = 0.5, and successively *A* = 1, 3, and 5; the evacuation time *T* significantly decreases as *dd* increases from 0% to 100% (Fig. 3(b)). While, for *lc* = 0.8, and successively *A* = 1, 3, and 5; the decrease of evacuation time *T* is obtained from *dd* = 0% to 100% (Fig. 3(c)). We also find that for all the value of *lc* (0.3, 0.5, and 0.8); by the increase of *A*, the evacuation time *T* decreases as *dd* increases from 0% to 100%.



(a)

(b)

(c)

FIGURE 4: *T* vs. *dd* for different *lc* at (a) *lc* = 0.3, (b) *lc* = 0.5, (c) *lc* = 0.8; *k* = 0.8.

C. The Case of the High Vehicle Density

For the high vehicle density *k* = 0.8; parameters $\overline{v}$ and *sd* for the initial velocity of each vehicle are 2 and 1, respectively. In Fig. 4(a), by using *lc* = 0.3 and successively *A* = 1, 3, and 5; we obtain that with the increase of *dd* from 0% to 100%, *T* significantly decreases, it happens either for *A* = 1, 3 or 5.

The condition is also experienced for *lc* = 0.5, and successively *A* = 1, 3, and 5; the evacuation time *T* significantly decreases as *dd* increases from 0% to 100% (Fig. 4(b)). While, for *lc* = 0.8, and successively *A* = 1, 3, and 5; the decrease of evacuation time *T* is obtained from *dd* = 0% to 100% (Fig. 4(c)). We also find that for all the value of *lc* (0.3, 0.5, and 0.8); by the increase of *A*, the evacuation time *T* decreases as *dd* increases from 0% to 100%.

4.2 Comparative Evaluation Between Proposed and Previous (NaSch) Model

The comparative evaluation between the proposed model and the previous one (NaSch) is performed by referring to *k* = 0.2; 0.5; and 0.8, respectively. For the proposed model, we use *dd* = 0.8; the value of *A* is in sequence 1, 3, and 5. Using the same value of *lc* = 0.8, the evaluation both of those is conducted for each *k*.

For the low density *k* = 0.2, we get *T* for the previous model is bigger than that the proposed one. The extreme comparison result occurs between *T* in the previous model and *T* in the proposed one using *A* = 5. We find *T* in the previous model is 164 and *T* in the proposed one is 83, thus the proposed model gets *T* almost double faster than that *T* in the previous one (there is the decrease of *T* for the proposed model around 49.4%).

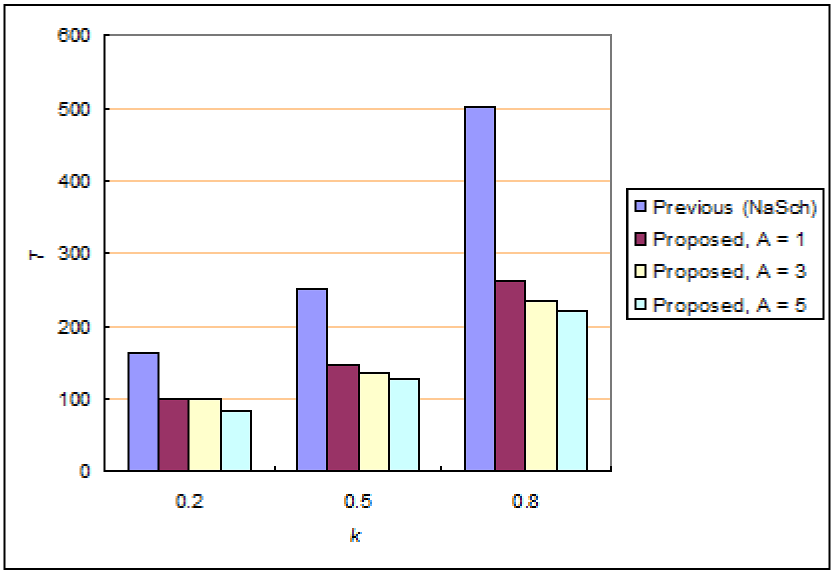


FIGURE 5: Comparative evaluation between the previous model (NaSch) and the proposed one for *lc* = 0.8 and *k* = 0.2; 0.5; 0.8, respectively. The proposed model uses *dd* = 0.8 and successively *A* = 1, 3, and 5.

For the intermediate density *k* = 0.5, we also get *T* for the previous model is bigger than that the proposed one. There is also the extreme comparison result between *T* in the previous model and *T* in the proposed one using *A* = 5. We find *T* in the previous model is 250 and *T* in the proposed one is 127, thus the proposed model gets *T* almost double faster than that *T* in the previous one (there is the decrease of *T* for the proposed model around 49.2%).

For the high density *k* = 0.8, we get *T* for the previous model is bigger than that the proposed one. We have the extreme comparison results between *T* in the previous model and *T* in the proposed one using either *A* = 1, 3, or 5. We find *T* in the previous model is 501, while *T* in the proposed one is 262; 236; and 221, respectively for *A* = 1; 3; and 5. Thus the proposed model gets *T* almost double faster than that *T* in the previous one for *A* = 1, and the proposed model gets *T* more than double faster than that *T* in the previous one for *A* = 3 and 5. It means that there is the decrease of *T* for the proposed model around 47.7%, 52.9%, and 55.9% for successively *A* = 1, 3, and 5.

4.3 The Effectiveness of Reduction the Evacuation Time

In this section, we present the effectiveness of reduction of *T* for unequal vehicle densities *k*. The effectiveness of the proposed model is measured by the comparative evaluation of the evacuation time *T* between the proposed model and the previous one (NaSch model). For the proposed model, we use the several of *dd* and *A*. Either the proposed model or the previous one, the value of *lc* used is 0.8.

	Evacuation time *T*						
	***A* = 1**	**Effectivenes (%)**	***A* = 3**	**Effectivenes (%)**	***A* = 5**	**Effectivenes (%)**	**Previous (NaSch)**
Proposed: *dd* = 0.2	136	17	132	20	124	24	164
Proposed: *dd* = 0.5	116	29	107	35	94	43	
Proposed: *dd* = 0.8	101	38	99	40	83	49	
Proposed: *dd* = 1	99	40	94	43	81	51	

TABLE 1: The effectiveness of *T* for *k* = 0.2, *lc* = 0.8.

A. For the Low Vehicle Density

In Table 1, for the low density *k* = 0.2; *lc* = 0.8; parameters $\bar{v}$ and *sd* used are 4 and 1, respectively; *dd* are consecutively set to 0.2, 0.5, 0.8, and 1; and using A = 1, 3, and 5; we find the effectiveness of reduction of *T*. We provide the effectiveness of *T* for the proposed model is almost double when the percentage ratio of *dd* = 0.8 and *A* = 5, it is 49%. While by using the percentage ratio of *dd* = 1 and *A* = 5, the effectiveness of *T* for the proposed model is more than double, it is 51%.

	Evacuation time *T*						
	***A* = 1**	**Effectivenes (%)**	***A* = 3**	**Effectivenes (%)**	***A* = 5**	**Effectivenes (%)**	**Previous (NaSch)**
Proposed: *dd* = 0.2	224	10	202	19	187	25	250
Proposed: *dd* = 0.5	183	27	164	34	147	41	
Proposed: *dd* = 0.8	146	42	136	46	127	49	
Proposed: *dd* = 1	128	49	125	50	124	50	

TABLE 2: The effectiveness of *T* for *k* = 0.5, *lc* = 0.8.

B. For the Intermediate Vehicle Density

In Table 2, for the intermediate density *k* = 0.5; *lc* = 0.8; parameters $\bar{v}$ and *sd* used are 3 and 1, respectively; *dd* are consecutively set to 0.2, 0.5, 0.8, and 1; and using A = 1, 3, and 5; we find the effectiveness of reduction of *T*. We provide the effectiveness of *T* for the proposed model is almost double when the percentage ratio of *dd* = 1 and *A* = 1, and also occurs for the percentage ratio of *dd* = 0.8 and *A* = 5, those are 49%. While by using the percentage ratio of *dd* = 1 and *A* =

3; and also using *dd* = 1 and *A* = 5, the effectiveness of *T* for the proposed model are double, those are 50%.

	Evacuation time *T*						
	***A* = 1**	**Effectivenes (%)**	***A* = 3**	**Effectivenes (%)**	***A* = 5**	**Effectivenes (%)**	**Previous (NaSch)**
Proposed: *dd* = 0.2	425	15	413	18	393	22	501
Proposed: *dd* = 0.5	341	32	321	36	286	43	
Proposed: *dd* = 0.8	262	48	236	53	221	56	
Proposed: *dd* = 1	220	56	190	62	180	64	

TABLE 3: The effectiveness of *T* for *k* = 0.8, *lc* = 0.8.

C. For the High Vehicle Density

In Table 3, for the high density *k* = 0.8; *lc* = 0.8; parameters $\overline{v}$ and *sd* used are 2 and 1, respectively; *dd* are consecutively set to 0.2, 0.5, 0.8, and 1; and using A = 1, 3, and 5; we find the effectiveness of reduction of *T*. We provide the effectiveness of *T* for the proposed model is almost double when the percentage ratio of *dd* = 0.8 and *A* = 1, it is 48%. While by using the percentage ratio of *dd* = 1 and *A* = 1; *dd* = 0.8 and *A* = 3; *dd* = 1 and *A* = 3; *dd* = 0.8 and *A* = 5; *dd* = 1 and *A* = 5, we get the effectiveness of *T* for the proposed model are more than double, those are 56%; 53%; 62%; 56%; and 64%, respectively.

5. CONCLUSION

Agent drivers and diligent ones are incorporated into the car-following NaSch model. The modified car-following NaSch model is proposed. The relations between the evacuation time and diligent drivers, comparison between the previous model (NaSch) and the proposed one, and the effectiveness of reduction the evacuation time are investigated.

The simulation results find the impact of agent drivers and diligent ones with respect to the evacuation time. Regarding the relations between evacuation time and diligent drivers are obtained that with the increase of diligent drivers, evacuation time decreases either in the low vehicle density, in the intermediate one, or in the high one. In these relations are also shown that with the increase of the number of agent drivers, the evacuation time decreases for each the value of diligent drivers in the same number of agent drivers. Based on the comparative simulation study, this work shows that the proposed model has the faster way than that the previous one in the case of evacuation. The proposed model gets the evacuation time at least almost double faster than that the evacuation time in the previous one for the number of agent drivers is five with a certain value of diligent drivers, it occurs either in the low vehicle density; in the intermediate one; or in the high one. The impact of diligent drivers is depends on the percentage ratio of diligent drivers and is double when the percentage ratio of diligent driver is 100% in the low vehicle density and in the intermediate one, and is more than double when the percentage ratio of diligent driver is 80% or 100% in the high vehicle density. It is also found that the impact of agent drivers is depends of the number of agent drivers and is approximately double when the number of agent drivers is five in the low vehicle density and in the intermediate one (with any certain value of diligent drivers); or is more than double when the number of agent drivers is five in the high vehicle density (with any certain value of diligent drivers), in comparison to the existing simulation results without any agent (NaSch model).

6. REFERENCES

[1] Sven Maerivoet, Bart De Moor. ”*Cellular automata models of road traffic*”. Physics Reports 419: 1 – 64, 2005

[2] B.S. Kerner. “*The Physics of Traffic—Empirical Freeway Pattern Features, Engineering Applications, and Theory, Understanding Complex Systems*”, Springer, (2004)

[3] H. X. Ge, S. Q. Dai, L. Y. Dong, Y. Xue. “*Stabilization effect of traffic flow in an extended car-following model based on an intelligent transportation system application*”. Phys. Rev. E 70: 066134, 2004

[4] H.X. Ge, S.Q. Dai, Y. Xue, L.Y. Dong. “*Stabilization analysis and modified Korteweg–de Vries equation in a cooperative driving system*”. Phys. Rev. E 71: 066119, 2005

[5] H.X. Ge, R.J. Cheng, Z.P. Li. “*Two velocity difference model for a car following theory*”. Physica A 387: 5239–5245, 2008

[6] D. E. Wolf. “*Cellular automata for traffic simulations*”. Physica A 263: 438–451, 1999

[7] K. Nagel, D.E. Wolf, P. Wagner, P. Simon. “*Two-lane traffic rules for cellular automata: A systematic approach*”. Phys. Rev. E 58 (2): 1425–1437, 1998

[8] Rachman Rifai. “*Spatial Modelling and Risk Assessment of Sidoarjo Mud Volcanic Flow*”. *Master Thesis*, Gadjah Mada University Indonesia, International Institute For Geo-Information Science and Earth Observation, Enschede – The Netherlands, February 2008

[9] M. Bando, K. Hasebe, A. Nakayama, A. Shibata, Y. Sugiyama. “*Dynamical model of traffic congestion and numerical simulation*”. Physical Review E, 51(2): 1035-1042, 1995

[10] D. Helbing, B. Tilch. “*Generalized force model of traffic dynamics*”. Physical Review E, 58(1): 133-138, 1998

[11] R. Jiang, Q. Wu, Z.J. Zhu. “*Full velocity difference model for a car-following theory*”. Physical Review E, 64(1): 017101-1 - 017101-4, 2001

[12] K. Nagel, M. Schreckenberg. “*A cellular automaton model for freeway traffic*”. J. Phys. I France 2: 2221–2229, 1992

Information Technology (IT) Security Framework for Kenyan Small and Medium Enterprises (SMEs)

Michael Kimwele mikekimwele@yahoo.com
Institute of Computer Science and Information Technology
Jomo Kenyatta University of Agriculture and Technology
P. O. BOX 62000- 00200 Nairobi, Kenya

Waweru Mwangi waweru_mwangi@icsit.jkuat.ac.ke
Institute of Computer Science and Information Technology
Jomo Kenyatta University of Agriculture and Technology
P. O. BOX 62000- 00200 Nairobi, Kenya

Stephen Kimani skimani@icsit.jkuat.ac.ke
Institute of Computer Science and Information Technology
Jomo Kenyatta University of Agriculture and Technology
P. O. BOX 62000- 00200 Nairobi, Kenya

Abstract

To address challenges faced by SMEs especially in Kenya, this paper aims to establish an Information Technology (IT) framework that can allow Kenyan Small and Medium Enterprises (SMEs) implement cost effective security measures. Particularly this paper discusses IT security requirements and appropriate metrics. There is evidence from the survey to suggest that despite having some IT security measures in place, Kenyan SMEs still face some serious IT security challenges. In the light of the challenges faced by Kenyan SMEs, this work recommends a framework which is supposed among other things provide some metrics of evaluating the effectiveness of implemented security measures. The framework is likely to assist SME stakeholders measure the effectiveness of their security enhancing mechanisms.

Keywords: Information Technology, Security, Metrics, Framework, Kenya, SMEs.

1. INTRODUCTION

IT security is often treated solely as a technology issue, when it should also be treated as a governance issue. In looking at the growing abundance of rules, regulations, and guidelines, it is clear that information security is not solely a technical issue, but also a corporate governance challenge.

Implementation of an effective IT security program is a matter of enlightened organizational interest. Companies are taking action to protect their own information and information entrusted to them by customers, suppliers, and other partners. They are establishing responsibility for information security in their companies and adopting programs to evaluate and address the vulnerabilities and the internal and external threats to their electronic information [1]

There is a lack of framework for action within SMEs- how to set priorities, assign tasks, get started and monitor implementation of IT security measures. To aid organizations in attacking the problem, numerous guides have been developed. These documents range from detailed technical guidance to high-level principles. But there is no recognized, standard approach at an organization-wide level to help in determining what should be done and who should do it [1]. Without such an approach, firms and particularly SMEs are unclear on how to allocate information security tasks, where to fund, and how to measure the return on investment [2].

We propose a framework that spells out what needs to be done by SMEs owners through borrowing lessons from other policy reports, guidelines, and combining these with our Kenyan experience through a survey (collected data) that was conducted to establish the current measures Kenyan SMEs have in place. This framework is supposed among other things to:

- Specify roles of SME owners in reference to IT security
- Indicate or spell out some metrics to measure the effectiveness of IT security enhancing mechanisms in SMEs
- Provide guidelines on implementation of IT security for SMEs in Kenya

The objective of the framework is to provide a way of tackling IT security challenges faced by Kenyan SMEs. In addressing this issue, this paper is organized into six sections. Following a brief introduction, the next section highlights some IT security requirements and metrics. Section three addresses the research methodology. Section four presents results and analysis. Section five discusses the recommended framework. The last section draws conclusions and future research directions.

2. IT SECURITY REQUIREMENTS AND METRICS

A survey of published literature shows that most reports on IT security [3], [4], [5], [6] cite the following requirements:

- The need for risk assessments. Risks must be understood and acknowledged and the IT security measures that are taken must be commensurate with these risks.
- The need for an IT security organizational culture.
- The need to create, communicate, implement, endorse, monitor, and enforce security policies across an organization.
- The need to make every member of the organization aware of the importance of IT security and to train them in good IT security practices.
- The need for access controls to make certain only identified and authorized users with a legitimate need access information and system resources.
- The need to monitor, audit, and review IT security measures regularly.
- The need for business continuity plans that are tested regularly.

We propose a framework that considers the above requirements in defining a coherent way of dealing with IT security in SMEs. In an endeavor to address IT security challenges in SMEs, there is need to resolve the following:

- Who is responsible for ensuring security?
- Who authorizes decisions that have to be made in regard to IT security?
- Who has to be consulted to ensure that every aspect of IT security is covered?
- Who has to be kept informed to ensure that the organization copes with resulting changes resulting from putting in place IT security measures?

To be able to measure the effectiveness of IT security measures in SMEs, our recommended framework requires that there should be some “IT security metrics”. IT security metrics are quantifiable measurements or any identifiable attributes that collectively characterize changes in security awareness/behavior of employees. It is against those metrics that the effectiveness of the proposed IT security measures in place can be evaluated.

IT security metrics should be designed to yield quantifiable information [7], [8]. The quantifiable information is useful for the following purposes:

- Comparison of security maturity
- Cost justification when insecurities occur can be clearly shown in metrics
- Indication and determination of critical and non-critical security parameters
- Redirect assets and set proper priorities for most critical security needs
- Security problem isolation

- Determine the effectiveness of security testing efforts

IT security metrics can be created to guide each aspect of security program including systems evaluation, internal security processes such as training and systems testing and risk assessment. The use of IT security metrics will allow organizations to determine effectiveness of implemented IT security processes, and control by relating results of IT security activities measurements [9].

IT security metrics may vary from one organization to another depending on the business environment of the organization in question among other factors [10]. Some of the IT security metrics which this research views are applicable to SMEs include but not limited to the following:

- Number of reported security incidents
- Number of viruses or other malicious code outbreak
- Number of comments on the IT security measures in place
- Number of reported cases for use of pirated software
- Traffic to unethical websites
- Number of virus problems resulting from opening unexpected email attachments
- Number of malicious codes resulting from downloading contents from untrusted websites
- Adherence to back up routines and procedures
- Frequency IT equipment failure
- Reported cases of compliance to IT security standards

It is by use of the above metrics that our framework finds their application in Kenyan SME environment with a view of using them to evaluate the effectiveness of implemented security controls. IT security metrics should be reviewed on a regular basis. During the review, new metrics should be developed and those found obsolete discarded. Each organization should develop its own set of IT security metrics.

3. RESEARCH METHODOLOGY

The different categories of primary data collection methods include laboratory measurements, field observations, archives/collections, questionnaires and interviews [11]. However, only questionnaires and interviews are suitable for the data required, as the opinions of a large and diverse group of people are needed. Questionnaires provide a more structured way of gathering and recording data. The research entailed a survey of SMEs in Kenya, were primary data was collected by means of a questionnaire. Most of the questions were adopted from previous studies but modified to capture data relevant to the current SME study. These were measured on a five-point likert scale whereby 1 represented “strongly agree” and 5 “strongly disagree”. A preliminary version of the questionnaire was discussed with scholars and managers. Some questions were reworded and the original structure of the questionnaire was amended.

This research is based on collected data which is then analyzed and organized to unveil some problems regarding IT security in Kenyan SMEs. We believe that to be able to address IT security issues effectively in SMEs, it is important to properly understand how IT security is currently being practiced in Kenyan SMEs. SMEs targeted in the survey included those in the consulting, recruitment, vehicle sellers, cleaning, legal, estate agent, medical, equipment leasing/rental, equipment repairs, and any others so long as the organization has got not more than 100 full time employees.

The sample consisted of:

- Formally registered businesses, the informal sector was not considered.
- The telephone directory was used to get regional distribution of SMEs
- Sectoral distribution of SMEs was based on national data from the Central Bureau of Statistics

The researchers administered the questionnaire over a period of four months between October 2009 and January 2010 to SMEs selected from all over Kenya. One hundred and twelve (112) SMEs were randomly identified to participate in the survey. The researchers then contacted the

SMEs requesting them to participate in the survey. Those who responded positively were then e-mailed the questionnaire which they were free to fill and e-mail back or they could fill and inform the researchers when to pick. In some cases, the questionnaire was delivered physically by the researchers and picked. The respondents were assured that all personal respondents would remain strictly confidential. Finally, twenty one (21) completed questionnaires were collected.

The respondents included business decision makers, IT managers, or people who take care of computers systems in SMEs. Out of the 21 SMEs that participated in the questionnaire survey, thirteen agreed to post-survey interviews to obtain “richer” information about IT security issues affecting them. As a consequence, in addition to responses to the questionnaire, other useful insights were also gathered. The exact of respondents in terms of nature of business, length of time the business has been in operation, current number of employees, number of computers used in the businesses and how long they have used computers are represented in Table 1 through to Table 5.

TABLE 1: What is the nature of your business?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Consulting	5	23.8	23.8	23.8
	Computers	3	14.3	14.3	38.1
	Equipment Repairs	2	9.5	9.5	47.6
	Other Professional Service	6	28.6	28.6	76.2
	Recruitment	1	4.8	4.8	81.0
	Vehicle Services	1	4.8	4.8	85.7
	Estate Agent	3	14.3	14.3	100.0
	Total	21	100.0	100.0	

Table 1 shows the nature of the surveyed firms in terms of their operations. Majority of the enterprises are in Consulting and Professional Services.

TABLE 2: How long has the business in operation?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	2	9.5	9.5	9.5
	2	2	9.5	9.5	19.0
	3	1	4.8	4.8	23.8
	4	2	9.5	9.5	33.3
	5	3	14.3	14.3	47.6
	6	1	4.8	4.8	52.4
	7	2	9.5	9.5	61.9
	8	2	9.5	9.5	71.4
	10	2	9.5	9.5	81.0
	12	1	4.8	4.8	85.7
	14	1	4.8	4.8	90.5
	37	1	4.8	4.8	95.2
	89	1	4.8	4.8	100.0
	Total	21	100.0	100.0	

Table 2 shows the length of time (years) the surveyed SMEs have been in operation. More than 90% of firms surveyed were less than 14 years old.

TABLE 3: What is your current number of employees?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0-5	4	19.0	19.0	19.0
	11-25	6	28.6	28.6	47.6
	36-50	1	4.8	4.8	52.4
	51-	5	23.8	23.8	76.2
	6-10	5	23.8	23.8	100.0
	Total	21	100.0	100.0	

From Table 3, we note that majority of the SMEs surveyed had 11-25 employees (28.6%), followed by 6-10 employees (23.8%) and 51-upwards (23.8%).

TABLE 4: How many computers do you use in your business?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	2	9.5	9.5	9.5
	2	1	4.8	4.8	14.3
	3	2	9.5	9.5	23.8
	5	2	9.5	9.5	33.3
	6	1	4.8	4.8	38.1
	7	1	4.8	4.8	42.9
	9	2	9.5	9.5	52.4
	11	1	4.8	4.8	57.1
	14	2	9.5	9.5	66.7
	15	1	4.8	4.8	71.4
	25	1	4.8	4.8	76.2
	35	1	4.8	4.8	81.0
	40	1	4.8	4.8	85.7
	50	1	4.8	4.8	90.5
	60	1	4.8	4.8	95.2
	80	1	4.8	4.8	100.0
	Total	21	100.0	100.0	

From Table 4, it is evident that more than 50% of the surveyed SMEs were using not more than 15 computers in their operations.

TABLE 5: How long have you been using computers in your

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	4	19.0	19.0	19.0
	3	2	9.5	9.5	28.6
	4	3	14.3	14.3	42.9
	5	2	9.5	9.5	52.4
	7	3	14.3	14.3	66.7
	8	1	4.8	4.8	71.4
	10	3	14.3	14.3	85.7
	14	1	4.8	4.8	90.5
	15	1	4.8	4.8	95.2
	19	1	4.8	4.8	100.0
	Total	21	100.0	100.0	

19% of the respondents have been using computers in their operations for one year or less while 4.8% have been using computers for 19 years as shown in Table 5.

4. RESULTS AND ANALYSIS

The survey was conducted to establish the nature of IT infrastructure particularly its organization, employees and state of security measures. Through the interviews we conducted, SMEs pointed out the need for the following to be incorporated in a security enhancing mechanism for SMEs

- Create more awareness programs amongst SMEs and offer them related products to help in protection
- Education on the topic of Internet security
- Hold vulnerability seminars to try and show SMEs what goes wrong in their day to day operations

Considering the proportion and scope of SMEs in Kenya, poor information technology security of SMEs can yield catastrophic results both socially and economically. Among the issues considered in the survey, the following were found to be SME problem areas:

- Security Policy: 47.6% of respondents strongly agreed and agreed that their organizations have a well documented information security policy.

TABLE 6: We have a documented Information Security policy

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	1	4.8	4.8	4.8
	Agree	9	42.9	42.9	47.6
	Undecided	2	9.5	9.5	57.1
	Disagree	6	28.6	28.6	85.7
	Strongly Disagree	3	14.3	14.3	100.0
	Total	21	100.0	100.0	

- Organizational Security: 38.1% of respondents reported having a director (or equivalent) member of staff being responsible for IT security.

TABLE 7: A Director (or equivalent) member of our staff has the responsibility for Information Technology security

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	4	19.0	19.0	19.0
	Agree	4	19.0	19.0	38.1
	Undecided	9	42.9	42.9	81.0
	Disagree	3	14.3	14.3	95.2
	Strongly Disagree	1	4.8	4.8	100.0
	Total	21	100.0	100.0	

- Personnel Security: Only 42.9% of employees have been trained to secure their computers at all times, especially when moving away from their workstations.

TABLE 8: Staff have been trained to secure their computers at all times, when moving away from their work stations

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	4	19.0	19.0	19.0
	Agree	5	23.8	23.8	42.9
	Undecided	3	14.3	14.3	57.1
	Disagree	7	33.3	33.3	90.5
	Strongly Disagree	2	9.5	9.5	100.0
	Total	21	100.0	100.0	

- Communications and Operations Management: 47.6% of respondents reported that they are confident, that in the event of equipment failure, theft or a site disaster, their back ups and storage would enable them to retrieve their information systems with minimal business interruption.

TABLE 9: We are confident, that in the event of equipment failure, theft or a site disaster, our data back ups and storage would enable us retrieve our information with minimal business interruption

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	3	14.3	14.3	14.3
	Agree	7	33.3	33.3	47.6
	Undecided	3	14.3	14.3	61.9
	Disagree	6	28.6	28.6	90.5
	Strongly Disagree	2	9.5	9.5	100.0
	Total	21	100.0	100.0	

- Business Continuity Management: 28.6% have a business continuity plan which specifies who must take action and what has to be done to ensure that the organization can continue functioning in the event of a disaster such as a fire/flood.

TABLE 10: We have a business continuity plan which specifies who must take what action and what has to be done to ensure that the organization can continue functioning in the event of a disaster such as fire/flood

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	1	4.8	4.8	4.8
	Agree	5	23.8	23.8	28.6
	Undecided	7	33.3	33.3	61.9
	Disagree	6	28.6	28.6	90.5
	Strongly Disagree	2	9.5	9.5	100.0
	Total	21	100.0	100.0	

- IT Security Standards: Despite the fact that there are some standards which organizations can adopt, 52.4% of SMEs surveyed reported that they were aware of any standards they could adopt.

TABLE 11: Prior to this survey, I was aware that there are established, international information security standards, available for organizations to adopt

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	3	14.3	14.3	14.3
	Agree	8	38.1	38.1	52.4
	Undecided	2	9.5	9.5	61.9
	Disagree	6	28.6	28.6	90.5
	Strongly Disagree	2	9.5	9.5	100.0
	Total	21	100.0	100.0	

In view of the above problem areas, we recommend that SMEs should adopt the following in their quest to realize enhanced IT security:

- Development of IT security policies
- Identification of roles and responsibilities of each individual regarding IT security
- Make all employees aware of IT security issues
- Select and implement appropriate security measures
- Put in place data recovery measures in case of accidents
- Identify and protect all organizational assets that need to be protected
- Adopt appropriate IT security standards

We aim at synthesizing from the discussions, analysis, and interpretations made so far in an attempt to establish a means that can help in evaluation, formation, and implementation of possible IT security controls to address the security situation observed and described in the previous section. Based on empirical analysis of security practices in organizations, this work proposes a framework that can be used to evaluate SME IT security measures.

The resulting framework brings together numerous concepts into a coherent explanation that should be useful for SMEs or any other individual seeking to evaluate the effectiveness of implemented security measures. Because of limited IT budgets for SMEs, the framework is necessary to enable SMEs evaluate IT security measures at low costs.

5. IT SECURITY FRAMEWORK FOR SMES

Our recommended framework consists of the following:

- A mapping of identified IT security metrics and the IT security issues/activities/aspects the metrics can measure (Table 12).
- An approach for tackling IT security issues which deals with continual improvement and establishment of new measures should the implemented ones at any one particular time appear ineffective (Figure 2).
- An illustration of how the approach can be utilized in an IT security enhancing mechanism for SMEs. This illustration is done using data that was collected during the survey (Table 13).

		IT SECURITY METRICS									
		Number of reported security incidents	Number of viruses or other malicious code outbreak	Number of comments on the IT security measures in place	Number of cases for use of pirated software	Traffic to unethical websites	Number of virus problems resulting from opening unexpected email attachments	Number of malicious codes resulting from downloading contents from untrusted websites	Adherence to back up routines and procedures	Frequency of IT equipment failure	Reported cases of compliance to IT security standards
IT CONTROL ISSUES/ACTIVITIES/ASPECTS	**Security Policy** (Is our IT security policy effective?)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Organizational security (Is there a Director or equivalent member of staff responsible for IT security?)			✓						✓	✓
	Asset Control (Can all assets including hardware and software used for information security handling be identified and located?)								✓		
	Personnel Security (Are Staff aware that security incidents should be reported to management immediately?)	✓	✓	✓							
	Physical and Environmental Security (Is there appropriate physical and environmental security procedures in place to prevent interference with business premises and IT systems?)			✓						✓	
	Communications and Operations Management (Are we confident that our anti-virus systems are up to date, and in the event of a virus outbreak, we should be able to protect our systems?)	✓	✓				✓	✓			✓
	Access Control (Can users logon/gain access to our systems without being formally registered with their own user account?)			✓							✓
	System Development and Maintenance (Can our systems provide audit trails so that usage of the system and data input/changes can be audited?)		✓			✓		✓			✓
	Business Continuity Management (Have our security measures been reviewed within the last year?)								✓		✓
	Compliance (Is our organization aware that there are established, international IT security standards available for adoption?)	✓									✓

TABLE 12: Mapping of IT Security Metrics and the IT Security Issues/Activities/Aspects they can Measure

Table 12 demonstrates various IT security control issues/activities/aspects and the metrics which can be used to measure such issues. Although metrics have been proposed over a long period of time, an ideal metrics is one which is easy to understand, effective and efficient [12]. In order to develop an ideal metric, metrics should be validated and characterized effectively.

For a security awareness program to be effective, it has to be recursive and must be evaluated on regular intervals based on predefined corporate awareness metrics [10]. Casmir [10] further suggests that an organization's information security program should be recursive and cyclic in nature as depicted below:

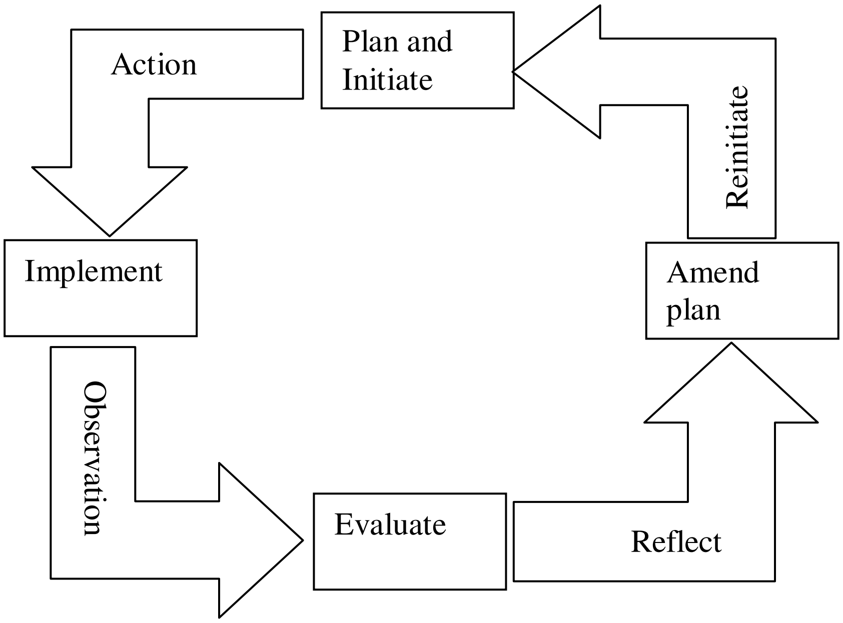


FIGURE 1: Information security awareness program lifecycle [10]

Our framework recommends the following approach to tackling IT security issues in SMEs (Figure 2). This approach is based on the recursive lifecycle put forward by Casmir (Figure 1).

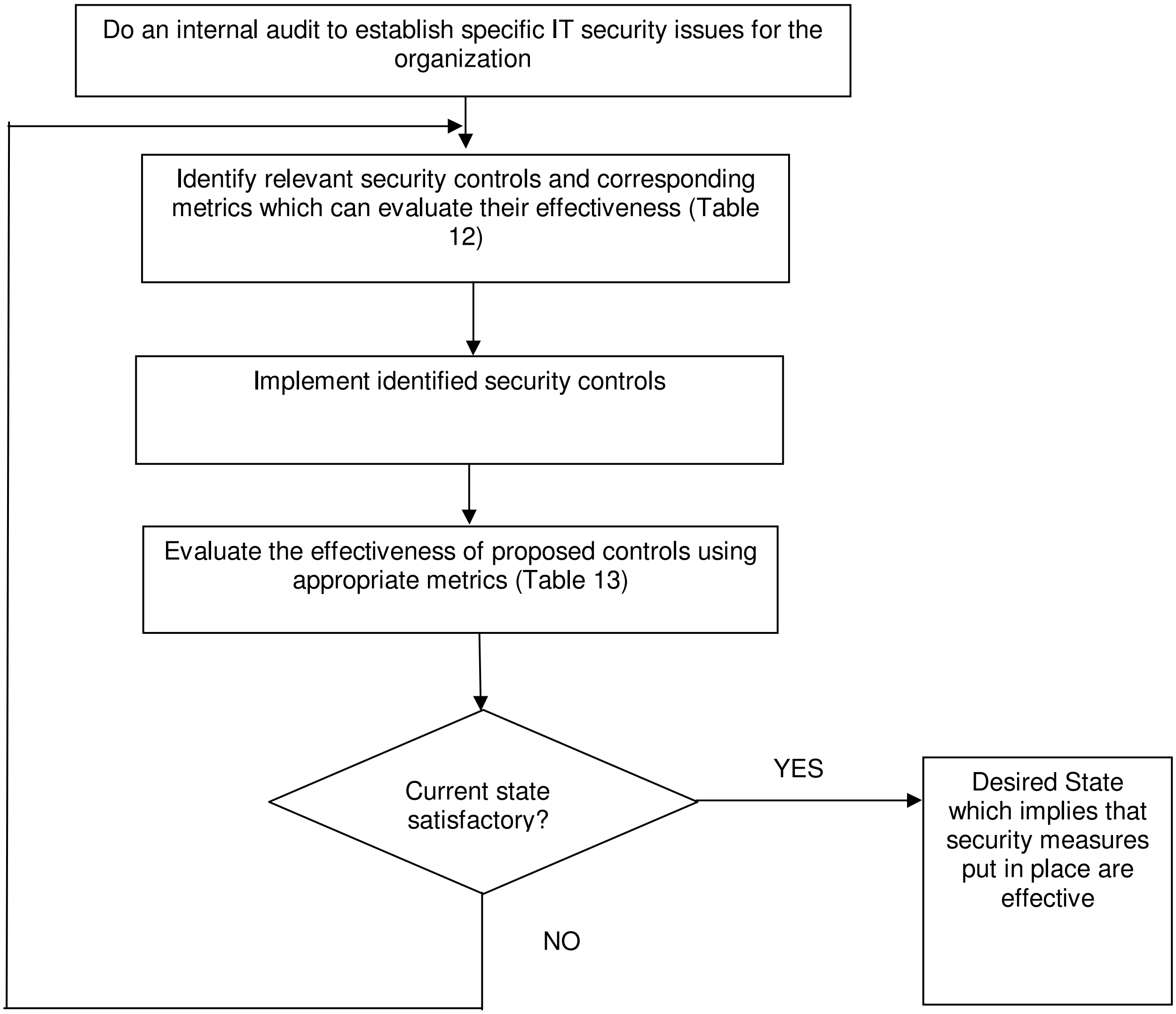

Do an internal audit to establish specific IT security issues for the organization
Identify relevant security controls and corresponding metrics which can evaluate their effectiveness (Table 12)
Implement identified security controls
Evaluate the effectiveness of proposed controls using appropriate metrics (Table 13)
Current state satisfactory?
YES
NO
Desired State which implies that security measures put in place are effective

FIGURE 2: Approach for evaluating the effectiveness of IT security measures in SMEs

In Table 13 below we provide a summary of selected SMEs in terms of the security controls they have in place and then evaluate them in light of the security breaches the organizations have suffered within the past year. Through this it is possible to examine and show that some measures are effective than other based on experience of the surveyed SMEs.

IMPLEMENTED SECURITY CONTROLS	**SME 1**	**SME 2**	**SME 3**	**SME 4**
Have a security policy	YES	YES	YES	YES
A director (or equivalent) member of staff has responsibility for IT security	NO	YES	YES	YES
All assets can be identified	NO	YES	YES	YES
Security incidents are reported to management immediately	NO	NO	YES	YES
Have appropriate physical and environmental procedures	YES	YES	YES	YES
Up to date antivirus systems	YES	YES	YES	YES
Proper system access control mechanisms like user accounts	YES	YES	YES	YES
System usage audit trails	NO	NO	NO	NO
Security measures have been reviewed within past year	YES	NO	YES	YES
Adopted/Complied with IT security standards	NO	NO	NO	NO
SECURITY BREACHES SUFFERED WITHIN PAST YEAR				
No information security breeches				
Inadvertent breech (e.g. user accidentally deleted files or changed computer configuration)	✓	✓		
Deliberate attack (e.g. hacker/disgruntled staff gained access, deleting or stealing data)			✓	✓
Asset theft (e.g. software application misplaced causing re-installation delay/costs)	✓	✓		
Equipment failure (e.g. hard drive crashed causing loss of data and business disruption)	✓		✓	✓
Back up failure (e.g. system restore failure due to corrupt/ inadequate back ups)			✓	
Data theft (e.g. espionage which resulted in data loss and possible legal exposure)				
Site disaster (e.g. fire or flood causing damage to systems and business disruption)	✓			
Copyright infringement (e.g. staff loading pirated software, legally exposing the organization)	✓			✓
Compliance (e.g. passing on confidential information, legally exposing the organization)	✓			

TABLE 13: Implemented Security Controls and Security breaches suffered within the last year

The above checklist (Table 13) is an illustration of the use of the recommended approach in Figure 2 above. The illustration is based on four randomly selected SMEs from the survey. It shows that despite SMEs having implemented various security controls, they still suffered various security breaches within the past one year. This is essential in determining whether the current state of affairs (security controls in place and resulting reduction/increase in security breaches) is satisfactory. In the event that the security breaches increase in number and the organization considers them significant, then as per our approach, new controls should be established and the process as shown in figure 2 iterated/repeated. This process should continue until the organization is satisfied that the security measures/controls in place yield the desired results/state in terms of IT security.

It is worth appreciating the fact that in our checklist (Table 13) time is essential since the security breaches have to be observed and reported over a determined time (say, one year). This helps in measuring the effectiveness of implemented security controls and is also consistent with the way other metrics are established/defined. For instance, Reliability can be defined as the ability of the software product to perform its required functions under stated conditions for a specified period of time, or a specified number of operations. Reliability can be measured using ‘mean time between failure’ (MTBF), which is the average time between successive failures [12]. A similar measure to MTBF is ‘mean time to repair’ (MTTR) which is the average time taken to repair the software after a failure occurs.

6. CONCLUSION & FUTURE WORK

To address current difficulties of organizations reluctant to invest in IT security due to cost, this work proposes an IT security implementation framework that will allow SMEs adopt cost effective security measures whose effectiveness can be evaluated using appropriate metrics.

This framework is significant in that it allows SMEs to take necessary security measures and to realize what actions they can take in case they are faced with IT security issues. This will help SMEs protect their information assets. It is also significant in that it is a new approach presenting an IT security framework for SMEs that is recursive and cyclic and therefore can be improved continually in line with the changing IT security landscape.

Since the framework has not been tested in a real working environment of SMEs, further analysis on the effectiveness of the framework is required, and the results should be reflected in future frameworks.

ACKNOWLEDGEMENT

The authors would like to thank the German Academic Exchange Service (DAAD) for funding this research.

7. REFERENCES

1. B. Conner et al., (2004), Business Software Alliance, http://www.bsa.org [20/8/2010]

2. R. Casmir and L. Yngstrom (2005), Towards a Dynamic and Adaptive Information Awareness Approach. In proceedings of the fourth world conference on information security education, Moscow, Russia, ISBN: 5-7262-0565-0

3. C. T. Upfold and D. A. Sewry (2005), An Investigation of Information Security in Small and Medium Enterprises (SME's) in the Eastern Cape.

4. C. N. Tarimo (2006), ICT Security Readiness Checklist for Developing Countries: A Social-Technical Approach, Stockholm University, Department of Computer and Systems Sciences, December 2006.

5. M. R. Pattinson and G. Anderson, G (2007), "How Well are Information Risks being Communicated to your Computer end-users?" Information Management and Computer Security, Vol. 15. No. 5. (2007), pp 362-371

6. R. Werlinger et al. (2009), "An Integrated View of Human, Organizational, and Technological Challenges of IT Security", Information Management and Computer Security, Vol. 17. No. 1. (2009)

7. M. Swanson, N. Bartol, J. Sabato, J. Hash, and L. Graffo (2003), Security Metrics Guide for Information Technology Systems. http://csrc.nist.gov/csspab/june13-15/sec-metrics.html [16/8/2010]

8. P. E. Ammann P. E and Black, P. E. (2001), "A Specification-Based Coverage Metric to Evaluate Test Sets", International Journal of Reliability, Quality, and Safety Engineering, Vol. 8 No. 4, pp 275-300; Singapore, World Scientific Publishing.

9. J. A. Chaula (2006), "A Socio-Technical Analysis of Information Systems Security Assurance: A Case Study for Effective Assurance", Stockholm University: Department of Computer and Systems Sciences, Report Series/DSV No. 06-016, ISSN 1101-8526

10. R. Casmir (2005), A Dynamic and Adaptive Information Security Awareness (DAISA) Approach, Stockholm University, Department of Computer and Systems Sciences, December 2005.

11. J. A. Sharp and K. Howard (1998), The Management of a Student Research Project, 2nd Edition. http://www.hlss.mmu.ac.uk/infocomms/people/staffpub/rjh.doc [12/2/2010]

12. R. Khurana (2007), Software Engineering: Principles and Practices, ITL Education Solutions Ltd, New Delhi, India, 2007.

Image Recognition With the Help of Auto-Associative Neural Network

Moumi Pandit moumi_pandit@yahoo.co.in
Department of Electrical and Electronics Engineering
Sikkim Manipal Institute of Technology
Majhitar,Rangpo,East Sikkim-737132,India

Mousumi Gupta mousmi_gt@yahoo.co.in
Department of computer science Engineering
Sikkim Manipal Institute of Technology
Majhitar,Rangpo,East Sikkim-737132,India

Abstract

This paper proposes a Neural Network model that has been utilized for image recognition. The main issue of Neural Network model here is to train the system for image recognition. In this paper the NN model has been prepared in MATLAB platform. The NN model uses Auto-Associative memory for training. The model reads the image in the form of a matrix, evaluates the weight matrix associated with the image. After training process is done, whenever the image is provided to the system the model recognizes it appropriately. The weight matrix evaluated here is used for image pattern matching. It is noticed that the model developed is accurate enough to recognize the image even if the image is distorted or some portion/ data is missing from the image. This model eliminates the long time consuming process of image recognition.

Keywords: Image Recognition, Artificial Neural Network, Pattern Matching, Associative Memory, Weight Matrix.

1. INTRODUCTION

Neural network as the name suggests is interconnection of nerve cells. The nervous system in human brain is highly interconnected neural cells which makes the nervous system. The Artificial Neural Network technology is built up with a inspiration of functioning of human nervous system. Many of human intelligent behavior which is the direct functioning of human nervous system are implemented artificially by using Artificial Neural Network. Artificial neural network is an information processing devices, which are built from interconnected elementary processing elements called neurons. It is inspired by the way biological nervous systems works.

ANN is composed of a large number of highly interconnected processing elements working in union to solve specific problems. Like human, artificial neural network also learn by example. ANN is configured for specific application, such as pattern recognition or data classification through learning process. Learning involves adjustments to the synaptic connection known as weights that exist between the neurons [8] [9].

In artificial neural network, the information processing elements are known as nodes. There are two or more layers of nodes. The first layers of nodes are known as input layer whereas the last layer is known as output layer. The layers in between which may or may not exist is known as hidden layer(s).The information is transmitted by means of connecting links. These links possess an associated weight, which is multiplied with the incoming signal for any typical neural network. The output is obtained by applying activations to the net [8] [9].

Image recognition is a key component in application areas like biometric identification. Image recognition is also one of the important functions relevant to image processing of brain in addition to image segmentation and associative memory. For this reason, many studies on the image recognition can be found in computer vision and computational intelligence, e.g., see [8], [7]. It is not a surprising to see that actually the human identifying methods by possessions (cards, badges, keys) or by knowledge (userid, password, Personal Identification Number (PIN)), are being replaced by biometrics (fingerprint, face, ear). A human being has the capacity to memorize a pattern and can also recall it.

It is well-known that neural network is effective for classification problems. Some studies that a neural network was applied to Braille recognition have been reported. In [9], Braille documents read by tactile were considered as time series information, and a new SOM architecture with feedback connections was proposed. Wang et al. have introduced the coupled neural oscillator networks to model synchronous oscillatory firings and applied it to image segmentation [3]

The hierarchical neural network with back-propagation method is widely used as network model. However, it requires a lot of time for learning. Furthermore, modifying, adding and deleting memory patterns are not easy. Here Auto Associative Neural Network has been used because the training time is comparatively lower than previous mentioned methods.

2. ARCHITECTURE OF AUTO-ASSOCIATIVE NEURAL NETWORK

An Auto-Associative Neural Network is basically feed forward multilayered neural network which has same number of nodes in the input layer and the output layer. The output layer is actually the computing layer.

The architecture of Auto-Associative Neural Network is given in FIGURE 1. The inputs are given in matrix[x] ,the output is given in matrix [y] and the associated weights are in matrix [w].

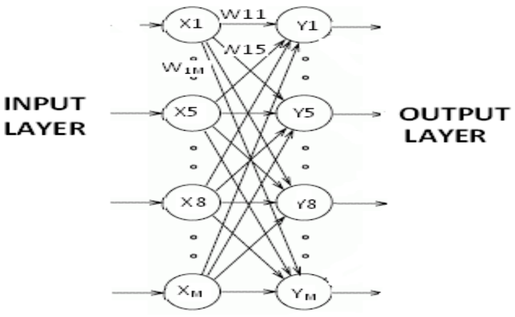


FIGURE1: Architecture of auto-associative network

The output of the matrix[y] is can be represented as:

$$\begin{bmatrix} y_{k1} \\ y_{k2} \\ \vdots \\ y_{km} \end{bmatrix} = \begin{bmatrix} w_{i1} & w_{i2} & w_{1m} \\ w_{21} & w_{22} & w_{2m} \\ \vdots & \vdots & \vdots \\ w_{m1} & w_{m2} & w_{mm} \end{bmatrix} \begin{bmatrix} x_{k1} \\ x_{k2} \\ \vdots \\ x_{km} \end{bmatrix} \qquad \text{...............(i)}$$

$$\begin{bmatrix} w_{i1} & w_{i2} & w_{1m} \\ w_{21} & w_{22} & w_{2m} \\ \vdots & \vdots & \vdots \\ w_{m1} & w_{m2} & w_{mm} \end{bmatrix} = \begin{bmatrix} x_{k1} \\ x_{k2} \\ \vdots \\ x_{km} \end{bmatrix} \begin{bmatrix} y_{k1} \\ y_{k2} \\ \vdots \\ y_{km} \end{bmatrix}^{t} \qquad \text{..............(ii)}$$

When two vectors are processed with outer products the result is a matrix. If one of the two vectors u is having m rows and the other vector v is having n column. Their outer product is defined by a matrix whose dimention is m*n and is defined as u * v^t. The resulting matrix can map the vectors. Applying this rule to the auto associative memory we have:

$$[w(k)] = [x_k] *[y_k^t]$$

The resulting matrix obtained by finding the outer product of vector [Y_k] and[X_k] should be considered associative memory. If in the considered associative memory Neural Network we assume [X_k] = [Y_K] hence the weight matrix becomes [x_k]*[x_k^t].

Let us consider two examples:

Exampe1:

A vector [X] = [1 1 -1 -1] is given as input to the Auto-Associative network. The weight matrix w can then be calculated as :

[w]=[x]*[y]^t, where y is the output. As already mentioned that in auto associative net the output and the input is same so [x]=[y],therefore the weight matrix becomes

$$[w]=[x]*[x]^t= [1\ 1\ -1 -1] \begin{bmatrix} 1 \\ 1 \\ -1 \\ -1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 \\ -1 & -1 & 1 & 1 \end{bmatrix}$$

$$[Y] =[W]*[X]= \begin{bmatrix} 4 \\ 4 \\ -4 \\ -4 \end{bmatrix}$$

The output is passed through activation function. Here the condition is if the input is 1 or above then then the output will be 1.if it is -1 or below then the output will be -1.Passing the output through activation function the output becomes $\begin{bmatrix} 1 \\ 1 \\ -1 \\ -1 \end{bmatrix}$ which is same as the given vector[x].

Example2:

Now, if the input matrix is changed slightly and it is taken as [0 1 -1 -1].then the output will be :

$$[Y] = [W]*[X]= \begin{bmatrix} 3 \\ 3 \\ -3 \\ -3 \end{bmatrix}$$

The output is passed through activation function. Here the condition is if the input is 1 or above then then the output will be 1.if it is -1 or below then the output will be -

Passing the output through activation function the output becomes $\begin{bmatrix} 1 \\ 1 \\ -1 \\ -1 \end{bmatrix}$.

The same example can be implemented in real life application as in case of image recognition where the image can be read as a matrix with the help of MATLAB. Even if the image is slightly distorted or some data gets lost then also we can recognize the image provided the distortion do not change the image completely. Firstly the computer is trained with a particular image. The weight matrix is found out. Secondly, the net is tested to check whether it is working properly.

3. DEVELOPMENT OF THE NETWORK

3.1 Training the Network

An Auto-Associative neural network has a very simple architecture. It has an input layer and an output layer. The input layer is linked with the output layer with associated weights. In this process the input and the output is the same that is, the same image is used as input and output. The network is thus trained with an image and associated weight is found out as in (ii) i.e.

When the output matrix is [y], the input matrix is [x] and the weight matrix is [w] then:

$$\begin{bmatrix} w_{i1} & w_{i2} & w_{1m} \\ w_{21} & w_{22} & w_{2m} \\ \vdots & \vdots & \vdots \\ w_{m1} & w_{m2} & w_{mm} \end{bmatrix} = \begin{bmatrix} x_{k1} \\ x_{k2} \\ \vdots \\ x_{km} \end{bmatrix} \begin{bmatrix} y_{k1} \\ y_{k2} \\ \vdots \\ y_{km} \end{bmatrix}^{t} \qquad \text{..............(ii)}$$

Where the input matrix is the image read as matrix[x], the output matrix is the same image read as matrix [y] and the weight matrix[w] is calculated by using (ii). As the input and output is the same matrix of the same image we can say [y]=[x],so we can rewrite (ii) as:

$$\begin{bmatrix} w_{i1} & w_{i2} & w_{1m} \\ w_{21} & w_{22} & w_{2m} \\ \vdots & \vdots & \vdots \\ w_{m1} & w_{m2} & w_{mm} \end{bmatrix} = \begin{bmatrix} x_{k1} \\ x_{k2} \\ \vdots \\ x_{km} \end{bmatrix} \begin{bmatrix} x_{k1} \\ x_{k2} \\ \vdots \\ x_{km} \end{bmatrix}^{t} \qquad \text{..............(iii)}$$

3.2 Testing the Network

Case 1: Testing with same image

For testing, first the same image is given to the network as input. The image is read as matrix. The weight matrix is same as calculated during training the network by equation(iii).The output [y] was calculated with (i) i.e.:

$$\begin{bmatrix} y_{k1} \\ y_{k2} \\ \vdots \\ y_{km} \end{bmatrix} = \begin{bmatrix} w_{i1} & w_{i2} & w_{1m} \\ w_{21} & w_{22} & w_{2m} \\ \vdots & \vdots & \vdots \\ w_{m1} & w_{m2} & w_{mm} \end{bmatrix} \begin{bmatrix} x_{k1} \\ x_{k2} \\ \vdots \\ x_{km} \end{bmatrix}$$

Now the output matrix[y] is passed through activation function and then compared with input matrix [x]. As the input and output matrix is same the image is declared to be ”**same**”.

Case 2: Testing with different image:

A different image is given as input. The weight matrix is same as calculated during training the network by equation (iii).Now the output is calculated as in (i)

$$\begin{bmatrix} y_{k1} \\ y_{k2} \\ \vdots \\ y_{km} \end{bmatrix} = \begin{bmatrix} w_{i1} & w_{i2} & w_{1m} \\ w_{21} & w_{22} & w_{2m} \\ \vdots & \vdots & \vdots \\ w_{m1} & w_{m2} & w_{mm} \end{bmatrix} \begin{bmatrix} x_{k1} \\ x_{k2} \\ \vdots \\ x_{km} \end{bmatrix}$$

Now the output matrix[y] is passed through threshold function and the compared to the input matrix[x]. As the input and output matrix is not same the image is declared to be" **not same**".

Case 3: With distorted form of same image

Though the brightness of the image is changed but the image is same. So the matrix [x] will be same. The weight matrix is same as calculated during training the network by equation(iii). Then again the output matrix [y] is calculated using equation (i) as done in earlier two cases. The output [y] is then passed through activation function and then compared with input matrix [x]. As they are same the image is declared to be "**same**".

Case 4: With same image but with some data missing:

Now in this case the same image is given but with slight change ie some data is missing. This case is same given in example 2. Here the input image is same as the trained one but with some data missing. The matrix is calculated as in equation (i). Though the output is slightly different from the input ,but after passing through the activation it becomes the same. So ,the image is again declared **"same"**.

The main advantages of this process**:**

i) The process is very simple

ii) Do not require any specific complicated software or hardware.

iii) Computational time is very less.

iv) Image can be recognized even if it is distorted.

v) Cost effective.

4. ALGORITHM

The algorithm for training the network and testing it is given below.

4.1 Training the Net

Step1: The image [y] is read in the form of square matrix [x] [mXm].

Step2: The image is changed to grayscale if it is in RGB format.

Step3: The matrix may be reduced to suitable size for quicker result.

Step4: The Gray scale image has been converted to binary 0,1 image (B1) by using a user defined threshold(t) parameter. The Gray value >= t is converted to 1 in original image. The gray value <t converted to 0.

Step5: The weight matrix is calculated as $[w] = [x] \times [x]^t$ ………. (A)

4.2 Testing the Output

Step1: Various images are taken as input in form of matrix [x] and changed it to grayscale. The matrix (B2) is then changed in terms of 0 and 1 using the previous threshold function as stated above. The matrix may be reduced to the size as given in training process i,e m X m matrix for quicker result.

Step2: Weight matrix [w] as evaluated by (A) is provided to the network.

Step3: Output is calculated as:

[Y]=[W]*[X] where [Y] is the output matrix.

Step4: The output is passed through the activation function by using equ (B) and output image is converted to 0 or 1.

```
Step5: For i=1 to m
          For j=1 to m
 if matrix B1== matrix B2
Then display the Y is matched
Otherwise Y not matched.
```

5. RESULT AND ANALYSIS

In the proposed method, auto-associative network is used for image recognition. The entire work is done in two parts: Firstly the network is trained with a particular image. The weight matrix is calculated which is acting as the mapping function. Once the network is trained, it can be used for matching the matrices for image recognition. In our work we have used gray scale images which have later been reconstructed as a square matrix. The whole process was done in MATLAB platform.

Here the network is trained with a gray scale image of a graph which is in JPEG. This validity of the process is tested with four different kind of images and has proved to be successful. The method is successful in recognizing the image even if the brightness of the image is reduced by 80%. Moreover the method can successfully recognize the image even if 10% data of the trained image is missing.

The network can be trained with various kinds of images whether it is in grayscale or it is a color image. The performance of the system is invariant to the size and brightness of the image. By using this method the network tests the identity of an image in 0.25 seconds in a Pentium machine at 500 MHz, and gives an average recognition rate of 99%. This technique is computationally inexpensive and involves only three parameters that are input, output and a weight matrix.

The training of the network is done by the following image;

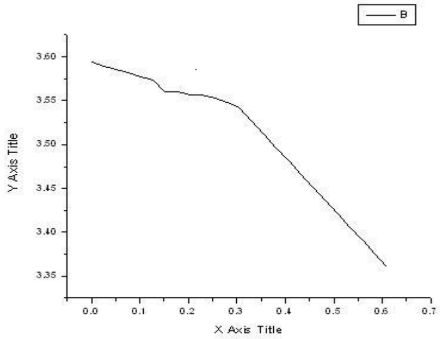


FIGURE2: Image with which the network is trained

The image was read as 5*5 matrix in term of 0 and 1. The weight matrix of this particular image was found to be:

$$\begin{bmatrix} 5 & 5 & 5 & 5 & 5 \\ 5 & 5 & 5 & 5 & 5 \\ 5 & 5 & 5 & 5 & 5 \\ 5 & 5 & 5 & 5 & 5 \\ 5 & 5 & 5 & 5 & 5 \end{bmatrix}$$

This weight matrix will be used as mapping parameter for image recognition. The output is tested based on four kinds of data as discussed in the following four cases:

Data 1: With the same image

Data 2: With different image

Data 3: With same image but distorted

Data 4: With the same image but some data missing

5.1 Case1- With the Same Image

The same image with which the network was trained is given as input as given in FIGURE 3. The weight matrix which was derived after training the network is also given. It was seen that with the same image the output given was “**same**”.

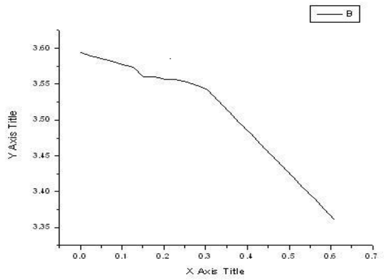


FIGURE3: The same image with which the training was done

5.2 Case 2-With Different Image

Now a different image image as given in FIGURE4 trained is given to the network as input. The weight matrix which was derived after training the network is also given. It was seen that with the different image the output given was “**not same**”

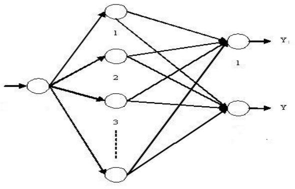


FIGURE4. A different image

5.3 Case 3- With Same Image Dut Distorted

The same image with which the network was trained is given as input with lot of distortion i.e the brightness of the has been changed completely as shown in FIGURE 5. The weight matrix which was derived after training the network is also given. It was seen that with the distorted form of the same image the output given was “match”.

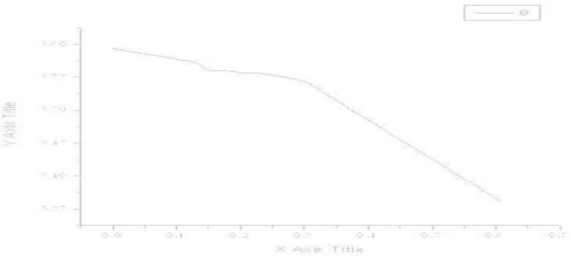


FIGURE 5: The distorted form of same image with which the training was done

5.4 Case 4 - With the Same Image But Some Data Missing

The same image with which the network was trained is given as input with some data missing as shown in FIGURE 6. The weight matrix which was derived after training the network is also given. It was seen that with the distorted form of the same image the output given was “match”.

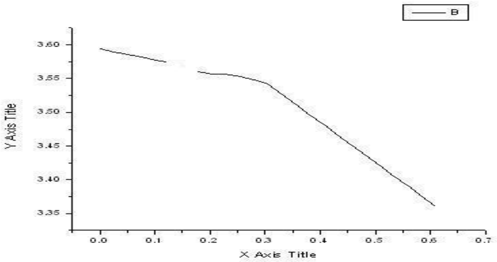


FIGURE 6: The same image with which the training was done but with some data missing

The whole process was done in MATLAB platform. This process is tested with numerous images and has proved to be successful. The proposed method takes less than 0.5 secs for recognizing. From experimental results we have to

5.5 Comparison With Others Algorithm

The authors [5] [9] uses different parameters to get optimum recognition rate, the parameters they have used were distance measurement technique to find distance between two points for face recognition. The calculation for different parameters increases the computational time and its complexity.

The strength in our proposed methods is that we are using very few parameters to train the system. Therefore we can conclude that the proposed method is able to train the image and gives output within very short memory space requirement, and the network can be trained with even one image.

6. CONCLUSION AND FUTURE WORK

In this paper an image recognition model for pattern matching has been proposed. The weight matrix is the correlation matrix and the advantage of correlation matrix is the ease of storing new association or deleting odd ones. The image is trained with the proposed auto associative memory architecture. The advantage of this model is training time is very less and this model recognize the image even if the original image contains less information.

The limitation of this model is that it can store only m-1 images for recognition where m is the number of elements in the input matrix. To improve the performance, input patterns can be selected orthogonal among themselves [8] [9]. Storing of more than one image can be done by simply updating the current weight matrix by adding the weight matrix of the new image [9]. The future scope of this project is to overcome this limitation.

7. REFERENCES

1. **FOR JOURNALS:** M. Burl, T. Leung, and P. Persona. "*Recognition of Planar Object Classes*". In Proc. IEEE Comput. Soc. Con! Computer. Vision and Pattern Recognition., 223-230 ,1996.

2. **FOR JOURNALS** : H. Waukee, H. Harada, *et al.* “*An Architecture of Self-Organizing Map for Temporal Processing and Its Application to a Braille Recognition Task,*” *IEICE Trans. on Information and Systems*, J87(3), 884–892, 2004.

3. **FOR JOURNALS** : Wang, D. L., & Terman, D. "*Locally excitatory globally inhibitory oscillator networks.*" IEEE Trans. Neural Networks, 6, 283-286 1995.

4. **FOR JOURNALS** : José R. Dorronsoro, Vicente López, Carlos Santa Cruz, and Juan A. Sigüenza, “*Autoassociative Neural Networks and Noise Filtering”* IEEE transactions on signal processing, 51(5) , 2003

5. **FOR JOURNALS***: S. Palanivel, B.S. Venkatesh and B. Yegnanarayana,* **R**eal time face recognition system using autoassociative Neural Network models, ICASSP 2003.

6. **FOR JOURNALS:** S. Amari “*Neural Theory of association and concept formation*” Biological cybernetics, 26, 175-185,1977.

7. **FOR CONFERENCES** : Csurka, G., Dance, c., Bray, c., and Fan, L., "*Visual categorization with bags of key points,*" In Proceedings Workshop on Statistical Learning in Computer Vision, I -22, 2004.

8. **FOR BOOKS**: Simon Haykin, "*Neural Networks A Comprehensive Foundation*", Pearson Educartion (Singapore) Pvt. Ltd. pp. 1-49 (2004).

9. **FOR BOOKS** : S.N. Sivanandam, S. Sumathi, S.N. Deepa, "*Introduction to Neural Networks using Matlab 6.0*", Tata McGraw-Hill pp. 10-29, pp 109-165(2006).

A Novel Mathematical Based Method for Generating Virtual Samples from a Frontal 2D Face Image for Single Training Sample Face Recognition

Reza Ebrahimpour ebrahimpour@ipm.ir
Assistant Professor, Department of
Electrical Engineering
Shahid Rajaee Univercity
Tehran, P. O. Box 16785-136, Iran

Masoom Nazari innocent1364@gmail.com
Department of Electrical Engineering
Shahid Rajaee Univercity
Tehran, P. O. Box 16785-136, Iran

Mehdi Azizi azizi_php@gmail.com
Department of Electrical Engineering
Shahid Rajaee Univercity
Tehran, P. O. Box 16785-136, Iran

Mahdieh Rezvan mhrezvan@gmail.com
Islamic Azad University south Tehran Branch
Tehran, P. O. Box, 515794453, Iran

Abstract

This paper deals with one sample face recognition which is a new challenging problem in pattern recognition. In the proposed method, the frontal 2D face image of each person is divided to some sub-regions. After computing the 3D shape of each sub-region, a fusion scheme is applied on them to create the total 3D shape of whole face image. Then, 2D face image is draped over the corresponding 3D shape to construct 3D face image. Finally by rotating the 3D face image, virtual samples with different views are generated. Experimental results on ORL dataset using nearest neighbor as classifier reveal an improvement about 5% in recognition rate for one sample per person by enlarging training set using generated virtual samples. Compared with other related works, the proposed method has the following advantages: 1) only one single frontal face is required for face recognition and the outputs are virtual images with variant views for each individual 2) it requires only 3 key points of face (eyes and nose) 3) 3D shape estimation for generating virtual samples is fully automatic and faster than other 3D reconstruction approaches 4) it is fully mathematical with no training phase and the estimated 3D model is unique for each individual.

Keywords: Face Recognition, Nearest Neighbor, Virtual images, 3D face modelModel, 3D shape.

1. INTRODUCTION

Face Recognition is an effective pathway between human and computer, which has a lot of applications in information security, human identification, security validation, law enforcement, smart cards, access control etc. For this reasons, industrial and academic computer vision and pattern recognition researchers have a significant attention to this task.

Almost the face recognition systems are related to the set of the stored images of a person, which called training data. Efficiency of these types of systems considerably falls when the size of training data sample is small (Small Sample Size Problem). For example in ID card verification and mug-shot we have only one sample per person. Several methods have done with the mentioned problem which we will introduce some of them that our idea is given from.

From the primary and most famous appearance based methods we can mention to PCA [1]. Then for one training sample per person, J. Wu et al. introduced $(PC)^2A$ [2] method. In this method, at first a pre-process on image is done to compute a projection matrix of face image and combine it with the original image, then PCA have being applied on projection combined image. Then, S.C. Chen et al. offered E(PC)^{2}A [3] method which was the enhanced version of (PC)^{2}A. To increase the efficiency of system they could increase the set of training samples by calculating the projection matrix in different orders and combining it with the original image. In [4] J. Yang offered 2DPCA method for feature extraction. 2DPCA is a 2D extension of PCA and has less computational load compared to PCA with higher efficiency compared to PCA for few training samples.

From another point of view, one can generate virtual samples to enlarge the training set and improve its representative ability, variant analysis-by-synthesis methods are put forward, i.e., the labeled training samples are warped to cover different poses or re-lighted to simulate different illuminations [5-8]. Photometric stereo technologies such as illumination cones and quotation image are used to recover the illumination or relight the sample face images. From this point of view, Shape from shading algorithms [9-11] has been explored to extract 3D geometry information of a face and to generate virtual samples by rotating the result 3D face models.

In our proposed method, we divided the frontal face to some sub-regions. After estimating the 3D shape of each sub-region, we combined them to create 3D shape of whole face. Then, we add the 2D face image with its 3D shape to construct 3D face models. Finally, different virtual samples with different views can be obtained by rotating the 3D face model in different angels.

Compared to previous works [8], this framework has following advantages: 1) only one single frontal face is required for face recognition and the outputs are virtual images with variant views for the individual of the input image, which avoids the burdensome enrollment work; 2) this framework needs only 3 key point of face (eyes and nose) 3) the proposed 3D shape estimation for generating virtual samples is fully automatic and faster than other 3D reconstruction approaches 4) this method has no training phase and is fully mathematical and also the estimated 3D model is unique for each individual .

Experimental results on ORL dataset also prove the efficiency of our proposed method than traditional methods in which only the original sample of each individual uses as training sample.

2. OVERVIEW OF THE PROPOSED SCHEME

Aiming to solve the problem of recognizing a face image with single training sample, an integrated scheme is designed which is composed of two parts: database image synthesis part and face image recognition part. Before recognition, synthesis work would be done on frontal pose of face image. Through the synthesis part, the training database will be enlarged by adding virtual images with other different views. In the recognition stage, One Nearest Neighbor is used to classify the test images. Therefore, the most important part in the proposed scheme is the synthesis one which has crucial affect on the recognition accuracy.

2.1 Face image synthesis

This section gives a summary of the synthesis proposed in our scheme and introduces briefly the key techniques utilized for generating virtual views.

As we know the general shape of human face is almost uniform. It means that the main regions of face such as eyes, nose and mouth nearly have the uniform shape for all human. For example if we consider a typical 3D face image of human in frontal, the region around the eyes has some notch and also the region around the nose has some nub which begin from the center of the brow and its nub increases approximately linearly till tip of the nose. In the proposed method we divided the frontal face image to some sub-regions. After estimating the 3D shape of each sub-region, we combine them to create 3D shape of whole face.

To obtain the 3D shape of the face, we require a distance matrix which can be easily computed from the distance between two lenses in 3D cameras. But in 2D images we need to estimate the distance matrix. Consider the 2D image of face in 3D space as shown in Figure 1.

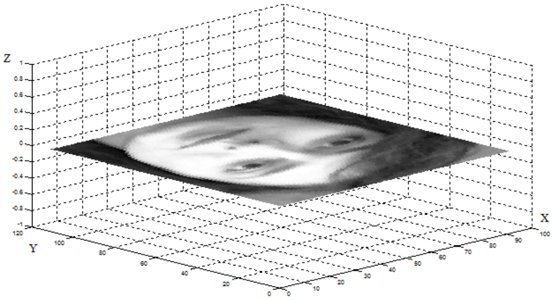


FIGURE 1: A 2D image of face in 3D dimension

Each pixel of this image represents one point in Cartesian X-Y coordinate system and Z can be regarded as distance axis of the image. In our proposed method we aim to estimate the Z matrix of face image to create virtual face images with different views that illustrated in detail as following:

It is worth noting that all of the equations used in our proposed method are obtained heuristically by some manipulation of different values and functions.

1- Consider an $m \times n$ face image. We locate three key points on face image (eyes and nose) automatically using the following method.

Note that to find the location of eyes and nose we need to crop the region of face. To accomplish our method for generating virtual sample, because it is the first step of the proposed scheme and affects the next steps dramatically, the region of face should be cropped with 100% accuracy,. There is no automatic algorithm with the accuracy of 100% until now (although some algorithms [12] with high accuracy need a manually located point of face such as nose location). Thus we crop all of ORL dataset manually as you see in Figure 2.

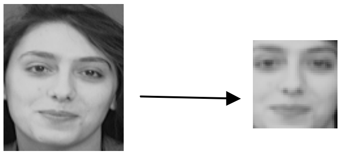


FIGURE 2: a sample of manually cropped face image

This method finds the region of eyes and nose as following:

a) Illumination Adjusting the face image and converting into a binary face image (see Figure 3)

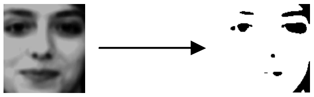


FIGURE 3: converting illumination adjusted face image into binary image

b) Dividing the binary image into three regions to locate the position of left eye, right eye, nose and lips (Figure 4).

To accomplish this task, we have used an eye detector, based on histogram analysis. In order to eye, nose and lip localization, the following steps are performed: 1. Compute the vertical and horizontal projections on the face pixels 2. Locating the top, down, right and left region boundaries where the projecting value exceeds a certain threshold.

We assume that eyes should be located in the upper half of face skin region. Once the face area is found, it may be assumed that the possible eye region is the upper portion of the face region. By analyzing the curve, we find the maximum and minimal point of the projection curve. Figure 4 shows the corresponding relation between these points and the position of facial organ: eyes, nostril, and mouth. Only the positions of eyes and lips are calculated in this case.

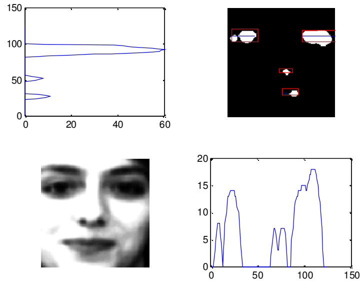


FIGURE 4: Eye, nose and lip localization using vertical and horizontal projections on the face pixels. The red rectangles indicate the boundaries of eyes, nose and lips and blue lines indicate the central lines of them.

Let the center of left and right eye and the tip of nose e_r, e_l and p_n respectively.

2- By using the position of eyes, we can compute the distance between eyes and also the middle point of the distance as shown in equation (1).

$$\begin{aligned} c_x &= \frac{(e_l(x)+e_r(x))}{2}, \quad x \in [1,n] \\ c_y &= \frac{e_l(y)+e_r(y)}{2}, \quad y \in [1,m] \\ \sigma &= \sqrt{(e_r(x)-e_l(x))^2+(e_r(y)-e_l(y))^2} \end{aligned} \tag{1}$$

Where σ is the distance and c is its middle point between left eye and right eye.

3-Through the equation (2), we make the face border (including the ears and head border) more sunken.

$$z_{gf}(x)|_{y\in[1,m]} = \frac{2000}{(50\sigma+(x-c_x)/\sigma)} \tag{2}$$

4-We know that the brow region is nearly slick and plane from the side-view and after the eyebrows there is the pone of eyes. By using eye situation, we find the part of the matrix Z which represents brow region and call it Z_{fh}. Thus we can have a good estimate of brow region according to equation (3).

$$z_{fh}(y)|_{x\in[1,n]} = \frac{1}{1+e^{(y-c_y-(\sigma/(.2\sigma)))/5}} \tag{3}$$

5- In the previous stage, the points under brow sunk whereas the cheek must be salient. To fix this notch and signalize the cheek region, we can use equations (4).

$$\begin{aligned} z_{c1}(y)|_{x\in[1,n]} &= \frac{1}{1+e^{(y-c_y-(\sigma/(.08\sigma)))/5}} \\ z_{c2}(y)|_{x\in[1,n]} &= \frac{1}{1+e^{(y-c_y-(\sigma/(.12\sigma)))/5}} \\ Z_{cheek} &= z_{c1}(x,y).z_{c2}(x,y) \end{aligned} \tag{4}$$

6- If we pay attention to the downward regions of face, we would find out that in most faces the notch of borders increases nearly exponentially with respect to the center of face. According to equation (5), we estimate the matrix that does this task.

$$z_{df}(x)|_{y\in[1,m]} = e^{-(x-c_x)^2/\sigma^2} \tag{5}$$

7- In this stage we obtain an estimate for the distance matrix of the nose. By little attention to the general form of human face we find out that the bridge begins from the middle point between of eyes and its nub almost increase linearly with the slight slope till nose tip and then decrease nearly with sharp slope while both side of nose sink exponentially as shown in equation (6).

$$Z_{nose}(x,y)=\begin{cases}(y-cy).(e^{\frac{-(x-cx)^2}{0.05\sigma^2}}) & , \quad cy<y<pn \\ 0 & , \quad others\end{cases} \tag{6}$$

8-In the preceding stages, we estimated some different sub-matrixes for the distance matrix (Z) that each of them can estimate one part of the face excellently and in the other regions cause increase in error. Thus, the only important point is how to combine these matrixes. Since in each sub-region of the face corresponding matrix must be used, we used equation (7) to combine estimated local matrixes in order to obtain the total estimate matrix for 3D shape of face image.

$$Z(x,y)=Z_{gf}(x,y).((1-Z_{df}(x,y)).(1-Z_{fh}(x,y)).(1-Z_{cheek}(x,y)))+Z_{nose}(x,y) \tag{7}$$

Figure 5 schematically represents our proposed method for estimating 3D shape of face.

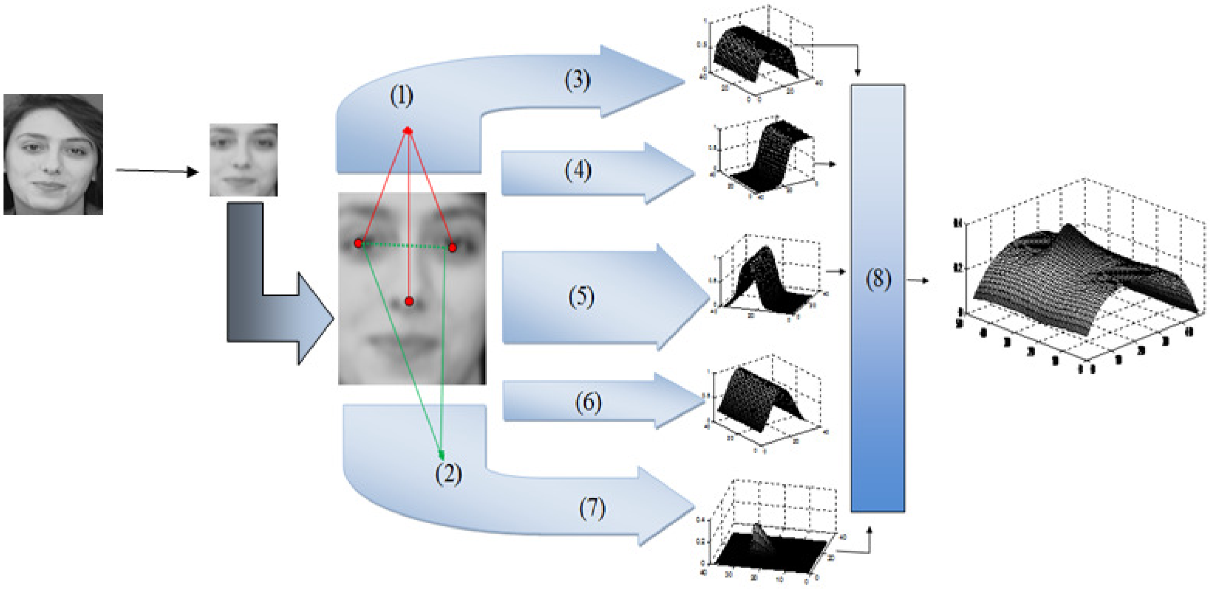


FIGURE 5: Our proposed method for estimating 3D shape of face

9-Now, since we have the distance matrix Z, we can drape the 2D face image over its 3D shape and create 3D face model as shown in Figure 6.

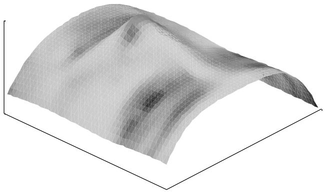


FIGURE 6: 3D face model after draping 2D face image over its 3D shape

10- Finally, we rotate the 3D face model in different views and produce virtual images in some different angles to obtain virtual images with different poses. Figure 7 shows some of virtually generated 3D faces with the proposed method on ORL dataset.

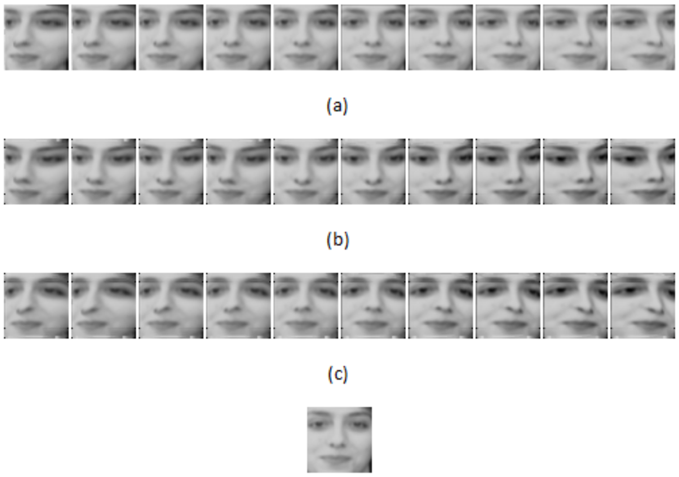


FIGURE 7: Virtual images with different views generated from only a frontal 2D face image (**a:** tilt up (6^0) and angle (-25^0 :$+25^0$) **b:** normal and angle (-25^0 :$+25^0$) **c:** tilt down (6^0) and angle (-25^0 :$+25^0$) **d:** original image)

3. EXPERIMENTAL RESULTS

In the proposed method we only used frontal face image and generated 18 virtual images with different views vary from -20^0 to $+20^0$. We systematically evaluated the performance of our algorithm compared with the conventional algorithm that do not uses the virtual faces synthesized from the personalized 3D face models.

To test the performance of our proposed method, some experiments are performed on ORL face database which contains images from 40 individuals, each providing 10 different images. For some subjects, the images were taken at different times. The facial expressions and facial details (glasses or no glasses) also vary. The images were taken with a tolerance for some tilting and rotation of the face of up to 20 degrees (-20^0 to $+20^0$) and also some variation in the scale of up to about 10 percent. All images are grayscales and cropped to a resolution of 48×48 pixels. Figure 8 shows some example of ORL dataset.

FIGURE 8: Some samples of ORL database

In all the experiments, the conventional methods used only the frontal faces of each person for training and the other faces are all used for testing. The comparison experiments have been conducted to evaluate the effectiveness of the virtual faces created from the 3D face model for face recognition. We used PCA and 2DPCA for dimension reduction as well as extracting useful features and nearest neighbor for classifying the test images.
Table 1 and 2 compare the results of our proposed method and conventional method.

Table 1 Recognition rate comparison between face recognition with/without virtual face using PCA

Dimension ***Method***	***5***	***20***	***40***	***70***	***100***
Without virtual views (%)	53.5	70.61	**72.58**	**72.58**	**72.58**
With virtual views (%)	70.12	73.22	**78.50**	78.40	78.30

Table 2 Recognition rate comparison between face recognition with/without virtual face using 2DPCA

Dimension ***Method***	***(48×1)***	***(48×2)***	***(48×5)***	***(48×8)***	***(48×10)***
Without virtual views (%)	64.89	73.50	**77.44**	75.22	74.44
With virtual views (%)	71.37	79.10	**82.10**	81.20	80.83

By enlarging training data using our proposed method achieve higher top recognition rate (about 5%) than traditional methods in which only one frontal face image is used as training sample.

4. CONCLUSION AND FUTURE WORK

In this paper, we proposed a simple but effective model to make applicable face recognition task in situations where only one training sample per person is available.

In the proposed method, we select a frontal 2D face image of each person and divide it to some sub-regions. After computing the 3D shape of each sub-region, we combine the 3D shape of ach sub-regions to create the total 3D shape for whole 2D face image. Then, 2D face image is draped over the corresponding 3D shape to construct 3D face model. Finally by rotating the 3D face image in different angels, different virtual views are generated and added to training sample. Experimental results on ORL face dataset using nearest neighbor as classifier reveal an improvement of 5% in correct recognition rate using virtual samples compared to the time we use only frontal face image of each person.

Compared with other related works, the propose method has the following advantages: 1) only one single frontal face is required for face recognition and the outputs are virtual images with variant views for the individual of the input image, which avoids the burdensome enrollment work; 2) this framework needs only 3 key points of face (eyes and nose) 3) the proposed 3D shape estimation for generating virtual samples is fully automatic and faster than other 3D reconstruction approaches 4) this method has no training phase and is fully mathematical and also the estimated 3D model is unique for each individual .

Our experiments also show the top recognition rate of 82.50% which still is far from satisfactory compared to average recognition accuracy that may be realized by human beings. It is expected that other techniques are needed to further improve the performance of face recognition. A possible way to achieve the mentioned goal is generating more virtual views with different expression and illumination using more complex techniques, another possible way could be explored on classifiers with more complexity and higher accuracy.

5. REFERENCES

[1] M. Turk and A. Pentland, “Eigenfaces for Recognition,” J. Cognitive Neuroscience, vol. 3, no. 1, pp. 71-86, 1991.

[2] J. Wu, Z.H. Zhou, “Face recognition with one training image per person,” Pattern Recognition Letters, vol. 23, no. 14, pp. 1711–1719, 2002.

[3] S.C. Chen, D.Q. Zhang, Z.H. Zhou, “Enhanced (PC)2A for face recognition with one training image per person,” Pattern Recognition Letters, vol. 25, no. 10, pp. 1173–1181, 2004.

[4] J. Yang, D. Zhang, “Two-Dimensional PCA: A New Approach to Appearance-Based Face Representation and Recognition,” IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 26, no. 1, pp. 1173–1181, 2004.

[5] T. Riklin-Raviv, A. ShaShua, “The quotient image: class based re-rendering and recognition with varying illuminations,” Pattern Anal. Mach. Intell, vol. 23, no. 23, pp. 129–139, 2001.

[6] A.S. Georghiades, P.N. Belhumeur, D.J. Kriegman, “From few to many: illumination cone models for face recognition under variable lighting and pose,” IEEE Trans. Pattern Anal. Mach. Intell, pp. 643–660, 2001

[7] Talukder, D. Casasent, “Pose-invariant recognition of faces at unknown aspect views,” IJCNN Washington, DC, 1999.

[8] T. Vetter, T. Poggio, “Linear object classes and image synthesis from a single example image,” IEEE Trans. Pattern Anal. Mach.Intell, vol. 19, no. 7, pp. 733–741, 1997.

[9] R. Zhang, P. Tai, J. Cryer, M. Sha,”Shape from shading: a survey,” IEEE Trans. Pattern Anal. Mach. Intell, vol. 21, no. 8, pp. 690–706, 1999.

[10] J. Atick, P. Griffin, N. Redlich, “Statistical approach to shape from shading: reconstruction of three dimensional face surfaces from single two dimensional image,” Neural Comput, vol. 8, pp. 1321–1340, 1996.

[11] T. Sim, T. Kanade, “Combining models and exemplars for face recognition: an illuminating example,” Proceedings of the CVPR 2001 Workshop on Models versus Exemplars in Computer Vision, 2001.

[12] T. Jilin, F. Yun, and S. Huang, “Locating Nose-Tips and Estimating Head Poses in Images by Tensorposes,” IEEE Trans. Circuit and Systems for Video Technology, vol. 19, no. 1, 2009

Authentication and Authorization Models

Prof. More V.N. vickymore12@gmail.com
Faculty, Bharati Vidyapeeth University, Pune (India)
Abhijit Kadam Institute of Management & Social Sciences, Solapur

ABSTRACT

In computer science distributed systems could be more secured with a distributed trust model based on either PKI or Kerberos. However, it becomes difficult to establish trust relationship across heterogeneous domains due to different actual trust mechanism and security policy as well as the intrinsic flaw of each trust model. Since Internet has been used commonly in information systems technologies, many applications need some security capabilities to protect against threats to the communication of information. Two critical procedures of these capabilities are authentication and authorization. This report presents a strong authentication and authorization model using three standard frameworks. They are PKI, PMI, and Directory. The trust in this approach is enabled by the use of public key infrastructure (PKI) which is applied for client two-factor authentication and secures the infrastructure. We introduce the preventive activity-based authorization policy for dynamic user privilege controls. It helps prevent successive unauthorized requests in a formal manner. At the core, we apply An Improved Trust Model to facilitate the authentication with the different keys with work flow of model efficiently. Also describes the X.509 standard to define the directory schemas of PKI and PMI to find the object classes and optional attributes.

Keywords: PKI, PMI, Kerberos, An Improved Trust Model, X.509 standard.

1. INTRODUCTION

PKI and Kerberos are two protocols, into which most of the researches in the field of a distributed system are made, and they have got the most widely application. In a PKI protocol, the information security of that system is assured through the adoption of public key technology and digital certificate. The purpose of the digital certificate is to verify the identity of the certificate holder.

Kerberos, based on symmetrical key algorithm, enables the establishment of mutual trust between the two communication sides through session key and ticket authorization. Both protocols, to a certain degree, have been put into application with relatively good results. Net technology are continuously advancing, especially a huge number of large-scale distributed information systems are setting up, which may adopt different authentication technology and its corresponding trust model, as a result, though its own system security is safeguarded, numerous authentication barriers and “information isolate islands” in a network will be also created.

PKI provides a framework to verify the identities of each entities of given domain. The framework includes the requesting, issuing, signing, and validating of the public-key certificates.

PMI provides a framework to determine whether or not they are authorized to access a specific resource. The framework includes the issuance and validation of attribute certificates. Public -key certificates are certificates for trusting public-key and attribute certificates are certificates for trusting privilege attribute.

Directory plays a significant role as an interconnection standard for PKI and PMI. This report describes the form of authentication and authorization information held by the Directory, and how such information may be obtained from Directory.

2. PKI (PUBLIC KEY INFRASTRUCTURE)

A public-key certificate has a special data structure and digitally signed by an authority called certificate Authority (CA). A public-key certificate binds a public key to a subject which holds the corresponding Private-key so that other entities could trust subject’s public-key. Public-key certificate can be used during some period of time specified in a certificate’s ‘validity’ filed. But, for some reasons, the certificate can be revoked by the CA before

the certificate expires. If an authority revokes a public -key certificate, users need to be able to know that revocation has occurred so they no longer use the revoked certificate.
A system using a public-key certificate needs to validate a certificate prior to using that certificate for an application. Since certificates are public information, certificates can be published and placed in public places Directory), with out special efforts to protect them.

2.1 Generation of Key Pairs

A user's key pair can be generated in three different ways according to the standards.

a) By the user
b) By a third party
c) By the CA

The advantage of method 'a' is that a user's private key is never released to another entity. But, the user needs a communication with the CA so that he can transfer the public key and distinguished name in a secure manner. In case of 'b' and 'c', the user's private key also needs to be transferred to the user in a secure manner.

2.2 Creation of Public-Key Certificate

A CA issues a public-key certificate by associating the user's public key and unique distinguished name of the user. It is important that CA should be satisfied of the identity of a user before creating a certificate, and should not issue certificates for two users with the same name. A public-key certificate contains following information and is digitally signed by issuer to provide the integrity.

- Version: the version number of certificate.
- Serial number: an integer uniquely assigned by the CA to each certificate.
- **Signature**: algorithm identifier for the algorithm and hash function used by the CA in signing the certificate.
- **Issuer:** the entity that has signed and issued the certificate.
- **Validity**: the time interval during which the CA warrants that it will maintain information about the status of the certificate.
- **Subject**: the entity associated with public-key found in the subject public key field.
- **Subject public key info**: the public key being certified and the algorithm which this public key is an instance of.
- **Issuer unique identifier**: used to uniquely identify an issuer in case of name re-use.
- **Subject unique identifier**: used to uniquely identify a subject in case of name re-use.
- **Extensions**: allows addition of new fields to the structure.

2.3 Certificate Validation

Certificates may be revoked by CA prior to their expiration time. Authorities are required to state the way for relying parties to obtain revocation information about certificates issued by that authority. The Certification Revocation List (CRL) is a commonly used mechanism for relying parties to obtain this information. The CRL is a periodically published data structure that contains a list of revoked certificate serial numbers. The CRL is time-stamped and digitally signed by the issuer of the certificates.

Generally a CRL is published within an X.500 directory which also stores the certificates for the particular CA domain. Delta-CRL is a partial CRL which is a list of only newly revoked certificates. Delta-CRL is useful when entire revocation list become large and unwieldy. An Authority Revocation List (ARL) is a CRL that is used exclusively to publish revocation information for CAs. It therefore does not contain any revocation information pertaining to end -user certificates.

2.4 Certification Path

According to the PKI standards, there are two primary types of public -key certificates, user certificates and CA-certificates. A user certificate is a certificate issued by a CA to a subject that is not an issuer of other public-key certificates. A CA-certificate is a certificate issued by a CA to a subject that is also a CA. If a Certification Authority is the subject of a certificate issued by another Certification Authority, the certificate is called a cross-certificate. A list of cross-certificates needed to allow a particular user to obtain the public key of another, is known as a certification path.

A certification path logically forms an unbroken chain of trusted points between two users wishing to authenticate.

3. PKI AND ITS TRUST MODELS

PKI (Public Key Infrastructure) is the most widely used security authentication technology, mainly including encryption, digital signature and digital certificate. In a PKI system, CA (Certificate Authority) is the authentication centre of a domain and represents a third institution of credible authority. All communication and authentication between the clients rely on the certificates issued by CA. The trust models of PKI include the strict hierarchy trust model, reticulated trust model and the composite trust model.

3.1 Strict Hierarchy Trust Model

Strict hierarchy trust model is a centralized mode. This model has a tree-shaped structure with the root as the root CA. The branch nodes are the sub-CAs and the leaves represent the clients. All the nodes (sub-CAs and clients) trust root CA and reserve a copy of root CA's certificate with its public key. Before user A communicates with B, they must verify each other's certification through the root CA. Only their certificates have both been verified by root CA, shall the communication between the users established. All the one-way trust relationship must be established through the central authentication server (root CA). Therefore, the structure of this model can be easily extended by adding a sub-CA or more. In this model, the verification path of the certification is correspondingly short. The longest one will be Nlevel + 1; the Nlevel stands for the number of the layers.

Root CA is the unique trust-point. If the root CA is rendered into unreliable, the trust relationship of the whole PKI system will be destroyed right away. It is almost impossible to recover the whole trust relationship. In practical network environment, it is hard to establish an exactly dependable trust-point. It is not even an easy thing to integrate established CAs due to different security policies. Any adjust to the trust relationship would be extremely difficult once a system is established.

3.2 Reticulate Trust Model

The Reticulate trust model includes several CAs to provide PKI service. Each terminal trusts a Certain CA which issues him the certificate. The CAs trusts each other by issuing certificates to each other peer-to-peer. Each user trusts others by means of this kind of certificate. CAs issues the cross authentication certificate with each other, which contains the public key of the issuing CA. In this way, trust relationship will be established and extended. This model can easily add new group of users, because of multiple reliable CAs.

Security weakness of a single CA or a number of CAs will not affect the overall operations of the whole system, because the trust can be reestablished through other paths. It is also easier to renew the trust relationship after malfunction or accidents, only a few CAs or users will be affected. It is a complex and difficult thing to construct a certificate verification path, because there may be many possibilities. The user may try many times to find the proper one. With the increase of CAs, cross trust authentication would become more complex and a heavier burden would be imposed on the management and maintenance of the system. This model is not appropriate to the organizations with strict affiliation, such as the government and the military. Hierarchic relationship of the real entities could not be reflected by this model.

3.3 Composite Trust Model

This kind of trust model is based on the cross authentication, like the reticulate trust model, but is different. There is a bridge CA which is responsible for establishing the cross-authentication for heterogeneous trust-domain. Other CAs from different domains can authenticate each other through the bridge CA. This bridge CA is a medi-point of trust transfer as well as an influx-point. Any structured PKI application or system can be connected with one another without having to modify its own structure so that the trust relationship could be established and extended through the whole system.

The Bridge CA plays a role as a third part sponsor for establishing the trust relationship between different domains. The independent and surveillant status of the Bridge CA is suitable to maintain reliability and seriousness of the model. This model has a wheel-shaped and radiating structure as well as multiple trust chains of many other trust models. The Bridge CA does not manage the end-users, so the change of the user number does not affect it. Using this model, the number of the times of certificate authenticating will be the same as the number of CAs, which could make the management less costly and much easier. When the Bridge CA is disabled, every CA connected with the bridge only needs to release the certificate signed to the Bridge CA. They can still work separately before the Bridge CA returns to work.

4. KERBEROS

Kerberos is a network authentication protocol. It was designed to provide strong authentication based on the reliable third-party authentication system for the project Athena. Now, it is available in many commercial products. Kerberos builds a safe bridge between client and server by providing central authentication service and symmetrical key system. In other words, an appointed server works for the user only when the central authentication server validates the service request and access right sued by the user. The most important part of Kerberos is the key distribution centre, which called KDC for short. It provides two services, one is AS (Authentication service), and the other is TGS (Ticket granting service). The operation flowchart of the protocol is demonstrated in Fig.1.

Kerberos protocol is now widely used in the distributed network applications. Independent development platform, high speed communication of authentication, mutual authentication between entities and transferable relation-ship of trust, and a relatively strong compatibility with heterogeneous domains which may adopt various trust polices, are all the predominance of the Kerberos. However, many security flaws appear during its usage in that the protocol heavily relied on certain aspects when it was designed and the limitation is quite striking. From the point of view of the network attack, some serious problems demanding more attention are as followed:

4.1 Password Guessing Attack

Kerberos is not effective against password guessing attacks; if a user chooses a poor password, then an attacker guessing that password can impersonate the user. Similarly, Kerberos requires a trusted path through which passwords are entered. If the user enters a password to a program that has already been modified by an attacker (e.g. a Trojan horse), or if the path between the user and the initial authentication program can be monitored, then an attacker may obtain sufficient information to impersonate the user.

4.2 The Security of the Application System

At the present time, the worst network attack comes from vicious software. Kerberos authentication protocol depends on the absolute reliability of the software based on the protocol. An attacker may design software to replace the primary Kerberos application, which can execute the Kerberos protocol and record the username and password. Generally speaking, the cipher application which has been installed on unsafe computers will more or less face the problem. Also, Kerberos must be integrated with other parts of the system. It does not protect all messages sent between two computers, and it only protects the messages from software that has been written or modified to use it. While it may be used to exchange encryption keys when establishing link encryption and network level security services, this would require changes to the network software of the hosts involved.

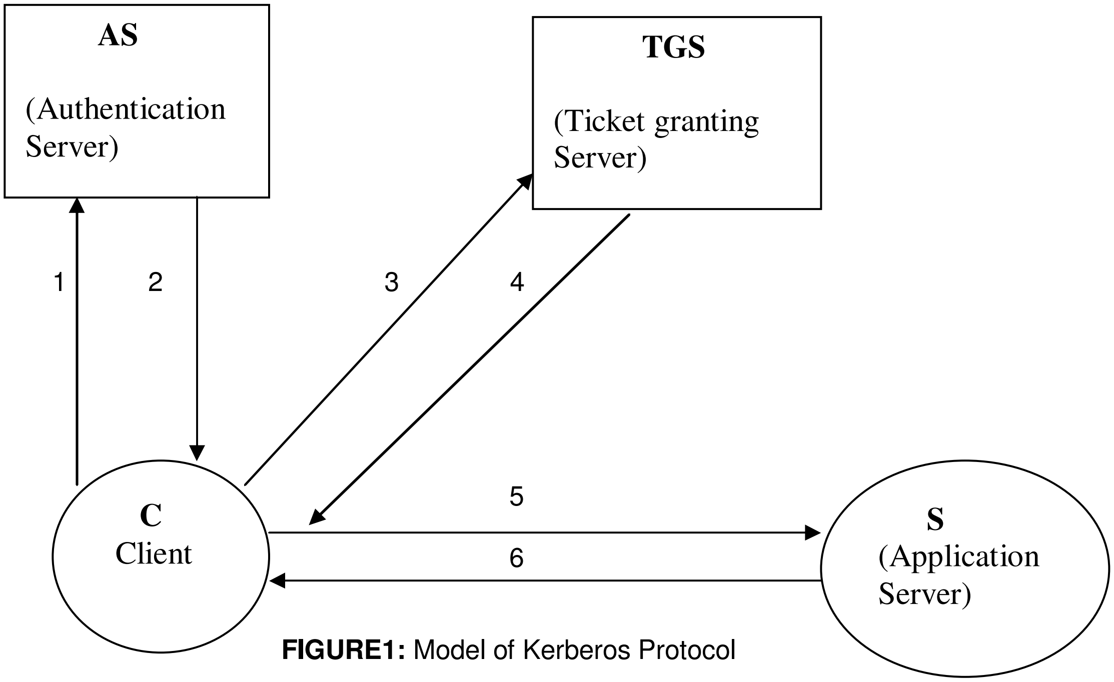


FIGURE1: Model of Kerberos Protocol

4.3 The Problem of Timestamp

Kerberos uses timestamp in order to prevent playback attack. But during the lifetime of the ticket, playback attack may still take effect. For example, in a certain Kerberos trust domain, all the clocks of the equipments keep synchronous. The period of validity for the message is 5 minutes, if the message arrives during the period, it is regarded as fresh.

In fact, the attacker can easily fabricate a message according to the protocol format beforehand. Once he intercepts and captures the ticket from the user to server, the attacker could send the fake message within 5 minutes; server can not easily find what exactly happened.

4.4 Secure Storage for Session Key

In Kerberos system, each user shares a session key with the server. KDC of the Kerberos system must provide a service to store a huge number of session keys. It is arduous to manage or update the keys and information related. Special measures must be taken to protect the KDC.

Naturally, the KDC becomes the targets of the attackers. Especially for the government or the military, it will be a disaster if the KDC has been destroyed which will result in failed communication among users of the domain. It is also quite demanding to store the system. So Kerberos, the authentication and authorization protocol based on symmetric key algorithm, is fitter with the environment which does not own a large number of registered users, but demands high efficiency.

5. AN IMPROVED TRUST MODEL

It is a model for authentication and authorization between trust domains. It is based on PKI and Kerberos.

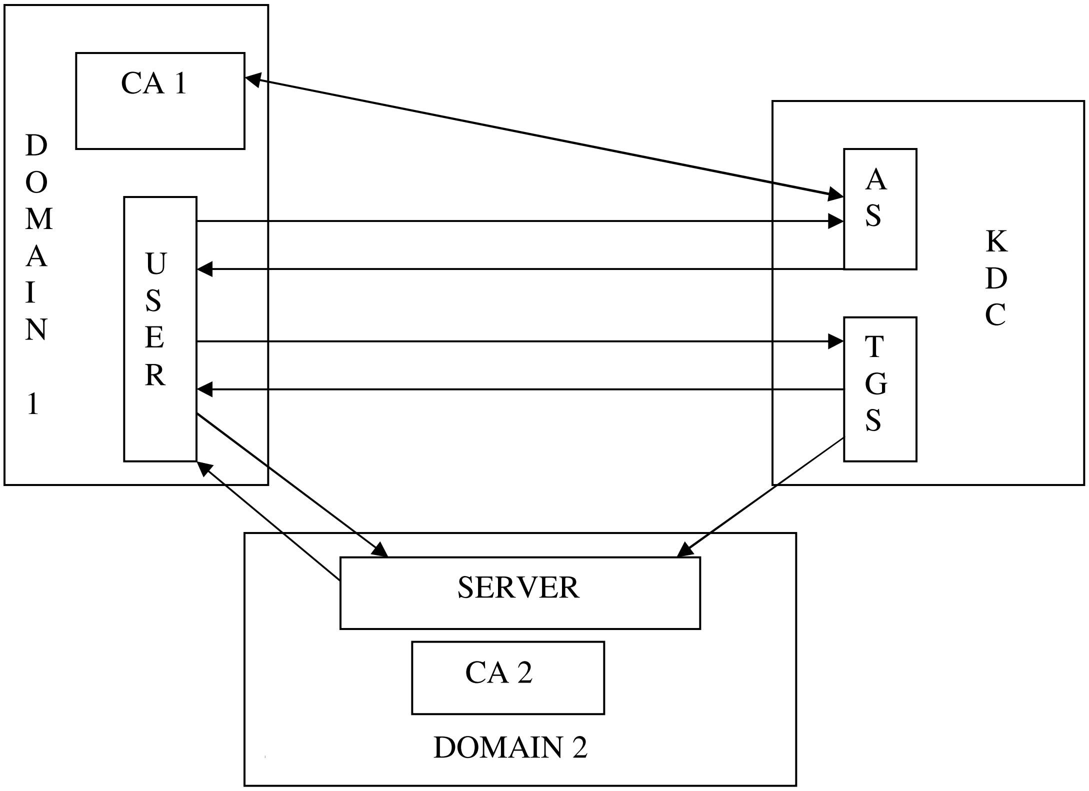


FIGURE2: New model based on PKI and Kerberos

5.1 Model Work Flow

5.1.1 U → AS: PKAS (CertU, U, TGS)

U→S: First, user sends a request to the AS (Authentication server) for establishing session with TGS. The message is encrypted with PKAS (public key of AS) by the user. The message also contains the user's digital certificate CertU, which is issued by CA1.

5.1.2 AS→U: PKU (KU, TGS, KAS, TGS (TU, TGS), PKTGS)

AS→U: When AS decrypt the request, he gets the CertU and verifies the user's identity. If AS can make sure the request sender is unquestionable the one asserted, AS generates the session key KU, TGS which will be used for the communication of the user and TGS. The response to the user from AS will be encrypted by PKU (user's public key). The response contains the session key KU, TGS, the ticket ZU, TGS which will be encrypted by KAS, TGS shared only by AS and TGS.

5.1.3 U→TGS: PKTGS (KU, TGS, S, KA, TGS (TU, TGS))

U→TGS: User uses his private key SKU to decrypt the response, and then he will get a session key KU, TGS and a cipher text TU, TGS. Second, user sends a request to the TGS in order to get the permission for visiting the server S. The request contains the name of the server, the session key KU, TGS shared between the user and the TGS, and the ticket TU, TGS which encrypted with KA, TGS by AS. User can not modify the ticket in private.

5.1.4 TGS→U : KU, TGS (TU, S, KU, S)

TGS→U: When the request arrives, TGS uses his private key SKTGS to decrypt the request and get the session key KU, TGS and the cipher text of ticket TU, TGS. Then, TGS decrypts the cipher text and gets the ticket. If the ticket is authentic, TGS issues the ticket TU, S and the session key KU, S which is shared by the user and the server.

5.1.5 TGS→S: SKTGS (U, H (TU, S), SHA1, KU, S)

TGS→S: While TGS sends the session key to the user, TGS also sends the server a message of notification which contains the name of the user, a message digest of the ticket TU,S , the hash algorithm and the session key KU, S .

5.1.6 U→S: KU, S (TU, S, U, CertU, R1):

U→S: The user access the resource server as soon as he gets the ticket. Before establishing the secure communication between them, user has to send a message encrypted with KU, S. The message contains the ticket TU, S, the user's name U, user's certificate CertU and a random number R1.

5.1.7 S→U : KU, S (R1,"OK"):

S→U: When the server has verified the identity of the user, he sends a response back. From now on, the trust relationship has been established.

5.2 Model Analyses:

- Trust relationship between heterogeneous domains can be established by adopting this model, featuring strong expandability and capability of mutual communication. The demand of interlinking different domains without any modification to the security policy or the architecture of the domain could be met.

- The model uses Kerberos protocol for the authentication between domains, greatly cutting down time waste and resource waste on building and verifying the certificate path, which is a disadvantage of the old PKI model.

- The trust between domains is built on the validity of the ticket, which is issued by the KDC of the Kerberos system. The format and content of the ticket is much more fixed than the certificate based on X.509. In this way, valid certificate regarded as invalid due to its different format will be avoided during the process of authentication.

- The Kerberos system would only store the session keys with which to communicate with CAs of different domains, rather than generate or maintain a large number of session keys for the users.
- The Kerberos server is only responsible for setting up cross-domain communication and granting tickets, while any addition or reduction to the number of the users or authentication registration falls to the CA's Obligation. Users in different domains follow the different security policies based on PKI. Each domain' CA takes the responsibility of user management, such as user's registration, increasing or decreasing a member. This model not only lightens the burden of the system, but will not affect or depend on the domains' architecture which might be different because of various working styles. When the KDC is under attack or fails to work properly, it will not cause trouble to the inter-domain management and communication.

- How the KDC distributes or isochronously updates the session keys to the CAs is not included, as proper answers could be found in the field of security requirement of the actual system.

6. PMI (Privilege Management Infrastructure)

The binding of a privilege to an entity is provided by an authority through a digitally signed data Structure called an attribute certificate. In general case, entity privileges have lifetimes that do not match the validity period for a public -key certificate.

The use of attribute certificates, issued by an Attribute Authorities (AA) provides a flexible Privilege Management Infrastructure (PMI) which can be established and managed independently from a PKI. At the same time, there is a relationship between the two infrastructures. Since PMI doesn't provide the mechanism to trust certificate holder's identity, PKI is used to authenticate identities of issuers and holders in attribute certificates.

6.1 Attribute Certificates

The public-key certificate proves the identity of the entities. However, they do not specify what the entities can do. Attribute certificates were developed to provide this access control. An attribute certificate has the similar data structure as a public-key certificate. But an attribute certificate does not contain the subject's public key. Instead, it contain s the attributes (privileges) of the holder.

6.2 Attribute Authority, SOA

The Attribute Authority (AA) and Certification Authority (CA) are completely independent. The creation and maintenance of 'identity' can be separated from the PMI. The Source of Authority (SOA) – analogous to a 'root CA' in the PKI – is the entity that is trusted by a privilege verifier as the entity with ultimate responsibility for assignment of a set a privileges. An SOA is itself an AA as it issues certificates to other entities in which privileges are assigned to those entities.

PMI framework support privilege delegation as an optional feature. SOA assigns privilege to an entity that is permitted to also act as an AA and further delegate the privilege. Delegation may continue through several intermediaries AA's until it is ultimately assigned to an end -entity that cannot further delegate that privilege. The attribute certificate extension provide one mechanism that can be used by an SOA to make privilege attribute definitions and associated domination rules available to privilege verifiers.
An attribute certificate that contains this extension is called an attribute descriptor certificate and is a special type of attribute certificate.

7. DIRECTORY SCHEMA OF PKI AND PMI

X.509 standard defines the directory schema of PKI and PMI.

Directory schema:

A directory schema specifies the types of objects that a directory may have and the mandatory and optional attributes of each object type. The schema is made up of two things: object classes, and attributes. Following definitions of object classes and attributes are cited from Netscape Directory Administration Guide.

Object Classes

Object classes define the types of attributes an entry can contain. Most object classes define a set of required and optional attributes. This attribute list represents the kind of data that you both must and may store on the entry.

7.1 PKI directory schema

X.509 standard defines PKI directory schema as follows:

Object classes	Attributes
Certificate Authority	CA certificates, cross-certificates CRLs, ARLs
Certificate User	Public-key certificate
CRL distribution point	CRLs, ARLs, delta -CRLs
CP & CPS	CPs, CPSs
Certification Path	Certification path(Sequence of cross-certificates)

TABLE 1: PKI directory schema

7.2 PMI directory schema

X.509 standard defines PMI directory schema as follows:

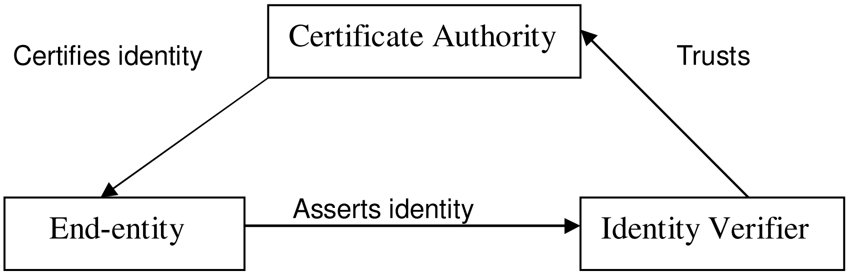
Object classes	Attributes
Source of Authority (SOA)	ACRLs, AARLs, attribute descriptor certificate
Attribute Authority (AA)	AA certificate, ACRLs, AARLs
Certificate Holder	attribute certificate
CRL distribution point	ACRLs, AARLs, delta-ACRLs
Privilege Policy	Privilege policies
Delegation Path	Delegation path(Sequence of attribute certificates)

TABLE 2: PMI directory schema

8. AUTHENTICATION AND AUTHORIZATION MODEL IN PKI and PMI

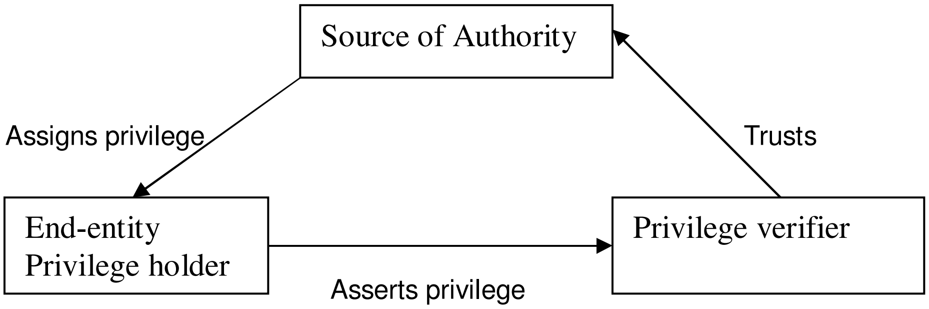
8.1 Authentication Model

The authentication model consists of three entities: the Certificate Authority, the End-entity, and the identity verifier. The identity verifier is the entity that makes the determination as to whether or not asserted identity is correct. The Certificate Authority certifies the end -entities by issuing public-key certificates for them. The identity verifier trusts the CA as the authority for a given certification for the identity. If an end entity's certificate is not issued by that CA, then the identity verifier must locate a certification path of certificates from that of the entity to one issued by the CA.



8.2 Authorization Model

X.509 attribute certificate framework defines authorization models in PMI environment as follows. The basic privilege management model consists of three entities: the SOA, the privilege holder and the privilege verifier. The privilege holder is the entity that holds a particular privilege and asserts its privileges for a particular cont ext of use. The privilege verifier is the entity that makes the determination as to whether or not asserted privileges are sufficient for the given context of use.



8.3 A Comparison of PKI with PMI

Sr. No.	Concept	PKI Entity	PMI Entity
1.	Certificate	Public Key Certificate	Attribute Certificate
2.	Certificate issuer	Certification Authority	Attribute Authority
3.	Certificate user	Subject	Holder
4.	Certificate binding	Subject’s name to public key	Holder’s name to privilege attribute(s)
5.	Revocation	Certificate revocation list (CRL)	Attribute certificate revocation list (ACRL)
6.	Root of trust	Root certification authority	Source of authority
7.	Subordinate authority	Subordinate certification authority	Attribute authority

TBALE 3: Comparison of PKI with PMI

9. OUTPUT OF THE RESEARCH WORK

9.1 PKI: A PKI is not an authentication method; rather it is an infrastructure that uses digital certificates as an authentication mechanism and is built to better manage certificates and their associated keys. A digital certificate is itself a way to reliably identify the user or computer claiming to be the owner of a specific public key.

If we find the use of PKI as authentication we are comes to know that certificate authority checks the user. Different CA's have different identity validation procedures. Some may grant the user a digital certificate with only a name and email address, while others may involve personal interviews, background checks etc. (Remembering that authentication is a process of validating an identity based on risk means that certificate authorities' digital certificate has a wide range of trust…caveat emptor). The user is granted a digital certificate. Often there are two components to this; private and public keys.

The user wishes to send an email to a business associate. The user digitally signs the email with their private key. The email is sent to the business associate. The business associate uses the sending user's public key to decrypt the message. The use of digital certificates in this example provides confidentiality, message integrity and user authentication without having to exchange secrets in advance. PKI was oversold on its capabilities when it was originally introduced several years ago. There were serious problems with browser incompatibilities, costs associated with issuing and managing digital certificates and a business environment that had not yet widely adopted the internet to rethink business processes between enterprises.

9.1.1 What is the PKI Made Of?

A PKI can be implemented within an organization, for the use of the users on its network, or it can be a commercial entity that issues certificates to Internet users, for example. Either way, the PKI consists of the following components:

- At least one certification authority (CA) to issue certificates.
- Policies that govern the operation of the PKI.
- The digital certificates them selves.
- Applications that are written to use the PKI.

9.1.2 Applications of PKI

Applications must be PKI-aware in order to work with the certificates and use them for authentication purposes. Web browsers, email clients and many applications that are built into the Windows 2000/XP operating systems such as EFS and IPSec are PKI-aware, as are the operating systems themselves.

9.2 Kerberos: Kerberos is a solution to your network security problems. It provides the tools of authentication and strong cryptography over the network to help you secure your information systems across your entire enterprise. We hope you find Kerberos as useful as it has been to us.

9.2.1. Benefits of Kerberos

A properly deployed Kerberos Infrastructure will help you address these problems. It will make your enterprise more secure. Use of Kerberos will prevent plaintext passwords from being transmitted over the network. The Kerberos system will also centralize your username and password information which will make it easier to maintain and manage this data. Finally, Kerberos will also prevent you from having to store password information locally on a machine, whether it is a workstation or server, thereby reducing the likelihood that a single machine compromise will result in additional compromises. To summarize, in a large enterprise, the benefits of Kerberos will translate into reduced administration costs through easier account and password management and through improved network security. In a smaller environment, scalable authentication infrastructure and improved network security are the clear benefits.

9.3 An Improved Trust Model:

An Improved Trust Model was introduced which is a model for authentication and authorization between trust domains. It is based on PKI and Kerberos. How the data should encrypt and decrypt by using user’s private, public and session keys through model work flow.

9.4 PMI: PMI is depends on the attribute certificates issued by an Attribute Authorities, PMI doesn’t provide the mechanism to trust certificate holder’s identity while PKI is used to authenticate identities of issuers and holders in attribute certificates.

9.4.1 Significance and use of PMI

Supporting distributed heterogeneous application architecture with a homogeneous distributed security infrastructure leveraged across the enterprise; providing user and service identities and propagation; and providing a common, consistent security authorization and access control infrastructure. It used in the existing standards like ANSI X9.45, ISO 9594-8, IETFRFC 3280 X.509, OASIS SPML, SAML, WS-*, and XACML etc..

9.5 X.509 Standard: X.509 standard defines the directory schema of PKI and PMI where directory schema is describes the types of objects in the directory and its optional attributes.

9.5.1 Applications with X.509 standard

Probably the most widely visible application of X.509 certificates today is in web browsers (such as Netscape Navigator and Microsoft Internet Explorer) that support the SSL protocol. SSL (Secure Socket Layer) is a security protocol that provides privacy and authentication for your network traffic. These browsers can only use this protocol with web servers that support SSL.

9.5.2 Other technologies that rely on X.509 certificates include

- Various code-signing schemes, such as signed Java Archives, and Microsoft Authenticode.
- Various secure E-Mail standards, such as PEM and S/MIME.
- E-Commerce protocols, such as SET.

10. APPLICATION WITH AUTHENTICATION AND AUTHORIZATION MODELS

In case of finding use of authentication and authorization model with system application I am giving example of tool provided by the Microsoft called as SharePoint on the role based membership to access only restricted data. Microsoft SharePoint Foundation supports security for user access at the Web site, list, list or library folder, and item levels. Security management is role-based at all levels, providing coherent security management across the SharePoint Foundation platform with a consistent role-based user interface and object model for assigning permissions on objects. As a result, list-level, folder-level, or item-level security implements the same user model as Web site–level security, making it easier to manage user rights and group rights throughout a Web site. SharePoint Foundation also supports unique permissions on the folders and items contained within lists and document libraries. Authorization refers to the process by which SharePoint Foundation provides security for Web sites, lists, folders, or items by determining which users can perform specific actions on a given object. The authorization process assumes that the user has already been authenticated, which refers to the process by which SharePoint Foundation identifies the current user. SharePoint Foundation does not implement its own system for authentication or identity management, but instead relies solely on external systems, whether Windows authentication or non-Windows authentication.

SharePoint Foundation supports the following types of authentication:

- Windows: All Microsoft Internet Information Services (IIS) and Windows authentication integration options, including Basic, Digest, Certificates, Windows NT LAN Manager (NTLM), and Kerberos. Windows authentication allows IIS to perform the authentication for SharePoint Foundation

Finally, we found that the authentication model consists of three major entities like Certificates Attributes, End-entity, and the identity verifier and authorization model consists of three major entities like SOA, the privilege holder and the privilege verifier. A PMI is to authorization what a PKI is to authentication

CONCLUSION

In this paper, two representative protocols of authentication and authorization are analyzed and compared with. Then a new high-compatible trust model is proposed. This model helps to realize the aim of interlinking heterogeneous domains supported by different authentication technique and security policy. However a security policy or trust model, no matter how ideal it is theoretically, could not speak well for its feasibility. To imperfect this model, future studies will be focused into strengthening the ticket validity and enhancing mutual authentication efficiency according to the characteristics of the distributed network environment. The protocols are described in this paper are basically used on the basis of Certificate Authority to checks the users for security purpose and to introduce that on which major entities the authentication and authorization models are depends. I conclude that data from users are encrypt and decrypt by using the key through these protocols helps for the security of the distributed systems.

REFERENCES

[1] Thompson MR, Olson D, Cowles R, Mullen S, Helm M. CA-Based trust model for grid authentication and identity delegation. In: Proc. of the GGF7. 2003.

[2] Neuman C. RFC 1510, The Kerberos Network Authentication Service (V5) [S]. 1993.

[3] Bellovin S M, Merritt M. Limitation of the Kerberos authentication system [A].Proceedings of the Winter 1991 Usenix Conference [C]. 1991.

[4] Guan Zhen-sheng, Publication Key Infrastructure PKI and the applications. Beijing: Publishing House of Electronics Industry. 2008.1

[5] Wen Tei-hua, Gu Shi-wen, An improved method of enhancing Kerberos protocol security, Journal of China Institute of Communications, Vol 25 No 6. June 2004, pp. 76-79.

[6] Burr W E. Public Key Infrastructure (PKI) Technical Specifications: Part A-Technical Concept of Operations: [WORKING Draft] TWG-98- 59. Federal PKI Technical Working Group. Sep. 1998

[7] [X.509] CCITT Recommendation X.509, The Directory: Authentication Framework, 1997

[8] Internet X.509 Public Key Infrastructure Certificate and CRL Profile
URL: http://search.ietf.org/internet -drafts/draft-ietf-pkix-new-part1-09.txt

[9] An Internet Attribute Certificate Profile for Authorization
URL: http://search.ietf.org/internet -drafts/draft-ietf-pkix-ac509prof-09.txt

[10] X.509 4th edition: Overview of PKI & PMI Frameworks (Entrust, Inc.)
URL: http://www.entrust.com/resources/pdf/509_overview.pdf

[11] Certificate Revocation in Public Key Infrastructures
URL: http://www.sans.org/infosecFAQ/encryption/cert_ rev.htm

[12] Tips for LDAP users
URL: http://www.ymtech.co.kr/ref/java/jnditutorial -may1/ldap/index.html

[13] Netscape Directory Server Administration Guide
URL: http://home.netscape.com/eng/server/directory/3.0/ag/contents.html

[14] S. Chokhani (CygnaCom) & W. Ford (VeriSign, Inc.) Internet X.509 Public Key Infrastructure
Certificate Policy and Certification Practices Framework
URL: http://www.i etf.org/rfc/rfc2527.txt

[15] Kerberos and Authentication
URL: http://web.mit.edu/kerberos/#what_is

[16] Authentication, Authorization and Accounting
URL: www.infosectoday.com/Articles/Authentication.html

[17] Strong authentication and authorization models
URL: www.sans.org/.../strong-authentication-authorization-model-pki-pmi- directory_747

[18] Role of PKI
URL: www.windowsecurity.com/.../Understanding_the_Role_of_the_PKI.html

[19] An X.509 Role-based Privilege Management Infrastructure
URL: www.permis.org/files/article1_chadwick.pdf

[20] ASTM E2595 - 07 Standard Guide for Privilege Management Infrastructure.
URL: http://www.astm.org/Standards/E2595.htm

[21] Recommendation X.509 and ISO 9594-8, Information Processing System – Open Systems Interconnection - The Directory - Authentication Framework, 1988.
URL: http://csrc.nist.gov/nissc/1996/papers/NISSC96/paper075/paper.pdf.

Security Model for Hierarchical Clustered Wireless Sensor Networks

Kalpana Sharma kalpanaiitkgp@yahoo.com
Department of CSE, SMIT,
Sikkim, India

M.K. Ghose mkghose2000@gmail.com
Department of CSE, SMIT,
Sikkim, India

Abstract

The proposed security system for the Wireless Sensor Network (WSN) is based on the WSN security design goal that 'to design a completely secure WSN, security must be integrated into every node of the system'. This paper discusses on two main components of the security framework viz. the secure key management module and the secure routing scheme. The incorporation of security mechanism during the routing protocol design phase is the main focus of this paper. The proposed security framework viz. 'Secure and Hierarchical, a Routing Protocol' (SHARP) is designed for the wireless sensor network applications which is deployed particularly for data collection purpose in a battlefield where the security aspect of the network cannot be compromised at any cost. SHARP consists of three basic integrated modules and each module performs a well defined task to make the whole security framework a complete system on its own.

Keywords: WSN, Security, Hierarchical Clustering, Cluster Heads, Routing, Key Management

1. INTRODUCTION

Wireless Sensor Networks (WSN) are a class of mobile ad-hoc network(MANET) which consists of a hundreds/ thousands of sensor nodes deployed in the area of interest to accomplish a particular mission like habitat monitoring, agricultural farming , battlefield surveillances etc. The sensor nodes are resource constraint devices in the sense that they've limited memory, computational capacity, limited transmission range and operate on a battery thus having limited energy also. Despite these inherent limitations these tiny nodes are used in a variety of applications as they have the ability to sense the environment, process the captured data, aggregate the data and send it wirelessly to the destination which is a powerful entity called the Base Station (BS). Complex cryptographic solutions which are meant for traditional networks cannot be used in the WSN because such algorithms demand a huge computation capability, a large storage space, large bandwidth and unlimited energy supply which a tiny node cannot provide. So instead of concentrating on such complex security algorithms, a lightweight security solutions sound more realistic for the resource starved sensor nodes. Further a security solution concentrating in only one layer, for example physical layer or link layer or network layer, proves to be insufficient for the WSN because such security solution doesn't provide sufficient security to all the layers. So a more practical security solution for WSN would be the development of a security framework consisting of many security service components to provide multi-level security services [6, 8]. Such a framework should interact with all the modules of various protocol layers to provide robust security to the WSN. As per Boyle et al. 'to achieve a completely secure WSN, security must be implemented into every node of the system' [1]. This paper attempts to integrate services provided to the link layer and the network layer to come up with an integrated security solution. The integrated framework of this paper consists of three basic modules forming the core of the proposed security platform. Nevertheless these modules can be used as stand alone modules as well.

There are basically three types of communication in a WSN environment. Theses are one to one communication, many to one and one to many. To secure these communications, the key management module establishes various kinds of keys. To secure the whole WSN, all communication types needs to be secured. Secure keying techniques presented in this paper provides a combination of different kind of keys for secure communication .The secure routing scheme presented in this paper ensures that the messages, using these keys,are securely routed by the nodes and the Cluster Heads (CH) to their final destination i.e. the BS.

The topology that has been considered in this paper is a hierarchical clustering approach. Using this topology the coupling of the security mechanisms like the key usage as well as the routing has been proposed. The proposed security framework is composed of three different modules. These modules are 1) Hierarchical Cluster formation module in which the issues like the formation of tracks, sectors, cluster heads, and neighbor selection are addressed. 2) Key Management module which is responsible for the distribution and maintenance of the keys used in the network. 3) Secure Routing module is responsible for the communication between the BS and other nodes of the network.

The rest of the paper is organized as follows. Section 2 deals with the overview on the related work followed by section 3 which deals with the details pertaining to the module which is responsible for cluster formation. Key management techniques of the proposed framework is presented in section 4 followed by section 5 in which proposed ‘Routing Scheme’ is discussed. Finally in section 6l results and discussions are presented followed by conclusions in section 7.

2. RELATED Work

The various efforts to design optimal security architectures for the WSNs that have been specified/implemented to-date have been described in [1]. The authors have reported that the symmetric key cryptography based architectures have been the main source of security in the WSN to date. Key management is an important activity for ensuring sensor data integrity and securing the WSN communications through cryptographic technique. Design efforts to achieve optimal security architectures of key management for the WSNs are discussed in [1].Key management techniques that have been reported so far can be categorized as follows [24, 25]:

a. Random key Pre-distribution scheme: An example of Random-key pre-distribution schemes is Peer Intermediaries for Key Establishment (PIKE) [26]. PIKE uses probabilistic techniques to establish pair wise keys between neighboring nodes in the network. However, in this approach, each node has to store a large number of keys.

b. Master-key-based scheme: In this scheme, the nodes share unique symmetric keys with the Base station. These keys are assigned before the network is deployed. This involves a significant pre-deployment overhead which is not scalable. Examples of this scheme are Security Protocols for Sensor Networks (SPINS) [2] and Localized Encryption and Authentication Protocol (LEAP) [3], which is discussed in detail in subsequent sections.

c. BS based scheme: Hierarchical Key Establishment Scheme (HIKES) proposed by Ibriq et al. [27] is an example of BS based scheme. In this scheme, the Base station, acts as the central trust authority and empowers randomly selected sensors to act as local trust authorities. These nodes authenticate the cluster members and issue all secret keys on behalf of the Base station. HIKES uses a partial key scheme that enables any sensor node selected as a CH to generate all the cryptographic keys needed to authenticate other sensors within its cluster. The main drawback of this scheme is the storage overhead of the partial key table in every node.

Undercoffer et al. [28] have proposed a security model considering the BS as a trustworthy authority of the entire framework of the sensor network. In this protocol the BS disallows a sensor node from participating in the network, if it detects a node behaving anomalously or becomes compromised. The main drawback of this scheme is the usage of shared keys among the nodes as Zhu et al. [10] have pointed out that a single keying scheme is not sufficient to secure the entire WSN.

Four different keying mechanisms have been provided in Localized Encryption and Authentication Protocol (LEAP) [3], keeping in mind the need for different security requirements for different types of messages. These include the Individual Keys, Group Keys, Cluster Keys and Pairwise Shared Keys. The usage of four different keys supports in-network processing and at the same time restricts the security impact of a node- compromise to only the group members of that node. LEAP + [4] is an improved version of LEAP. Unlike LEAP, a new node sends a message to establish both the pairwise key and the cluster key in LEAP +.

The concept of ‘Secure Triple-Key Management Scheme’ is proposed in [6]. The main drawback of the scheme is that it supports the pre-development key management scheme. TinySec [14] assumes to have a global common secret key among the nodes that is assigned prior to the deployment of the network in order to provide encryption and authentication in the link layer. A standard 8 byte key length is specified for use in the protocol [4], thus making it possible to address smaller sized messages. In [7] the authors have described a scheme for pre-key distribution based on the prior deployment knowledge of the sensor nodes. New schemes for key management for confidential communication between node and its cluster head in hierarchical sensor networks is discussed in [5] wherein the performance analysis was done which shows that Tree- Based Scheme exhibits better performance with some additional storage. SHARP is motivated by the security framework presented by Zia and A.Y. Zomaya, in their research paper “A Secure Triple-Key Management Scheme for wireless sensor networks” [6]. In their paper the authors have used the concept of secure triple-key management scheme. In [8] the authors have presented a security framework discussing the cluster formation and leader election process, secure key management scheme, secure routing and their algorithms, which is the main motivation of this research work presented in this paper. TinySec [14] has been the de facto security solution at Berkeley. The performance of the proposed framework SHARP has been compared with TinySec and is discussed in section 6. Raman et. al. in their paper [16] has bought out that WSN protocols are very deeply dependent on application scenarios, but most of protocols does not use any specific application in its design to achieve this interaction. In [17] the authors have in general described the relationship between the development of various security algorithms and the resources constraint nature of the sensor nodes. A Path Redundancy Based Security Algorithm for Wireless Sensor Networks is discussed in [18] but this security solution is also not integrated security solution and concentrates only in one aspect of security service for the WSN. In [19] Khalil et al. have described an interactive solution only for the resource allocation for the WSN but is not intended for security solution .So it is to be noted that very less research work is being reported in the integration of the security solution.

3. CLUSTER FORMATION MODULE

The main aim of hierarchical routing is to efficiently maintain the energy consumption of sensor nodes by involving them in multi-hop communication within a particular cluster and by performing data aggregation and fusion in order to decrease the number of transmitted messages to the sink. Cluster formation is typically based on the energy reserve of sensors and sensor’s proximity to the cluster head [20]. The hierarchical clustering technique proposed is described in this section.

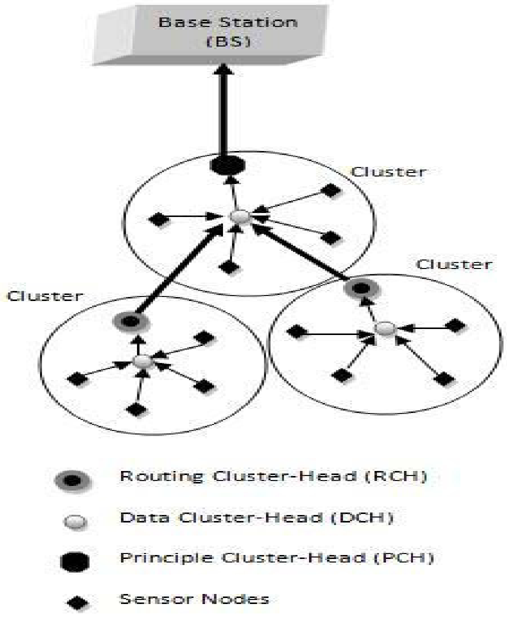


FIGURE1: DCH/RCH of a cluster

Division of the whole network is done in terms of track and sector in order to provide energy efficient and storage efficient key establishment. A detail pertaining to track- sector is available in [9]. The Base station (BS) would divide the network into tracks and sectors. Tracks are required in order to reduce the communication with the BS as most of the nodes belonging to track 1 would serve as “Routing CH” (RCH). In this context the BS would be assumed to be in track 0. Tracks are further divided into sectors. The nodes belonging to the same sector communicate with each other as buddy and in order to be buddy ,each node after getting its sector information and track information from the BS, starts “Neighbor finding phase’ or ‘buddy discovery phase’. Once the neighbors are identified each node stores their neighbor information in ‘buddy info table’. This work is an extension of [11] in which a naïve idea about the selection of the Data Cluster Head (DCH) and Routing Cluster Head (RCH) as well as ‘ Neighbor finding” algorithms are already presented. The reason for dividing the Cluster Heads (CHs) into RCH and DCH is as follows: Rather than a single CH performing both data aggregation and data transmission to the BS this load is divided among two sensor nodes which act as the DCH and RCH in a sector. The BS selects two sensor nodes in each sector as the DCH and the RCH as shown in figure 1. The node preferably in the centre of each sector is selected as the DCH and the node with the minimum distance to the BS in that sector is selected as the RCH. Figure 1 has been reproduced from [13].

DCH is responsible for data aggregation and sending the aggregated data to the RCH. RCH in turn transmits these data packets to the BS if it is in track1 or else it sends to the nearest DCH/RCH belonging to a track of higher level in the track-sector hierarchy. When the number of the nodes in a particular sector is less, then a single CH would act as both RCH/DCH in order to conserve energy.

Division of the network into track-sector and selection of RCH/DCH is the responsibility of the BS. The following assumptions are made in the context of the role of BS in the proposed security framework.

1) Location of each node is known to the BS.
2) Time Division multiplexing (TDM) is used for communication in a group.
3) The BS is very powerful with a huge computational capability.

4) Before any transmission takes place, all the nodes have to register themselves with BS.
5) The BS does the clustering on the basis of the location of the nodes thus dividing the whole network into say 'n' tracks and 'm' sectors where n>>m. The base station also selects cluster head for each sector.
6) The responsibility of the Cluster Head is as follows:
   i) Data aggregation
   ii) Encoding of the message sent by the nodes belonging to its track/sector.
   iii) Communication with the base station.
   iv) The "key table" maintenance.
7) The role of CH is rotational as CH has additional duties in comparison with other nodes. This is done in order to conserve energy or to increase the longitivity of the network.

4. KEY MANAGEMENT MODULE

It is a proven fact that a single keying technique is not appropriate to secure all the communication types of the WSN [10]. So a good keying mechanism should consist of a combination of variety of keying techniques like 'in-network generated keys', 'pre-deployed keys' and 'broadcast keys' [5]. The key management module of this work does not rely on a single key type but makes use of all the above mentioned keys.

4.1. Types of Keys of the Proposed Secure Keying Scheme

Once the 'neighbor discovery 'phase is over and all the nodes have updated their respective 'buddy info table', the BS initiates the key distribution process. In general pair-wise key distribution scheme is set up between the neighbors [12].

In the key management module of this paper there are three broad categories of key 1. Pre-deployed keys 2) In network generated keys and 3) BS broadcasted keys. Before introducing the keys used in this paper, the type of communication of WSN are to be noted. These are as follows:

1. Type 1 communication :Node to Node communication i.e. N:N
2. Type 2 communication :Node to Cluster Head Communication i.e. N : CH
3. Type 3 communication :Cluster Head to BS Communication CH:BS
4. Type 4 communication :Node to BS i.e. N: BS
5. Type 5 communication :BS to Nodes i.e. BS:N
6. Type 6 communication :DCH to RCH Communication i.e. D:R

The following keys are used in the proposed protocol;

1) Buddy key (K_b) is calculated by all the nodes once the neighbor finding work is over. It is used to communicate by each node within its own sector/cluster i.e. for N: N communication.
2) My-Own-Key (K_o) is used by each and every node initially. All the nodes are preloaded with its id and this key is a function of node id, sector-id, track-id, and its residual energy. Ko is used for N: BS communication.
3) Network key (K_n) is issued by the BS after authentication to all the nodes. If a node joins the network it has to send a request to BS for acquiring network key. This request is sent by all the nodes to the BS encrypting it by K_o. BS sends the 'K_n' to the requesting nodes encrypting it with 'K_o' of that particular node. Only the node which is authentic can decrypt this 'K_n'. K_n is used for BS: N as well as for N: CH communication.
4) Cluster Key (K_c) is calculated by CHs for D:R communication.
5) Broadcast Key (K_{bro}) is issued by the BS after authentication as CHs. K_{bro} is used for CH: BS communication.

Node to node communication is nothing but the intra cluster communication which is done using buddy- Key. For simplicity all the keys used in this proposed security framework is listed in the table 1 given below.

Type of key	Composition	Origin	User/communication type
My-Own-Key (K_o)	f(node-id, sector-id, remaining energy level)	Node id preloaded, Nodes calculate it and BS knows it all	All the nodes of the Network i.e. N: BS and BS: N communication.
Buddy-Key (K_b)	*Idsender + f(Idreceiver ,track-id)	All the nodes belonging to the same sector calculate it. Here sectorid (i)=sectorid(j)	All the neighboring nodes belonging to the same sector. For N: N Communications
Network key (K_n)	Calculated by BS	BS to all the nodes	All the nodes.
Broadcast key (K_{bro})	BS Generated	Distributed by BS to RCH & DCH	RCH to BS.
Cluster key (K_c)	f(node id, sector-id, track-id)	Calculated by DCH & RCH.	DCH and RCH.

TABLE 1: Keys usage in various WSN Communication types

* + indicates concatenation operation

4.2 Achieving Security Through the Usage of the Keys

Four rules have been devised for the usage of the keys and Routing.

1. Key distribution: Not all the keys are distributed by the BS. Keys like K_b, K_c and K_o are calculated by each node in the network.
2. Key usage : The key usage rules are discussed in section 4.2.1
3. Key refreshment
   - Broadcast key (K_{bro}) as well as Network key (K_n) are refreshed by the BS at regular interval of time. This refreshment ensures that the nodes belonging to the network is well authenticated from time to time.
4. Key Maintenance: Each node in the network maintains the databases of the following
   - Its own key (K_o).
   - Network key (K_n).
   - Buddy key (K_b).
   - Broadcast key (K_{bro}) and Cluster Key (K_c) (In case of the nodes playing the role of DCH or RCH).

4.2.1 Key Usage

It is essential for all the nodes to know/ calculate their own key K_o. Also all the nodes should possess K_n to take part in the communication as K_n is used for encrypting/ decrypting all the messages broadcasted by the BS from time to time.

Let the initial message to be sent to the DCH by the ordinary node be IM. This first message format would look like this:

$$\boxed{\text{Message(M) = \{ } K_b\text{, TS,MAC, IM\}}}$$

Here TS is the timestamp used to avoid replaying of the messages, MAC is used for authenticating the message. This first message is encrypted using K_b because RCH/DCH is nothing but a buddy to the node in the same sector.

DCH and RCH communicate with each other using cluster key. DCH and RCH compute their cluster-key which is simply a function of their own id, sector-id and track-id. Here sector id may be dropped but for generalization sector id is also considered though all the DCH and RCH should belong to the same sector. But to address the situations where RCH may not be directly communicating with the BS in hierarchical clustering nature of the network, a DCH may have to communicate with DCH or RCH of the cluster above it. So sector id is retained. DCH, RCH communication is encrypted using cluster key. Since DCH is responsible for data aggregation

DCH would send the aggregated message to RCH encrypting it using the K_c and the message format looks like this:

DCH Message(DM) = { K_c,{ K_b, TS,MAC, aggregated (M)}}

Since the number nodes in a particular sector varies and if the number of nodes are less then RCH will function as both DCH and RCH to save energy.

Now for type 3 communication, apart from K_c, another key called K_{bro} is needed. To get hold of Kbro DCH/RCH sends the request message to BS encrypting it using its own-key. BS knows which node has dual function as RCH, RCH and which all have separate DCH, RCH. Accordingly it sends K_{bro} to the requesting CH encrypting them with my-own-key of the requesting nodes. So once DCH, RCH acquire the K_{bro}, communication to RCH to BS takes place encrypting the message by K_{bro} and the message format looks like this

RCH Message(RM) = { K_{bro},{ K_c,{ K_b, TS,MAC, (DM)}}}

The real challenge here is the maintenance of the buddy key. It is already stated that all the nodes set up their keys by communicating with their neighboring node. If a node has to communicate with a large number of neighbors then the WSN has to compromise on its space requirement vs security.

5. SECURE ROUTING MODULE

BS initiates the routing process once the hierarchical clustering topology is fixed and also key distribution is done. Each node is authenticated by their unique id BS has in depth knowledge about a) Id of each node b) Sector no of each node. c) Track no of each node d) Energy level of each node. The BS keeps track of this information in a table which is updated from time to time. When the sensor nodes send a request to BS to join the network encrypting this request with K_o, the BS will be able to decrypt the request message of only the genuine nodes of the network. Once a node is authenticated BS sends the requesting node the network key. When any CH node makes a request for K_{bro} the BS sends the authentic node the broadcast key. Message pertaining to k_{bro} is encrypted using my-own-id key of the requesting CH. If BS needs to broadcast any message to all the nodes then it encrypts the message using K_n. The 'data collection table' which is maintained by the BS is updated after processing the data and obtaining the original message sent by the nodes.

The algorithm for 'Secure Routing' is presented in 5.1.

5.1 Algorithm BS

Algorithm: Secure Routing

```
Begin
Step1.  if BS receives request for authentication from a node then
                goto step2
            else
                goto step1
            end if
Step2.   Check the authenticity of the node
        Step2.1.   Request node sends its request message to BS
                Step2.1.1. M'=E (M, $K_0$)
                Step2.1.2. SEND M'
        Step2.2.  BS decrypts the request message
                Step2.2.1. RECEIVE M'
                Step2.2.2. M = D (M', $K_0$)
Step3. Send network key after node is authenticated by BS
        Step3.1. M'=E ($K_n$, $K_0$)
        Step3.2. Decrypts message to obtain network key
```

```
    Step3.3. $Kn=D(M',K_0)$
Step4. if CH node makes a request then
        BS sends broadcast key
        $M'=E(K_{bro},K_0)$
    end if
Step5. if BS needs to broadcast message then
        $M' = E (M, K_n)$
    else
        listen
        goto step1
    end if
Step6. if decryption successful at node then
        goto step7
    else
        discard M'
        goto step10
    end if
Step7. Compute $M = D (M', K_n)$
Step8. Update 'data collection table'
Step9. goto step11
Step10. if data retransmission necessary then
        Broadcast message
    else
        goto step1
    end if
Step11. End
```

This algorithm is implemented in C++ and the results have been compared with that of TinySec [14] and Triple-Key security algorithm [6].

It is also to be noted that the encryption/ decryption technique used in this algorithm is RC5 block cipher. A detail on feasibility on the RC5 usage in the WSN is available in [21, 22].

6. RESULT ANALYSIS

To analytically evaluate the cost of the security of the proposed security platform computation overhead, communication overhead and storage overhead for packet processing is considered.

To extend the battery life of resource constraint sensor nodes it is necessary to limit the energy consumption. But to provide security to the WSN a price have to be paid in terms of significant amount of energy consumption for bare minimum and unavoidable requirement of security services like encryption, decryption, and key management. Key management also demands extra storage space to store the required keys for the secure communication. The performance comparison provided in this section presents the space and computation overhead.

The packet format for SHARP is shown below. The performance comparison is done with TinySec [14] and Triple Key [6, 8] the packet format. All the values are in bytes.

6.1 Packet Formats

Dest	AM	GRP	Length	Data	CRC
2	1	1	1	29	2

Tiny OS

Dest	track-id	keys	L	sector id	Src	TS	Data	MAC
1	1	5	1	1	1	1	29	4

Proposed packet format

Dest	AM	Length	Data	MAC
2	1	1	29	4

TinySec –Auth

Dest	AM	Length	Src	Ctr	Data	MAC
2	1	1	2	2	29	4

TinySec-AE

ID	Keys	TS	Data	MAC
5	4	1	29	4

Triple Key

For SHARP since all the keys are the function of node-id, sector-id, track-id, at most (5+1+1+1+1) bytes i.e. 9 bytes are required for key and ID storage. MAC is used for message authentication and integrity. All the values are in bytes. In SHARP the data packet is not more than 44 bytes long and these packets can be transmitted easily in sensor nodes available in the market today.

6.2 Performance Comparison –Computation Overhead

The comparison of packet size overhead for TinySec, TripleKey and SHARP is shown in Table 5.2. The values pertaining to TinySec is obtained from [14] whereas TripleKey values are obtained from [21].

	Application data (bytes)	**Packet Overhead**	**Total Size**	**Time to transmit (ms)**	**Increase over TinyOS Stack (%)**	**Latency overhead (%)**	**Energy overhead (%)**
TinySec-Auth	29	8	37	26.6	1.5	1.7	3
TinySec-AE	29	12	41	28.8	8	7.3	10
TripleKeys	29	11	40	28.3	6.3	5.9	2.8
SHARP	29	15	44	30.7	12.8	11.5	12.2

TABLE 2: Comparison of SHARP with TinySec & Triple-Keys

There is an increase in the packet size for the proposed security solution. It results in an increase in the usage of bandwidth and energy needed to send the packets, as evident from Figure 2 and Table 2. However, this framework provides multiple layers of security. It is also observed that there is an increase in time to transmit parameter. Accordingly, there is 9% increase over current TinyOS stack, which can be compensated by multiple-layer of security provided by SHARP.

The energy overhead of TinySec and Triple keys is comparatively lesser than that of SHARP. However, SHARP overcomes the shortcomings of all these protocol with acceptable energy overhead. The graphical representation based on the packet sizes are provided in Figure 2.

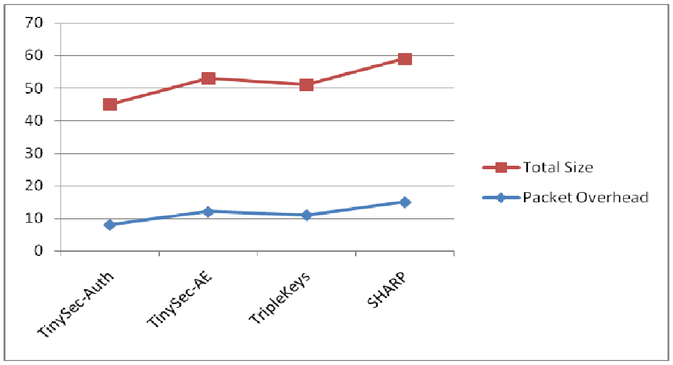


FIGURE 2: Packet size comparison.

6.2.1: Advantages of SHARP over TinySec:

TinySec is not a complete security framework. It is based on a number of assumptions as defined below:

- TinySec concentrates only on Link Layer Security.
- There is no particular keying mechanism specified for TinySec.

SHARP addresses both these shortcomings but it is at the cost of increased packet size. This increase in packet size is an acceptable to be used for the sensor nodes available in the market.

6.2.2: Advantages of ISF over TripleKeys

Triple-Keys have shown considerable savings in bandwidth and battery life, thus have energy advantage over both TinySec and SHARP. However, it has following deficiencies, which have been addressed in the proposed ISF scheme.

- To reduce the packet size, the AM field of the of the triple-key packet format is dropped. Hamed et al [26] have observed that the removal of AM type field introduces several major problems for upper layer services as it directly affects the Active Message Model of TinyOs.
- The id and key fields are combined. Moreover, the number of bytes reserved for the source / destination fields of the message are not mentioned.
- The scheme uses three keys, two of which are pre-deployed keys. These important pre-deployed keys when compromised, the whole network is compromised. ISF being a multilayered security scheme, the compromise of a key of a particular sector effect only that cluster but not the entire network.

6.3 Storage Overhead

As it is known that all the nodes in this WSN need to store keys for communication. A simple node stores at least three keys for encryption process throughout and the minimal keys being my-own-id key, network key and buddy key (which is with respect to its neighbors).Apart from this if the node is DCH / RCH it needs to store all the three above mentioned keys as well as cluster key and Broadcast key. It obviously increases the storage overhead. But not all the keys are pre-loaded. Two keys i.e. network key, and broadcast keys are always broadcasted by the BS and my-own-id keys are only pre-loaded. Yet the storage overhead is expressed as (for any node)

$$\boxed{\text{Storage overhead= [Size of}(K_o)+K_b\ (X\text{-}Y)+K_n]}$$

where X is the total number of the nodes in the WSN and Y is the subset of X which is nothing but the population of only those nodes which belong to the same sector i.e. selected neighbors of that particular node belonging to the same sector. The storage overhead for DCH/RCH would be

Storage overhead= [Size of(K_o)+K_b (X-Y)+K_n+ K_c+ K_{bro}]

Even if the default key size is considered to be 10 bytes each and the maximum number of neighbors is taken as 50, the storage overhead for an ordinary node would be 60 bytes and for a CH it would be at most 90 bytes which is less than 1 KB. This overhead is acceptable as almost all the sensor nodes available in the market including Berkeley's motes have a memory size of more than 4 KB.

Though there is an overhead in storage but on the flip side because of the hierarchical clustering techniques there're two CHs in a single cluster which results in a multi-hop communication which obviously results in energy efficiency in comparisons with those clustering techniques in which there is only one cluster head, as in [13]. The simulations results reported in [13] are comparable with that of LEACH [15] in certain cases.

To summarize the overall performance of SHARP it is to be noted that when the algorithm presented in section 5 is to be implemented in the same environment where TinySec is implemented and the same sized application data is considered then it can be predicted that there would be an increase in 'Time to transmit parameter. It is because of the increase in the packet size. Thus there would be at most 9% increase over current TinyOS stack. But this increase is compensated by 'multiple-layer' of security provided by SHARP.

Again it is to be noted that the security framework presented in [6] have single point of failure as there's only one cluster head. Moreover when the cluster keys are to be stored then it requires more storage space than SHARP as the clustering in this work is not only hierarchical but also energy efficient because of the division of the network into tracks and sector .As already stated the number of neighbors is restricted because of the division of the network into tracks and sectors. Tracking and sectoring not only restricts the no. of neighbors with whom key establishment needs to be done but also aids in energy conservation. Energy efficient key management technique is thus made possible by adapting the concept of sectoring and tracking which is a new concept in this proposed protocol. In case of a node compromise, the nodes belonging only to the' buddy set' are compromised but not the entire network. To manage the buddy set, computation is preferred over communication as communication is much more expensive than computation in WSN.

7. CONCLUSION

This work is motivated by the research work presented in [6, 8]. In this paper an effort has been made to couple Routing with Secure key management. Track /Sector and selection of two CHs has been unique features of this paper. The security scheme presented in this paper is energy efficient and at the same time it ensures that the whole network is never compromised even if there has been an attack in the network. This is possible because of clustering in terms of tracking and sectoring. However, there's a scope of improvement in this framework also. First of all if the nodes calculate most of the in its own level rather than depending on the BS to communicate the keys then there would be a lot of energy saving. If the packet size is reduced by dropping some of the redundant fields by decreasing the size of the keys stored then there would be less bandwidth usage. Further the whole security framework can be simulated/ implemented using the 'real sensor network scenario' using real sensor nodes. Further, the security framework can be implemented in Berkeley's motes for accurate results and for performance comparison with TinySec.

8. REFERENCES

1. David Boyle and Thomas Newe," Securing Wireless Sensor Networks: security Architectures" (2008), Journal of Networks, VOL. 3, NO. 1,pp 65-77.

2. Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, and J.D.Tygar. Spins: Security protocols for sensor networks. Wireless Networks, 8:521 – 534, 2002.

3. Zhu, S., Setia, S., Jajodia, S. (2003) ‘LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks’, CCS ’03, Washington D.C., USA, 27 – 31 October 2003, New York, USA: ACM Press, 62-72.

4. Zhu, S., Setia, S., Jajodia, S. (2006) ‘LEAP+: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks’, ACM Transactions on Sensor Networks TOSN,2(4), 500-528.

5. A.S.Poornima and B.B.Amberker,” Key Management Schemes for Secure Communication in Heterogeneous Sensor Networks”, International Journal of Recent Trends in Engineering, Vol 1, No. 1, May 2009.

6. T.A Zia and A.Y. Zomaya, ‘A Secure Triple-Key Management Scheme for wireless sensor networks’, in the proceedings of INFOCOM 2006,25th IEEE International Conference on Computer Communications, Barcelona, pp1-2 ,23-29 April 2006 .

7. W. Du, J. Deng, Y.S. Han, P.K. Varshney, A key predistribution scheme for sensor networks using deployment knowledge, IEEE Transactions on Dependable and Secure Computing, Vol. 3, issue 1, Jan-March 2006 pp.62-77.

8. Tanveer Zia and Albert Zomaya,” A Security Framework for Wireless Sensor Networks “, SAS 2006 – IEEE Sensors Applications Symposium Houston, Texas USA, 7-9 February 2006.

9. Navin Gautam, Won-Il Lee, Jae-Young Pyun, "Track-Sector Clustering for Energy Efficient Routing in Wireless Sensor Networks," cit, vol. 2, pp.116-121, 2009 Ninth IEEE International Conference on Computer and Information Technology, 2009.

10. Du X, Xiao Y, M Guizani, Chen H.H, (2007) “Effective key management for sensor networks, an effective key management scheme for heterogeneous sensor networks”, Ad Hoc Networks, Volume 5, Issue 1, 1 January 2007, Pages 24-34.

11. Kalpana Sharma, S.K. Ghosh, and M.K. Ghose ‘Establishing an Integrated Secure Wireless Sensor Network System: A New Approach’, International Journal of Next Generation Networks (IJNGN), Sept.2010

12. D. Liu and P. Ning, “Establishing Pairwise Keys in Distributed Sensor Networks”, ACM CCS 2003.

13. Kalpana Sharma, Anurag S. Rathor, S. R. Biradar, M.K Ghose ,‘Power-efficient Routing & Increased Yield Approach for WSNs ‘,International Journal on Computer Science and Engineering (IJCSE),Vol. 02, No. 03, 2010, pp 586-592.

14. C. karlof, N. Shastry and D. Wagner, TinySec: A link layer security architecture for wireless sensor networks, SenSys’04, November 3-5, 2004, Baltimore, Maryland, USA

15. Heinzelman, A. Chandrakasan and A. Balakrishnan,’ Energy-Efficient Communication Protocol for Wireless Microsensor Networks’, proceedings of the 33rd Hawaii International Conference on System Science, Jan 2000.

16. Bhaskaran Raman et. al, ‘Censor Networks: A Critique of “Sensor Networks” from a Systems Perspective’, ACM SIGCOMM Computer Communication Review, Volume 38, Number 3, July 2008.

17. Al-Sakib Khan Pathan et al. “Security in Wireless Sensor Networks: issues and Challenges”, ICACT2006 in Feb. 20-22, 2006, ISBN 89-5519-129-4 pp(1043-1048).

18. Sami S., Wakeel and Eng. Saad A. AL-Swailem,"PRSA: A Path Redundancy Based Security Algorithm for Wireless Sensor Networks", WCNC 2007 Proceedings, pp (4159-4163).

19. Ayman Khalil, Matthieu Crussière and Jean-François Hélard,'Cross Layer Resource Allocation Scheme under Heterogeneous constraints for Next Generation High Rate WPAN (2010),International Journal of Computer Networks and Communications(IJCNC) vol 2, No. 3.

20. A.R. Masoum, A.H. Jahangir,Z. Taghikhani, and R. Azarderakhsh, (2008) "A new multi level clustering model to increase lifetime in wireless sensor networks", Proceedings of the Second International Conference on Sensor Technologies and Applications, pp 185-190.

21. Germano Guimaraes, Eduardo Souto, Djamel Sadok, Judith Kelner (2005), "Evaluation of Security Mechanisms in Wireless Sensor Networks", proceedings of the 2005 Systems Communication (ICW '05) ,P 428-438, 0-7695-2422-2/05.

22. Kyung Jun Choi and Jong-In Song (2006), " Investigation of Feasible Cryptographic Algorithms for Wireless Sensor Network", in the proceedings of International Conference of Advanced Communication Techniques (ICACT 2006), 89-5519-129-4.

23. Soroush Hamed, Salajegheh Mastooreh and Dimitriou Tassos (2007) "Providing Transparent Security Services to Sensor Networks" Proceedings of IEEE International Conference on Communication (ICC'07).24-28 June 2007.

24. Zhou, Y., and Fang, Y. (2007), 'A two-layer key establishment scheme for WSN'. IEEE trans. Mobile Computing, Volume 6, No. 9, pp: 1009-1020.

25. Zhou, Y., Fang, Y., and Zhang, Y. (2008), 'A survey of Securing Wireless Sensor network'. IEEE communication surveys, Volume 10, No. 3, pp: 6-28.

26. Chan, H.,and Perrig, A., (2005), 'PIKE: Peer Intermediaries for Key Establishment in Sensor Networks'. In Proceedings of IEEE Infocom, Miami, Florida, pp: 524-535.

27. Ibriq, J., and Mahgoub, I. (2007), 'A Hierarchical Key Establishment Scheme for Wireless Sensor Networks'. 21st International Conference on Advanced Networking and Applications, pp: 210-219.

28. Undercoffer, J., Ayancha, S., Joshi, A., Pinkston, J. (2004), 'Security for Wireless Sensor Networks', Wireless Sensor Networks, Kluwer Academic Publishers Norwell, USA, pp: 253-275.

Security Architecture for On-Line Mutual Funds Trading With Multiple Mobile Agents

Nirmala C R nirmala_cr@hotmail.com
Asst. Professor /Department of CS &E
Bapuji Institute of Engineering & Technology
Davangere, 577004, India

Dr.V.Ramaswamy researchwork04@yahoo.com
Professor & Head, Computer Science & Engineering
S B M J C E
Bangalore, India

Abstract

In this paper we propose a security architecture for the transaction procedure of On-Line Mutual Fund Trading system which is implemented using multi mobile agents that helps an individual, who is a kind of Do It yourself investor to invest her/his money in mutual funds online. Here, we modify, design and implement the global standard which provides security for transaction processing in E-Commerce i.e. Secure Electronic Transactions (SET). This eliminates the fraud that normally occurs during money transaction on-line. Modified SET protocol provides authentication of the participants, non-repudiation, data integrity and confidentiality. These features give a guarantee of security during payment procedure. The system is implemented on Aglets Framework - ASDK2.0.2 which is Mobile Agent Development platform and using java programming language. The issues of security and performance are analyzed.

Keywords: Secure Electronic Transaction, User Agent1(UA1), User Mobile Agent1(UMA1), MFC Super Market, Banker Agent.

1. INTRODUCTION

Increasingly, people are dependent on computer networks and Internet to access and pay for goods and services with Electronic Money. E-money or digital cash is merely an electronic representation of funds. The primary function of e-cash or e-money is to facilitate transaction on the network. E-money is a necessary innovation in the financial markets. Where money is involved, fraud occurs by one or the other means. There must be a way to avoid such fraudulence. Hence we have come up with a complete security system for On-Line Mutual Funds Trading system by incorporating mobile agents and modified secure electronic transaction protocol. Our system is an E-commerce application, in which user can buy mutual funds online. This system is also implemented using mobile agent. The system has four interconnected modules namely user module, Mutual Funds Company Super Market module , Internet banking and Payment module and Share and stock market module.

The modifications that we have made to the original SET protocol is different from participants in SET, the card holder, merchant, acquirer and issuer. The main participants here are the Investor (I), The MFC Super Market (M), the IBP (P) and the certificate Authority (CA), which is trusted to issue X.509v3 public-key certificate for the participants. The IBP acts as a financial institution with which the Super market and the investor establish their accounts for processing payment On-Line. Each of these participants may possess two kinds of key certificates one for key exchange which is used for encryption and decryption operations, and the other for creation and verification of digital signature.

1.1 Secure Electronic Transaction

SET aims at achieving secure, cost-effective, on-line transactions that will satisfy market demand in the development of a single, open industry specification. VISA and MASTER CARD have jointly developed the SET protocol which is an application layer protocol. It is a method to secure payment card transaction over the open networks.

1) SET Business Requirements :These requirements specify the following aspects
    i. Provide confidentiality of payment and order information.
    ii. Ensure the integrity of all transmitted data
    iii. Provide authentication that a cardholder is a legitimate user of a credit card account
    iv. Provide authentication that a merchant can accept credit card transactions through its relationship with a financial institution
    v. Ensure the use of the best security practices and system design techniques to protect all legitimate parties in an electronic commerce transaction
    vi. Create a protocol that neither depends on transport security mechanisms nor prevents their use
    vii. Facilitate and encourage interoperability among software and network providers
2) Confidentiality: all messages encrypted
3) Trust: all parties must have digital certificates
4) Privacy: information made available only when and where necessary

1.2 Security Architecture of SET

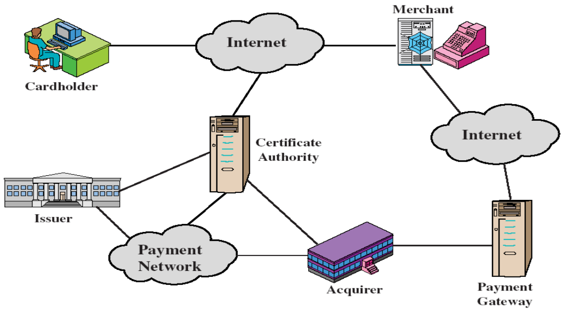


FIGURE 1: Security Architecture of SET

SET changes the way in which participants in the payment system interact. In face-to-face retail transaction or a mail order transaction, the electronic processing of the transaction begins with the merchant or the acquirer. Here the electronic transaction begins with the card holder. The other participant is Issuer, a financial institution which establishes an account for a card holder and issues the payment card. A merchant offers goods for sale or provides a service in exchange for payment. An acquirer is the financial institution that establishes an account with a merchant and processes payment card authorizations and payments. A payment gateway is a device operated by an acquirer or designated third party which processes merchant payment messages.

The encryption systems used by the SET Symmetric Key Encryption System

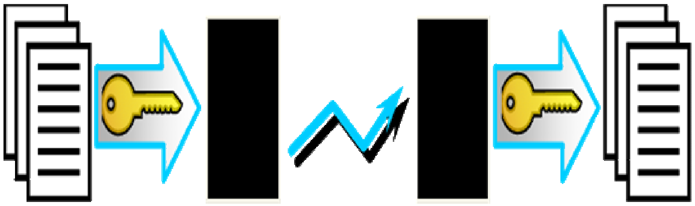
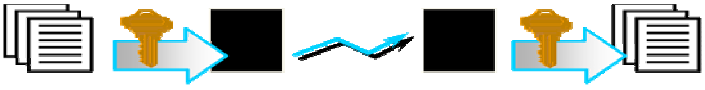


FIGURE 2: Symmetric Key Encryption

Here same key is used for both encryption and decryption. Examples are DES, 3DES and AES.

Public Key Encryption System



Each user has 2 keys: what one key encrypts, only the other key in the pair can decrypt.
Public key can be sent in the open.
Private key is never transmitted or shared.
Eg. RSA (Rivest, Shamir, and Adleman)

FIGURE 3: Public Key Encryption System

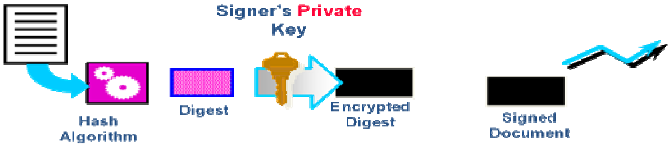


FIGURE 4 : Generating Dual Signature

- Links two messages securely but allows only one party to read each. Used in SET.

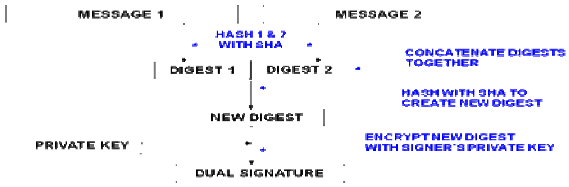

MESSAGE 1
MESSAGE 2
HASH 1 & 2 WITH SHA
DIGEST 1
DIGEST 2
CONCATENATE DIGESTS TOGETHER
HASH WITH SHA TO CREATE NEW DIGEST
NEW DIGEST
PRIVATE KEY
ENCRYPT NEW DIGEST WITH SIGNER'S PRIVATE KEY
DUAL SIGNATURE

FIGURE 5: Dual Signatures

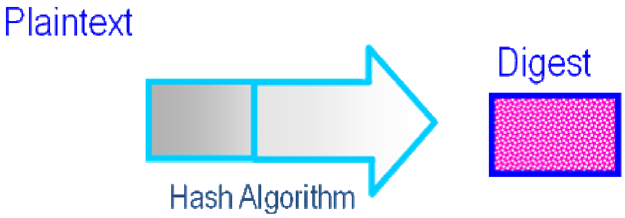


FIGURE 6: Generating Message Digest Using SHA-1

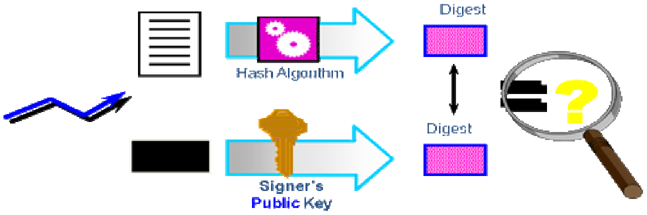


FIGURE 7: Verifying the Digital Signature.

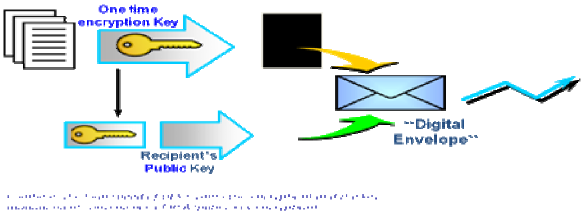


FIGURE 8: Generation of Digital envelop

1.3 Modified Secure Electronic Transaction Architecture

The modified Secure Electronic Transaction has the following architecture.

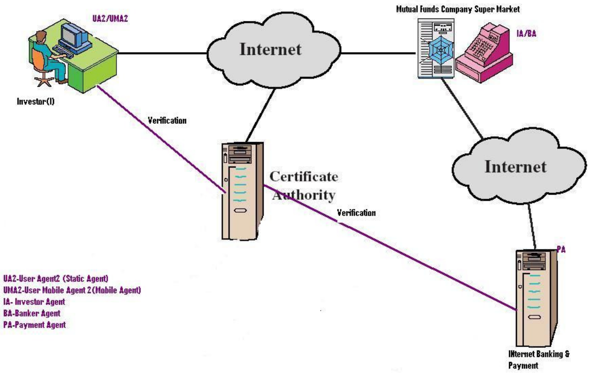


FIGURE 9: Modified SET Architecture

The participants in this architecture are Investor (I), Mutual Funds Company Super Market (M) and Internet Banking and Payment (B). The working process is given below. Consider an individual user who wishes to purchase mutual funds online.

- The user makes use of UA1 and UMA1, browses for the mutual funds and decides to purchase mutual funds.
- Now the second pair of agents at the client system UA2 and UMA2 dispatches encrypted dually signed order and payment information to MFC super market.
- Super market's Investor agent forwards payment Information to Banker Agent.
- Banker Agent in turn transfers the request to Payment Agent at IBP for payment authorization.
- The Investor Agent completes the order.

- Investor agent captures the transaction
- Notification is done to user/client

2. Applications of Modified SET and Multi Mobile Agents

Some of the notations used with the system are as follows.

$ENCk[M]$: encrypt message M with key k

KRi : IA's private Key

Kran: Random signature key generated by IA

Kub: IBP's Public key

Ds : Dual signature

$DS = ENCKRi[H(H(PI) \| H(OI))]$

PI: Confirmed Payment Information

OI: Selected Funds (Order Information)

Cert(x): X's certificate authorized by CA

ID: Transaction Identification

Following steps demonstrate how mobile agents and modified SET together work for securing a transaction of payment in case of user wants to purchase mutual funds online.

1. Investor creates UA2. This UA2 in turn creates UMA2 and fills it with funds selection form in which selected mutual funds are described in detail. The funds selection form later will be used as mutual fund order information (OI). UMA2 then transfers the request to investor agent of super market for performing the task of payment.

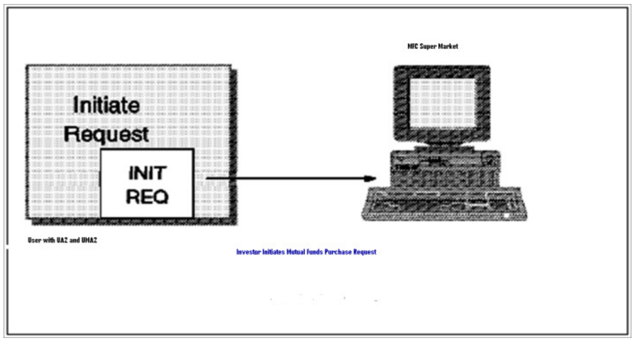


FIGURE 10: Investor Initiating the Purchase request

2. Investor agent who receives OI from UMA2 simply transfers this message to Banker Agent. BA in turn check the investors account balance. If there is sufficient balance, no money from IBP is required. The confirmation message is sent back to mobile agent to inform the investor and process the investor's portfolio management based on the request. Otherwise, the banker agent will assign a unique transaction identifier to the message and then pass its own signature certificate cert (M) and the IBP's key exchange certificate cert (IBP) along with the transaction ID to UMA2. UMA2 verifies super markets and IBP's certificate by tracing through the certificate authorities. It then holds them to be used later during the purchasing process. UA2 continues to create the approved selection form together with its payment.

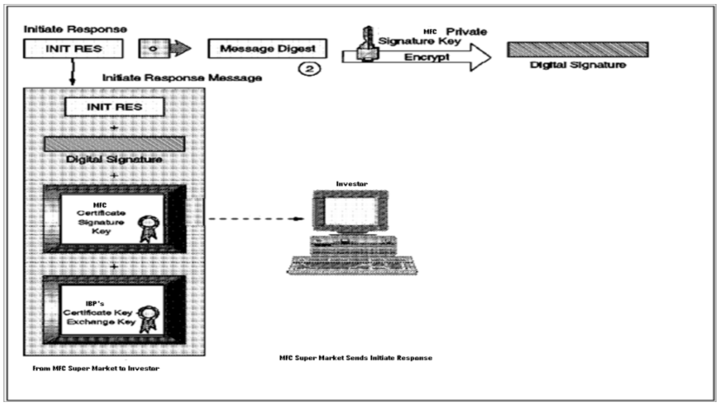


FIGURE 11: Super Market Initiating Response

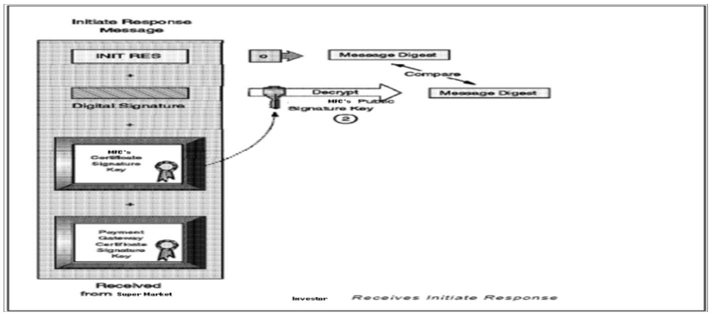


FIGURE 12 : Purchase Request.

3. UA2 dually signs on the two parts of the message (OI and PI) to generate dual signature. OI is the selected mutual fund and PI is the payment information. It then generates a random symmetric encryption key (Kran) and uses it to encrypt the dual signed payment information. Next, UA2 encrypts the PI as well as Kran into a digital envelop using Kub. Finally, UA2 transmits the whole message to UMA2 together with its certificate cert (I). UMA2 is dispatched to IA/BA at the super market.
4.

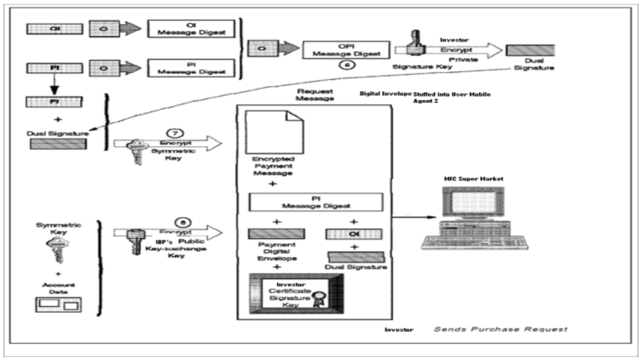


FIGURE 13: Creating and Sending the Digital Envelope

5. Banker Agent verifies the investor's certificate and the dual signature on the first part and then forwards the digital envelope to IBP for autherization. If the authorization response from IBP indicates that the transaction is approved, then the Banker Agent persues the service stated in the request form and at the same time generates the purchase complete message back to UMA2.

6. When UA2 retracts the UMA2 and recieves the message from super market, it verifies the super market signature certificate by traversing the trust ed CAs. It uses super market's public key to check the MFC's digital signature. If everything is correct, it takes necessary action.

In this sytem, most payment and redeem process are done by the mobile agents. The user agent need not be online all the time as defined by the SET protocol.

3. Analysis and Evaluation

The purpose of this work is to implement a secure payment procedure which provides security, confidentiality and data integrity during on-line purchasing of mutual funds. We will discuss some of the security and performance issues, advantages and disadvantages of the system.

3.1 Security Issues

System implementation is based on SET protocol specification with little modifications. Instead of card number, PAN number is used for authentication. Here, all the confidential actions such as signing, authentication, key generation and encryption are performed in the investor's computer (In SET it is done by the card holder). During transaction procedure, sensitive messages are encrypted using secret key. This can be decrypted using the entities which have the public key and read the messages. Finally, the transaction will be completed on IBP in a secured manner.

Note that in [7] MA has to compose OI, PI and generate random symmetric key while residing at the merchant server. This is a very dangerous operation since there is no highly secured way to protect MA from malicious hosts[10]. True there are approaches[11] using Hiding Encrypted Functions (HEF) which can build a secure mobile agent[9] that is capable of producing digital signature. But there is no clear, evidence to show that key materializing can be generated securely at remote server. Therefore, we place the key generation part in step 6 on UA and not on MA for providing secure transaction.

3.2 Performance

The major pit fall to an effective mutual fund transaction is the complexity of payment during the whole procedure. It delays the responses from the investors and thus brings the true compromise to this kind of business. How to make it more concise to pay becomes the crux of adapting proposed system to the real environment. The payment system in the real world is still a real bank based on off-line scheme.

In the system we have attempted to implement, while selecting a mutual fund, he or she can trigger Apriori Agent which does the auto selection of mutual funds. This saves time for user in searching and selecting mutual funds which match the investor profile at that instance. It also makes the choices more suitable to the investor.

In the transaction procedure, the investor payment from her/his online checking account, which is the account in the virtual bank (IBP) along with the certificates from the trusted CA. If it is a real deal, then money is transferred from real bank to IBP for which real bank gives security.

In this work, we have provided security only for transaction procedure. We would like to provide security for all agents and agents servers from malicious hosts and malicious agents using an inter IBP secure transaction and message exchange protocols, the system can be used under International scenario or in the larger perspective.

Beyond meeting the fundamental security and performance requirements, the system shall also have the following potential improvements.

Scalability

The proposed system can also be scaled to an international environment. Let us imagine such a scenario: in the near future where we can have an online network purchase and payment system around the world. There are many IBPs running at different levels, and different MFCs and investors from all over the world. The investors in one country can search for the MFCs from another country, and pay for her investment from an IBP from the third country, in which she has registered. Compared with the traditional system, the larger the application scenario, the more efficient the transaction.

Practicability

The whole system we describe here is a mutual fund system in the IBP environment. In fact, with the IBPs as the international financial service in the near future, we can also implement other transaction systems by referring to our online payment scheme.

Mobility

More and more mobile users are taking the convenience of mobile network. For example, the WAP users can enjoy great benefits from this system. Only with the mini-browser on her hand-phone, the investor can browse the investment information easily. Because the message exchanged online in this system is limited, with only a few clicks, the investor can finish the transaction assisted by MA in several minutes anywhere anytime via air.

Applicability

In this paper, we proposed a transaction scheme based on SET. It is fully compatible to the original SET. From the investor's point of view, she needs not to make any modification to her SET related software except embedding an agent that executes the investment functions. She may complete the whole transaction in a few steps without knowing the transaction details. This feature enables investors to provide uniform payment method to both online purchase and online investment on mutual funds with only one electronic IBP account, which improves the applicability of the proposed system.

4. Conclusion and Future Work

In this paper, we have analysed, implemented, designed and modified the secure electronic transaction protocol for our system “Multiple Mobile Agents for online Mutual funds trading”. This provides security in the form of authentication, data integration, non repudiation etc. This makes the investors to perform transaction without fear of losing their confidential information.

5. REFERENCES

1. Daniel Minoli and Emma Minoli “Web Commerce Technology Handbbok –Secure Electronic Transaction” –Tata McGraw-Hill Edition, 1999: ISBN:0-07-463742-8

2. Nirmala C R and Dr. V Ramaswamy “*Multiple Mobile Agent Architecture for On-Line Mutual Funds Trading*” – in the proceedings of IEEE -2nd International Conference on “E-Learning, E-Business, Enterprise Information Systems, and E-Government (EEEE 2010),. Volume No1. IEEE Catalogue Number: CFP1047I-PRT: ISBN: 978-1-4244-7689-3, pp. 243-246. Luoyang, China ,2010

3. Tieyan Li & Yan Jiang Yang *“Secure Mobile Agent Mediated System for Online Mutual Fund Trading”*

4. Krishna,V., Ramesh,V., *“Portfolio Management Using Cyberagents.”* IEEE international Conference on Systems, Man, and Cybernetics, 1998.

5. VISA INTERNATIONAL, and MASTERCARD INTERNATIONAL. “*Secure Electronic Transaction (SET) Specification.*” Version 1.0, May 1997.

6. Artur Romao and Miguel Mira de Silva. ``*An Agent-Based Secure Internet Payment System for Mobile Computing"*, Trends in Distributed Systems'98. Electronic Commerce, Hamberg, German, LNCS, June 3-5, 1998.

7. G.Vigna (Ed.). *Mobile Agents and Security*. Springer Verlag, LNCS 1419, 1998.

8. P. Kotzanikolaou et. al, "*Secure Transactions with Mobile Agents in Hostile Environments"*, LNCS1841, proceeding of 5th Australasian Conference, ACISP 2000, Brisbane, Australia, July 2000.

9. Sander,Tomas; Tschudin,Christian: *On Software Protection via Function Hiding*. Submitted to the 2nd International Workshop on Information Hiding, Dec 1998. http://www.icsi.berkeley.edu/~sander/publications/hiding.ps

ID-Based Directed Multi-Proxy Signature Scheme from Bilinear Pairings

B.Umaprasada Rao buprasad@yahoo.co.in
Research scholar
Dept. of Engineering Mathematics
A.U. College of Engineering
Andhra University
Visakhapatnam. A.P, INDIA.

Dr.P.Vasudeva Reddy vasucrypto@yahoo.com
Associate Professor
Dept. of Engineering Mathematics
A.U. College of Engineering
Andhra University
Visakhapatnam, A.P, INDIA.

Abstract

In a multi-proxy signature scheme, an original signer delegates his signing power to a group of proxy signers. Then the group of proxy signers cooperatively generates a multi-proxy signature on behalf of the original signer; and any one can verify the validity of the multi-proxy signature. But, when the signed message is sensitive to the signature receiver, it is necessary to combine the concepts of multi-proxy signatures with directed signatures. In this paper, we propose an identity based directed multi-proxy signature scheme using bilinear pairings. This scheme allows a group of proxy signers to generate a valid multi-proxy signature to a designated verifier. The designated verifier can only directly verify the multi-proxy signature generated by a group of proxy signers issued to him on behalf of the original signer and, in case of trouble or if necessary, he can convince any third party about the validity of the signatures. Finally, we discuss the correctness and security analysis of the proposed scheme.

Keywords: Public Key Cryptography, Proxy Signature Scheme, Multisignature Scheme, Proxy Signature Scheme, Bilinear Pairing, CDH Problem.

1. INTRODUCTION

Proxy signature, as an important cryptographic primitive, was firstly introduced by Mambo, Usuda, and Okamoto in 1996 [1]. In a proxy signature scheme, an original signer is allowed to delegate his signing power to a designated person called the proxy signer and the proxy signer is able to sign the message on behalf of the original signer. There are three types of delegation: full delegation; partial delegation and delegation by warrant. In full delegation, the original signer gives its private key to the proxy signer. In partial delegation, the original signer produces a proxy signature key from its private key and gives it to the proxy signer. The proxy signer uses the proxy signature key to sign. As far as delegation by warrant is concerned, warrant is a certificate composed of a message part and a public signature key. The proxy signer gets the warrant from the original signer and uses the corresponding private key to sign.

Since the proxy signature concept was proposed, various kinds of proxy signature schemes have been proposed such as threshold proxy signatures [2, 3, 4, 5, 6], multi proxy signatures [7, 8, 9], proxy multisignatures [10, 9, 8], proxy blind signatures [11, 12], multi proxy multi signatures [13, 14], ordered multi proxy [15], multi proxy multi signcryption [16,17] etc. In threshold proxy signature schemes, a group of *n* proxy signers share the secret proxy signature key. To produce a valid proxy signature on the message *m,* individual proxy signers produce their partial signatures on that message, and combine them into a full proxy signature on *m.* In a *(t, n)* threshold proxy signature scheme, the original signer authorizes a proxy group with *n* proxy members. Only the cooperation of *t* or more proxy members is allowed to generate the proxy signature. Threshold signatures are motivated both by the demand which arises in some organizations to have a group of employees agree on a given message or document before signing, and by the need to protect signature keys from attacks of internal and external adversaries.

In 1999, Sun proposed a threshold proxy signature scheme with known signers [4]. Then Hwang et al. [3] pointed out that Sun's scheme was insecure against collusion attack. By the collusion, any *t* - 1 proxy signers among *t* proxy signers can cooperatively obtain the secret key of the remainder one. They also proposed an improved scheme which can guard against the collusion attack. After that, [2] showed that Sun's scheme was also insecure against the conspiracy attack. In the conspiracy attack, *t* malicious proxy signers can impersonate some other proxy signers to generate valid proxy signatures. To resist the attack, they also proposed a scheme. Hwang et al pointed out [18] that the scheme in [3] was also insecure against the attack by the cooperation of one malicious proxy signer and the original signer.

As a special case of the threshold proxy signature, the multi-proxy signature scheme was first introduced by Hwang and Shi [7]. In a multi-proxy signature scheme, an original signer could authorize a group of proxy members and only the cooperation of all the signers in the proxy group can generate the proxy signatures on behalf of the original signer. Multi proxy signature scheme can be regarded as a special case of the (t,n) threshold proxy signature scheme [5] for$t=n$. It plays an important role in the following scenario: Suppose a president of a company needs to go on a business trip, during the trip he will receive many important documents must be signed by him. Some may need to be responded to quickly. To solve this problem, before going on a trip, the president can delegate his signing power to every department manager of the company. Then the document must be signed jointly by these department managers authorized by the president of the company. One solution to the case of this problem is to use a multi-proxy signature scheme.

A contrary concept, called proxy-multisignature is introduced by Yi et al. in 2000 [10], where a designated proxy signer can generate the signature on behalf of a group of original signers. Hwang and Chen [13] introduced the multi-proxy multi-signature scheme. Only the cooperation of all members in the original group can authorize a proxy group; only the cooperation of all members in the proxy group can sign messages on behalf of the original group.

Some designated verifier multi proxy signatures are also proposed in the literature [19]. In these schemes, an original signer could authorize a group of proxy members and only the cooperation of all the signers in the proxy group can generate the proxy signatures to a designated verifier on behalf of the original signer. The designated verifier only can directly verify the multi-proxy signature issued to him. In these schemes, the designated verifier cannot convince any third party about the validity of the multi-proxy signatures. To solve this problem, it necessary to combine the concepts of multi-proxy signatures with the directed signatures [20, 21, 22, 23].

Plenty of multi-proxy signature schemes have been proposed under the CA-based public key systems. The concept of ID-based public key system, proposed by Shamir in 1984 [24], allows a user to use his identity as the public key. It can simplify key management procedure compared to CA-based system, so it can be an alternative for CA-based public key system in some occasions, especially when efficient key management and moderate security are required. Many ID-based schemes have been proposed after the initial work of Shamir, but most of them are impractical for low efficiency. Recently, the bilinear pairings have been found various applications in cryptography, more precisely; they can be used to construct ID-based cryptographic schemes [25, 26, 27, 28, 29].

Motivated by the mentioned above, in this paper, based on Hess ID-based signature scheme [28], a directed multi-proxy signature scheme is proposed. In the proposed scheme, the designated verifier can only directly verify the multi-proxy signature generated by a group of proxy signers issued to him, on behalf of the original signer, and he can convince any third party about the validity of the signatures. To the best of our knowledge there is no existing scheme on this concept. The proposed scheme can provide the security properties of proxy protection, verifiability, strong identifiability, strong unforgeability, strong nonrepudiability, distinguishability, and prevention of misuse of proxy signing power.

The rest of the paper is organized as follows. Section 2 briefly explains the bilinear pairings and some computational problems on which of our scheme is based. The syntax and security model of ID-based Directed Multi Proxy Signature Scheme is given in Section 3. We then present our ID-based Directed Multi Proxy Signature (ID-DMPS) Scheme in Section 4. The correctness and security analysis of the proposed scheme is given in Section 5. Section 6 concludes this paper.

2. PRELIMINARIES

In this section, we will briefly review the basic concepts on bilinear pairings and some related mathematical problems.

2.1 Bilinear Pairings

Bilinear pairing is an important cryptographic primitive and has been widely adopted in many positive applications in cryptography.

Let G_1 be a additive cyclic group generated by P, whose order is a prime q, and G_2 be a multiplicative cyclic group of the same order q. A bilinear pairing is a map $e: G_1 \times G_1 \to G_2$ with the following properties:

1. Bilinear: $e(aP, bQ) = e(P,Q)^{ab}$, for all $P, Q \in G_1$ and all $a, b \in Z_q^*$.
2. Non –degenerate: There exists $P, Q \in G_1$ such that $e(P,Q) \neq 1$.
3. Computable: There is an efficient algorithm to compute $e(P,Q)$ for all $P, Q \in G_1$.

Such a pairing may be obtained by suitable modification in the Weil-pairing or the Tate-pairing on an elliptic curve defined over a finite field [25].

2.2 Computational Problems

Now, we give some computational problems, which will form the basis of security for our scheme.

Decisional Diffie-Hellman Problem (DDHP): For $a, b, c \in_R Z_q^*$, given $P,\ aP, bP, cP$ in G_1, decide whether $c \equiv ab \bmod q$.

Computational Diffie-Hellman Problem (CDHP): For $a, b, c \in_R Z_q^*$, given $P,\ aP,\ bP$ in G_1 Compute abP.

Bilinear Diffie-Hellman Problem (BDHP): For $a, b, c \in_R Z_q^*$, given $P,\ aP,\ bP, cP$ in G_1, compute $e(P,P)^{abc}$ in G_2.

Gap Diffie-Hellman Problem: A class of problems, where DDHP can be solved in polynomial time but no probabilistic algorithm exists that can solve CDHP in polynomial time.

Such groups can be found in supersingular elliptic curve or hyperelliptic curve over finite fields, and the bilinear pairings can be derived from the Weil or Tate pairings. For more details, see [25].

3. SYNTAX AND SECURITY REQUIREMENTS FOR ID-DMPS SCHEME

In this section, we give formal model and some security requirements for our ID-based directed multi-proxy signature scheme (ID-DMPS).

3.1 Syntax of ID-Based Directed Multi-Proxy Signature Scheme

Our scheme has five phases described as follows:
In our identity-based multi-proxy signature scheme, there is an original signer and a group of proxy signers. Let **O** be the original signer and $L = \{PS_1, PS_2, ..., PS_n\}$ be the group of proxy signers designated by **O**. Sometimes there may be a clerk or a chairman of the group. For $i \in \{1, 2, .., n\}$, PS_i has an identity IDs_i, **O** has an identity ID_o.

Our ID-DMPS scheme consists of the following five algorithms.

- **Setup:** This algorithm is run by the PKG on input a security parameter $l \in N$, and generates the public parameters of the scheme and a master secret $< s >$. The PKG publishes system parameters as *params* and keeps the $< s >$ as secret.

- **Extract:** Given an identity ID, *params*, this algorithm generates the private key d_{ID} of ID. The PKG will use this algorithm to generate private keys for all participants in the scheme and distribute the private keys to their respective owners through a secure channel.

- **Generation of the Proxy Key:** This is a protocol between the original signer and all proxy signers. All participants input their identities $ID_{s_i}, 0 \le i \le n,$ the proxy signers also take as input their private keys $d_{ID_{s_i}}, 1 \le i \le n,$ and the delegation warrant ω which includes the type of the information delegated, the period of delegation etc. The original signer also inputs his secret key d_{IDo}. As a result of the interaction, every proxy signer outputs a *partial proxy signing key* $SKP_i(1 \le i \le n)$.

- **Multi-proxy Signature Generation:** This is a randomized algorithm. Every PS_i takes input his partial signing key $SKP_i(1 \le i \le n),$ the warrant m_ω,the designated verifier's identity ID_V , and the message $M \in \{0,1\}^*$. In the end, outputs a *directed multi-proxy signature* σ on the message M on behalf of the original signer.

- **Multi-proxy Direct Verification:** It is a deterministic algorithm. It takes input the identities $ID_{s_i}, 0 \le i \le n,$ the warrant ω, the message M and a directed multi-proxy signature σ for M, the algorithm outputs 1 if σ is a valid multi-proxy signature for M by the proxy signers on behalf of the original signer, and outputs 0 otherwise.

- **Multi-proxy Public Verification:** It is a deterministic algorithm. It takes identity of the original signer ID_o, identities of the proxy signers IDs_i, identity of the designated verifier ID_V, message M, warrant ω, Aid provide by ID_V or Clark and multi-proxy signature σ as input, outputs 1if σ is valid or 0 otherwise.

3.2 Security Requirements of ID-Based Directed Multi Proxy Signature

The following are general security requirements of the proposed scheme.

- **Verifiability:** From the proxy signature, the verifier can be convinced of the original signer's agreement on the signed message.
- **Strong Identifiably:** Anyone can determine the identity of the corresponding proxy signer from the proxy signature.
- **Strong Undeniability:** Once a proxy signer creates a valid proxy signature of an original signer, he cannot repudiate the signature creation.
- **Distinguishability:** Proxy signatures are distinguishable from normal signatures by everyone.
- **Prevention of Misuse**: The proxy signer cannot use the proxy key for other purposes than generating a valid proxy signature. That is, he cannot sign, with the proxy key, messages that have not been authorized by the original signer.
- **Strong Unforgeability:** A designated proxy signer can create a valid proxy signature for the original signer. But the original signer and other third parties who are not designated as a proxy signer cannot create a valid proxy signature.
- **Strong Designated Verifiability:** The designated verifier uses his/her secret key to verify the proxy signature generated by a proxy signer on behalf of the original signer to designated verifier. So, only the designated verifier can verify the proxy signature issued to him.

4. PROPOSED SCHEME ID-BASED DIRECTED MULTI-PROXY SIGNATURE SCHEME FROM BILINEAR PAIRINGS

The proposed scheme involves four roles: the private key generator (PKG), the original signer, a set of proxy signers $L=\{PS_1,PS_2,.....,PS_n\}$ and the verifier. It consists of the following Six algorithms.

Setup: Given security parameter l, the PKG chooses groups G_1 and G_2 be additive and multiplicative groups of prime order $q>2^l$ with a bilinear pairing $e:G_1 \times G_1 \to G_2$ and a generator P of G_1. PKG then selects $s \in Z_q^*$ randomly and compute the public key $P_{pub}=sP$, also picks cryptographic hash functions $H_1,H_2:\{0,1\}^* \to G_1^*$ and $h:\{0,1\}^* \times G_2 \to Z_q^*$. The private key generator PKG now publishes system parameters as $params =< G_1,G_2,q,e,P,P_{pub},H_1,H_2,h >$, and keeps $< s >$ secret as the master secret key.

Private key Extraction: Let the original signer identity ID_o and his private key $d_{ID_o}=sQ_{ID_o}=sH_1(ID_o)$, and $\{PS_i\}$ be the proxy signers with identity $\{IDs_i\}$ and their corresponding private key $d_{IDs_i}=sQ_{IDs_i}=sH_1(IDs_i)$, for $1 \le i \le n$.

Generation of the Proxy Key: To delegate the signing power to proxy signers, the original signer uses Hess's ID-based signature scheme [28] to generate the signed warrant m_w and each proxy signer PS_i computes his proxy key SKP_i.

- The original signer computes $U_o = e(P,P)^{K_o}$, where $k \in_R Z_q^*$, $H_o = H_2(ID_o, m_w, U_o)$, $V_o = h(U_o, H_o)$ and then computes $W_o = V_o d_{ID_o} + k_o P$.
- The signature on m_w is the warrant $\langle m_w, W_o, V_o \rangle$ then he sends $\langle m_w, W_o, V_o \rangle$ to each proxy signer in the proxy group L.
- Each $PS_i \in L$ verifies the validity of the signature on m_w by computing $U_o = e(W_o, P)\, e\left(Q_{ID_o}, P_{pub}\right)^{-V_O}$ and $H_o = H_2(ID_o, m_w, U_o)$. Accepts the signature if and only if $V_o = h(U_o, H_o)$.

If the signature valid, each PS_i computes the *proxy key* SKP_i as $SKP_i = V_o d_{IDs_i} + W_o$.

Multi-Proxy Signature Generation: Suppose the proxy group L want to sign a delegated message m, on behalf of the original signer, to the designated verifier V. Each proxy signer PS_i generates the partial signature and an appointed clerk C, who is one of the proxy signers, combines the partial proxy signatures to generate the final multi-proxy signature.

- Each PS_i randomly selects two integers $k_i, r_i \in_R Z_q^*$, computes $U_{P_i} = e(P,P)^{k_i}$, $R_{P_i} = r_i Q_{IDs_i}$, $L_{P_i} = e\left(d_{IDs_i}, r_i Q_{IDv}\right)$ and broadcast U_{P_i}, L_{P_i} to the remaining (n-1) signers.
- Each PS_i computes $U_P = \prod_{i=1}^{n} U_{P_i}$, $L_P = \prod_{i=1}^{n} L_{P_i}$, $R_P = \sum_{i=1}^{n} R_{P_i}$, $V_P = h(U_P, H_P)$ and broadcast to the clerk .
- Each proxy signer also computes $V_{P_i} = h\left(U_{P_i}, H_P\right)$ and $W_{P_i} = V_P SKP_i + k_i P,$ where $H_P = H_2(M, L_P)$.

Finally the individual proxy signature of message m is $\langle V_{P_i}, W_{P_i}, R_{P_i} \rangle$.

- All the proxy signers send their partial signatures to the clerk C. The clerk verifies each individual signature by checking the equality

$$V_{P_i} = h\left(H_2(M, L_P), e\left(W_{P_i}, P\right)\left(e\left(Q_{ID_o} + Q_{IDs_i}, P_{pub}\right)^{V_o} U_o \right)^{-V_P} \right).$$

Once all individual proxy signatures are correct, the clerk C computes $W_P = \sum_{i=1}^{n} W_{P_i}$.

The valid directed multi-proxy signature is the tuple $\sigma = \langle m, m_w, V_P, W_P, R_p, U_o \rangle$.

Direct Verification: The designated verifier ID_V first evaluate

$$U_P = e(W_P, P)\left(e\left(\sum_{i=1}^{n} \left(Q_{ID_o} + Q_{IDs_i}\right), P_{pub} \right)^{V_O} .U_o^n \right)^{-V_P}$$ and $H_P = H_2\left(m, e\left(d_{ID_V}, R_P\right)\right)$. He then accepts the signature if and only if $V_P = h(H_P, U_P)$.

Public Verification: In case of trouble or if necessary, any third party T can verify the validity of multi-proxy signature with the help of the $Aid = e\left(d_{ID_V}, R_P\right) = L_P$ provided by either the clerk C or the designated verifier ID_V. Now with this Aid, T computes $U_P = e(W_P, P)\left(e\left(\sum_{i=1}^{n} \left(Q_{ID_o} + Q_{IDs_i} \right), P_{pub} \right)^{V_O} .U_o^n \right)^{-V_P}$ and $H_P = H_2(m, Aid)$. T accepts the signature if and only if $V_P = h\left(H_P, U_P \right)$.

5. ANALYSIS OF THE PROPOSED SCHEME

In this section first we discuss proof of correctness and then security analysis of the ID-DMPS scheme.

5.1 Proof of Correctness

The following equations give the proof of correctness for individual proxy signer's signature.

$$
\begin{aligned}
& e\left(W_{P_i}, P\right)\left(e\left(Q_{ID_O} + Q_{IDs_i}, P_{pub}\right)^{V_o} U_o\right)^{-V_P} \\
& = e\left(W_{P_i}, P\right)\left(e\left(Q_{ID_o} + Q_{IDs_i}, P_{pub}\right)^{V_o} U_o\right)^{-V_P} \\
& = e\left(V_P SKP_i + k_i P, P\right)\left(e\left(d_{ID_o} + d_{IDs_i}, P\right)^{V_o} U_o\right)^{-V_P} \\
& = e\left(V_P SKP_i, P\right) e\left(k_i P, P\right)\left(e\left(SKP_i - W_o + W_o - k_o P, P\right) U_o\right)^{-V_P} \\
& = e\left(SKP_i, P\right)^{V_P} e\left(P, P\right)^{k_i} e\left(SKP_i, P\right)^{-V_P} e\left(-k_o P, P\right)^{-V_P} U_o^{-V_P} \\
& = e\left(P, P\right)^{k_i} = U_{P_i}.
\end{aligned}
$$

The following equations give the proof of correctness for multi-proxy signature.

$$
\begin{aligned}
& e(W_P, P)\left(e\left(\sum_{i=1}^{n} \left(Q_{ID_o} + Q_{IDs_i} \right), P_{pub} \right)^{V_o} .U_o^n \right)^{-V_P} \\
& = e\left(\sum_{i=1}^{n} W_{P_i}, P \right)\left(e\left(\sum_{i=1}^{n} \left(Q_{ID_o} + Q_{IDs_i} \right), P_{pub} \right)^{V_o} U_o^n \right)^{-V_P} \\
& = e\left(\sum_{i=1}^{n} (V_P SKP_i + k_i P), P \right)\left(e\left(\sum_{i=1}^{n} \left(d_{ID_o} + d_{IDs_i} \right), P \right)^{V_o} U_o^n \right)^{-V_P} \\
& = \left(\sum_{i=1}^{n} (V_P SKP_i + k_i P), P \right)\left(e\left(\sum_{i=1}^{n} (SKP_i - W_o + W_o - k_o P), P \right) U_o^n \right)^{-V_P} \\
& = e\left(\sum_{i=1}^{n} SKP_i, P \right)^{V_P} \prod_{i=1}^{n} e\left(P, P\right)^{k_i} e\left(\sum_{i=1}^{n} SKP_i, P \right)^{-V_P} e\left(\sum_{i=1}^{n} -k_o P, P \right)^{-V_P} \left(U_o^n\right)^{-V_P} \\
& = \prod_{i=1}^{n} e\left(P, P\right)^{k_i} = U_P
\end{aligned}
$$

5.2 Security Analysis

Our ID-DMPS scheme satisfies the following security requirements which are stated in section 3.2.

Strong Identifiability: Because identity pubic key Q_{IDs_i} of all proxy signers are involved in the verification of the proxy signature, anyone can identify all the proxy signers.

Strong Undeniability: The clerk verifies the individual proxy signature of each proxy signer, so no one can be deniable of his signature.

Distinguishability: This is obvious, because there is a warrant m_w in a valid multi-proxy signature, at the same time, this warrant m_w and the public keys of the original signer and the proxy signers must occur in the verification process.

Prevention of Misuse: Due to using the warrant m_ω, the proxy signers can only sign messages that have been authorized by the original signer.

Strong Unforgeability: In general, there are mainly three kinds of attacks: *outsiders*, who are not participating in the issue of the proxy signature; some *signers* who play an active in the signing protocol and the *user* (signature owner). Furthermore, some of these attackers might collude. The outsider-attack consists of the original signer attack and any third adversary attack. We assume that the third adversary can get the original signer's signature on warrant m_ω (So, our scheme needs not the secure channel for the delivery of the signed warrant). Even this, he forges the multi-proxy signature of the message $m^{'}$ for the proxy group *L* and the original signer, this is equivalent to forge a Hess's ID-based signature with some public key. On the other hand, the original signer cannot create a valid multi-proxy signature since each proxy key includes the private key d_{IDs_i} of each proxy signer.

In our scheme, the clerk is one of the proxy signers, but he has more power than other proxy signers. Assume that the clerk wants the proxy group to sign the false message $m^{'}$. He can change his U_{P_i} , therefore U_P can be changed, but from the security of the basic ID-based signature scheme and public one-way hash function H_2, it is impossible for the clerk to get $V_P^{'}$ and $W_P^{'}$ such that $\left\langle m, m_w, V_P, W_P, R_p, U_o \right\rangle$ is a valid multi-proxy signature. Also, the attack of some signers collude can be prevented for the identity of each proxy signer is involved in the verification of the signature.

Finally, the user can not forge the multi-proxy signature because he can not obtain more information than the Clerk.

Designated Verifiability: The designated verifier ID_V has to use his secret key d_{ID_V} at the time of verification of the multi-proxy signature. So, only the designated verifier can directly verify the validity of the proxy signature. No one can verify the validity of the multi-proxy signature without the help of either the designated verifier ID_V or the designated Clark.

5.3 Performance Analysis

Performance of signature scheme protocols can be approximated in terms of computation and communication overheads. In this section, we mainly discuss the performance of pro posed ID-DMPS scheme.

For convenience, the following notations are used to analyze the computation and communication complexity. T_{smul} represents the time for one scale multiplication in G_1, T_{pair} denotes the total one pairing computation; T_{mhash} define the time for one Map-to-Point hash function; N_t denotes the total number of transmissions and N_b denotes the total number of broadcasts. Note that the times for other computations or operations are ignored, since they are much smaller than T_{smul}, T_{pair} and T_{mhash}.

We summarize the computation and communication overheads of our proposed ID-DMPS scheme in Table1. As shown in Table1, The computation complexity for Setup, Extract, Generation of proxy key, Multi signature generation, Direct verification, Public verification algorithms are $1T_{smul}$, $(n+1)T_{smul}+(n+1)T_{mhash}$, $(2n+1)T_{pair} + (2n+2)T_{mhash} + (n+2)T_{smul}$, $4nT_{pair}+(3n+1)T_{mhash}+4nT_{smul}$, $3T_{pair}+2T_{mhash}$ and $2T_{pair}+2T_{mhash}$ respectively. Also the total communication overheads for generation of Proxy Key and Multi-Proxy signature generation algorithms are nN_t, nN_b+2nN_t respectively in our ID-DMPS scheme.

	Computation overheads	**Communication overheads**
System Setup	$1T_{smul}$	--
Key Extract	$(n+1)T_{smul}+(n+1)T_{mhash}$	--
Generation of proxy key	$(2n+1)T_{pair}+(2n+2)T_{mhash}+(n+2)T_{smul}$	nN_t
Multi-Proxy Signature Generation	$4nT_{pair}+(3n+1)T_{mhash}+4nT_{smul}$	nN_b+2nN_t
Multi-Proxy Direct Verification	$3T_{pair}+2T_{mhash}$	--
Multi-Proxy Public Verification	$2T_{pair}+2T_{mhash}$	--

TABLE 1: Computation and Communication Overheads for ID-DMPS Scheme

6. CONCLUSION

Proxy signature is an indispensable mechanism in the modern e-business and e-government infrastructures. Many variants of proxy signatures have been proposed in the literature. In this paper, we propose an ID-based directed multi-proxy signature scheme using bilinear pairings. This scheme allows only a designated verifier to directly verify the multi-proxy signature, generated by a group of proxy signers on behalf of the original signer, issued to him. In case of trouble or if necessary the designated verifier can prove the validity of the multi-proxy signature to any third party. Our scheme satisfies the security requirements such as strong identifiability, strong undeniability, distinguish ability, prevention of misuse of proxy signing power, strong unforgeability and designated verifiability. The proposed scheme is suitable for some applications where the signed message is personally or commercially sensitive to the signature receiver.

REFERENCES

[1] M. Mambo, K. Usuda, and E.Okamoto. “Proxy Signatures for Delegating Signing Operation”. *In: 3rd ACM Conference on Computer and Communications Security(CCS'9),* pp.48-57, *New York*, ACM, 1996.

[2] C.L Hsu, T.S. Wu and T.C. Wu. “New Nonrepudiable Threshold Proxy Signature Scheme with Known Signers”. The Journal of Systems and Software, 58, pp.119-124, 2001.

[3] M.S.Hwang, I.C. Lin and J.L. Lu Eric. “A Secure Nonrepudiable Threshold Proxy Signature Scheme with Known Signers”. International Journal of Informatica, 11(2), pp.1-8, 2000.

[4] H.M. Sun. “An Efficient Nonrepudiable Threshold Proxy Signature Scheme with Known Signers”. Computer Communications, 22(8), 1999, pp.717-722.

[5] K. Zhang. “Threshold Proxy Signature Schemes”. Information Security Workshop, pp.191-197, Japan, 1997.

[6] J. Liu and S. Huang. “Identity-Based Threshold Proxy Signature from Bilinear Pairings”. Informatica, Inst. Math & Science, Vol. 21, No. 1, pp. 41-56, IOS press, 2010.

[7] S.J. Hwang, and C. H. Shi. “A Simple Multi-Proxy Signature Scheme”. Proceeding of the Tenth National Conference on Information Security, Taiwan, pp.134-138, Techinical report, 2000.

[8] X. Li, and K. Chen. “ID-based Multi-Proxy Signature, Proxy Multi-Signature and Multi-Proxy Multi-Signature Schemes from Bilinear Pairings”. Applied Mathematics Computation, Vol. 169, Issue 1, pp. 437-450, Elsevier, 2005.

[9] X. Li, K. Chen, and S. Li. “Multi-Proxy Signature and Proxy Multi-Signature Schemes from Bilinear Pairings”. Proceedings of PDCAT 2004*,* LNCS 3320, pp. 591–595, Springer-Verlag, 2004.

[10] L.Yi, G. Bai and G. Xiao. “Proxy Multi-Signature Scheme: A New Type of Proxy Signature Scheme”. Electronic Letters, Vol.36, No.6, pp.527-528, IEEE, 2000.

[11] S. Lal and A. K. Awasthi. “Proxy Blind Signature Scheme”. IACR, Cryptology e-print Archive*,*Report 2003/072, 2003. http://eprint.iacr.org.

[12] B. Majhi, D.K. Shau, and R.N. Subudhi. “An Efficient ID-Based Proxy Signature, Proxy Blind Signature and Proxy Partial Blind Signature”. International conference on Information Technology*,* pp. 19-23, IEEE, 2008.

[13] J.Hwang, and C. H. Chen. “A New Multi-Proxy Multi-Signature Scheme”, *2001* National Computer Symposium: Information Security, Taiwan, pp.19-26, 2001.

[14] X. Li, and K. Chen. “ID-based Multi-Proxy Signature, Proxy Multi-Signature and Multi-Proxy Multi-Signature Schemes from Bilinear Pairings”. Applied Mathematics Computation, Vol. 169, Issue 1, pp. 437-450, Elsevier, 2005.

[15] M. S. Hwang, S. F. Tzeng, S. F. Chiou. “An Ordered Multi-Proxy Multi- Signature Scheme”. Proceedings of the 8th International Conference on Intelligent Systems Design and Applications*,* Vol. 03, pp. 308-313, IEEE Computer Society, 2008.

[16] Y.Sun, C. Xu, F.Li, and Y.Yu. “Identity Based Multi-Proxy Multi-Signcryption Scheme for Electronic Commerce”. Proceedings of the5th International Conference on Information Assurance and Security, Vol.02, pp. 281-284, IEEE, 2009.

[17] Z. Xiaoyan, W.Yan, D .Wiefeng, and G. Yan. “An Improved ID-Based Multi-Proxy Multi-Signcryption Scheme”. Proceedings of the 2nd International Symposium on Electronic Commerce and Security, Vol.01, pp. 466-469, IEEE Computer Society, 2009.

[18] S.J Hwang and C.C. Chen. “Cryptanalysis of Nonrepudiable Threshold Proxy Signature Scheme with Known Signers”. INFORMATICA, 14(2), pp.205-212, 2003.

[19] F. Li, Q. Xue, and Z. Cao “Bilinear pairings based designated-verifier multi-proxy signature scheme”, IT Revolutions, 2008 First Conference on, 2008.

[20] S. Lal and M. Kumar. “A directed signature scheme and its applications”. Proceedings of National conference on Information Security, pp. 124-132, New York, 8-9 Jan, 2003.

[21] R.Lu, X.Lim, Z.Cao, J.Shao and X.Liang, "New (t, n) threshold directed signatures schemes with provable security", Information Sciences 178, pp.156-165,2008.

[22] X. Sun, Jian-hua Li, Gong-liang Chen, and Shu-tang Yung. "Identity-Based Directed Signature Scheme from Bilinear Pairings". Cryptology eprint Archive, Report 2008/305, 2008. http:// *eprint.iacr.org.*

[23] B.Umaprasada Rao, P.Vasudeva Reddy, and T.Gowri. "An efficient ID-based DirectedSignature Scheme from Bilinear Pairings". Cryptography e-print Archive Report 2009/617, Available at http://eprint.iacr.org.

[24] A. Shamir. "Identity-based cryptosystems and signature schemes". Advances in Cryptology-Crypto 84, LNCS 196, Springer-Verlag, pp.47-53, 1984.

[25] D. Bonech and M. Franklin. "Identity Based Encryption from the Weil pairing". Advance in CRYPTO'01, LNCS 2139, pp.213-229, Springer-Verlag, 2001.

[26] D. Boneh, B. Lynn, and H. Shacham. "Short signatures from the Weil pairing". Advances in Cryptology-Asiacrypt'01, LNCS 2248, pp.514-532, Springer-Verlag, 2001.

[27] J.C. Cha and J.H. Cheon. "An identity-based signature from gap Diffie-Hellman groups". Public Key Cryptography 03, LNCS 2139, pp.18-30, Springer-Verlag, 2003,.

[28] F. Hess. "Efficient identity based signature schemes based on pairings". SAC 02, LNCS 2595, pp. 310-324, Springer-Verlag, 2002.

[29] F. Zhang and K. Kim. "ID-based blind signature and ring signature from pairings". Advances in Cryptology-Asiacrypt 02, LNCS 2501, pp. 533-547, Springer-Verlag, 2002.

Systematic Digital Forensic Investigation Model

Mr. Ankit Agarwal cs.ankit11@gmail.com
Sr. Lecturer,Northern India Engineering College, GGSIPU
Delhi- 110053 India

Ms. Megha Gupta meghag2@gmail.com
Lecturer,Northern India Engineering College, GGSIPU
Delhi- 110053 India

Mr. Saurabh Gupta er.saurabh@gmail.com
HOD,Northern India Engineering College, GGSIPU
Delhi- 110053India

Prof. (Dr.) Subhash Chandra Gupta gupta_subhash@yahoo.com
Director,Northern India Engineering College, GGSIPU
Delhi- 110053 India

Abstract

Law practitioners are in an uninterrupted battle with criminals in the application of digital/computer technologies, and require the development of a proper methodology to systematically search digital devices for significant evidence. Computer fraud and digital crimes are growing day by day and unfortunately less than two percent of the reported cases result in confidence. This paper explores the development of the digital forensics process model, compares digital forensic methodologies, and finally proposes a systematic model of the digital forensic procedure. This model attempts to address some of the shortcomings of previous methodologies, and provides the following advantages: a consistent, standardized and systematic framework for digital forensic investigation process; a framework which work systematically in team according the captured evidence; a mechanism for applying the framework to according the country digital forensic investigation technologies; a generalized methodology that judicial members can use to relate technology to non-technical observers.

This paper present a brief overview of previous forensic models and propose a new model inspired from the DRFWS Digital Investigation Model, and finally compares it with other previous model to show relevant of this model. The proposed model in this paper explores the different processes involved in the investigation of cyber crime and cyber fraud in the form of an eleven-stage model. The Systematic digital forensic investigation model (SRDFIM) has been developed with the aim of helping forensic practitioners and organizations for setting up appropriate policies and procedures in a systematic manner.

keywords : Digital Crime, Digital Devices, Forensic Investigation, Search & Seizure, Wireless devices.

1. INTRODUCTION

Computer forensics emerged in response to the escalation of crimes committed by the use of computer systems either as an object of crime, an instrument used to commit a crime or a repository of evidence related to a crime. Computer forensics can be traced back to as early as 1984 when the FBI laboratory and other law enforcement agencies begun developing programs to examine computer evidence. Research groups like the Computer Analysis and Response Team (CART), the Scientific Working Group on Digital Evidence (SWGDE), the Technical Working Group on Digital Evidence (TWGDE), and the National Institute of Justice (NIJ) have since been formed in order to discuss the computer forensic science as a discipline including the need for a standardized approach to examinations [1].

Digital forensics has been defined as the use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal or helping to anticipate the unauthorized actions shown to be disruptive to planned operations. One important element of digital forensics is the credibility of the digital evidence. Digital evidence includes computer evidence, digital audio, digital video, cell phones, digital fax machines etc. The legal settings desire evidence to have integrity, authenticity, reproductively, non-interference and minimization [2].

Since computer forensics is a relatively new field compared to other forensic disciplines, which can be traced back to the early 1920s, there are ongoing efforts to develop examination standards and to provide structure to computer forensic examinations. This paper attempts to address the methodology of a computer forensic investigation.

2. PREVIOUS INVESTIGATION

Computer and network forensics methodologies consist of three basic components that Kruse and Heiser[3] refer to as the three as of computer forensics investigations. These are:

- Acquiring the evidence while ensuring that the integrity is preserved;
- Authenticating the validity of the extracted data, which involves making sure that it is as valid as the original
- Analyzing the data while keeping its integrity.

The field of digital forensics is undergoing a rapid metamorphosis: it is changing from skilled craftsmanship into a true forensic science. Part of this change is expressed by the interest in this field as an academic study. Ironically, the teaching portion of academe has led the way and research is trying to catch up.

Research usually starts with a literature review. That is particularly difficult in this field for a number of reasons. Some of the work predates the Internet and therefore is only available in paper form, in largely obscure or unavailable documents. Much discussion and learning has not been published at all. And few are familiar with the work that has been published.

2.1 The Forensic Process Model [4]

The U.S. Department of Justice published a process model in the Electronic Crime Scene Investigation: A guide to first responders that consists of four phases: -

- **Collection**

which involves the evidence search, evidence recognition, evidence collection and documentation.

- **Examination**

This is designed to facilitate the visibility of evidence, while explaining its origin and significance. It involves revealing hidden and obscured information and the relevant documentation.

- **Analysis**: This looks at the product of the examination for its significance and probative value to the case.

Reporting: This entails writing a report outlining the examination process and pertinent data recovered from the overall investigation.

here. Write the body of the paper here. Write the body of the paper here. Write the body of the paper here.

2.2 The Abstract Digital Forensic Model [5]

The Abstract Digital Forensics model proposes a standardized digital forensics process that consists of nine components:

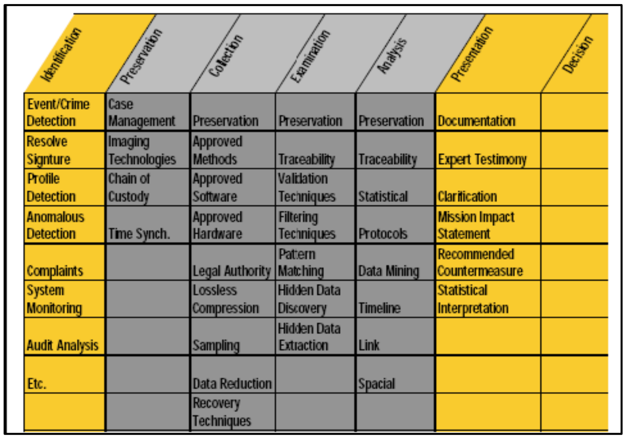
1. **Identification:** which recognizes an incident from indicators and determines its type.
2. **Preparation:** which entails the preparation of tools, techniques, search warrants, and monitoring authorizations and management support.

3. **Approach strategy**: that develops a procedure to use in order to maximize the collection of untainted evidence while minimizing the impact to the victim.
4. **Preservation:** which involves the isolation, securing and preservation of the state of physical and digital evidence.
5. **Collection:** that entails the recording of the physical scene and duplicate digital evidence using standardized and accepted procedures.
6. **Examination:** which involves an in-depth systematic search of evidence relating to the suspected crime.
7. **Analysis:** which involves determination of the significance, reconstructing fragments of data and drawing conclusions based on evidence found.
8. **Presentation:** that involves the summary and explanation of conclusions.
9. **Returning evidence:** that ensures physical and digital property is returned to proper owner.

2.3 Digital Forensic Research Workshop 2001[6]

At the first Digital Forensic Research Workshop held in Utica, NY in 2001, the group created a consensus document which outlined the state of digital forensics at that time. Among their conclusions was that digital forensics was a process with some reasonably agreed upon steps

.



Identification	Preservation	Collection	Examination	Analysis	Presentation	Decision
Event/Crime Detection	Case Management	Preservation	Preservation	Preservation	Documentation	
Resolve Signture	Imaging Technologies	Approved Methods	Traceability	Traceability	Expert Testimony	
Profile Detection	Chain of Custody	Approved Software	Validation Techniques	Statistical	Clarification	
Anomalous Detection	Time Synch.	Approved Hardware	Filtering Techniques	Protocols	Mission Impact Statement	
Complaints		Legal Authority	Pattern Matching	Data Mining	Recommended Countermeasure	
System Monitoring		Lossless Compression	Hidden Data Discovery	Timeline	Statistical Interpretation	
Audit Analysis		Sampling	Hidden Data Extraction	Link		
Etc.		Data Reduction		Spacial		
		Recovery Techniques				

FIGURE 1: DFRW Model

2.3 The Integrated Digital Investigation Model(IDIP)

Brian Carrier and Eugene Spafford [7] proposed yet another model that organizes the process into five groups consisting all in all 17 phases.

2.3.1 Readiness phases

The goal of this phase is to ensure that the operations and infrastructure are able to fully support an investigation. It includes two phases:

- **Operations Readiness phase**
- **Infrastructure readiness phase**

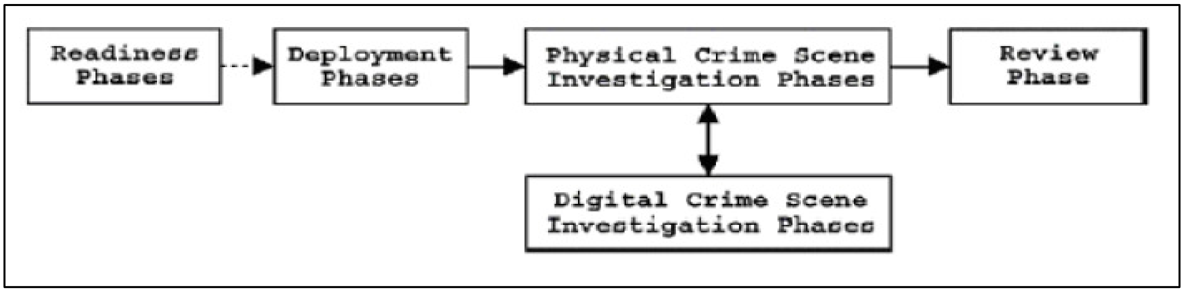

Readiness Phases
Deployment Phases
Physical Crime Scene Investigation Phases
Review Phase
Digital Crime Scene Investigation Phases

FIGURE 2: Phases of the IDIP Model

2.3.2 Deployment phases

The purpose is to provide a mechanism for an incident to be detected and confirmed. It includes two phases:

1. Detection and Notification phase; where the incident is detected and then appropriate people notified.
2. Confirmation and Authorization phase; which confirms the incident and obtains authorization for legal approval to carry out a search warrant.

2.3.3 Physical Crime Scene Investigation phases

The goal of these phases is to collect and analyze the physical evidence and reconstruct the actions that took place during the incident. It includes six phases:-

1. Preservation phase; which seeks to preserve the crime scene so that evidence can be later identified and collected by personnel trained in digital evidence identification.
2. Survey phase; that requires an investigator to walk through the physical crime scene and identify pieces of physical evidence.
3. Documentation phase; which involves taking photographs, sketches, and videos of the crime scene and the physical evidence. The goal is to capture as much information as possible so that the layout and important details of the crime scene are preserved and recorded.
4. Search and collection phase; that entails an in-depth search and collection of the scene is performed so that additional physical evidence is identified and hence paving way for a digital crime investigation to begin.
5. Reconstruction phase; which involves organizing the results from the analysis done and using them to develop a theory for the incident.
6. Presentation phase; that presents the physical and digital evidence to a court or corporate management.

2.3.4 Digital Crime Scene Investigation phases

The goal is to collect and analyze the digital evidence that was obtained from the physical investigation phase and through any other future means. It includes similar phases as the Physical Investigation phases, although the primary focus is on the digital evidence. The six phases are:-

1. Preservation phase; which preserves the digital crime scene so that evidence can later be synchronized and analyzed for further evidence.
2. Survey phase; whereby the investigator transfers the relevant data from a venue out of physical or administrative control of the investigator to a controlled location.
3. Documentation phase; which involves properly documenting the digital evidence when it is found. This information is helpful in the presentation phase.
4. Search and collection phase; whereby an in-depth analysis of the digital evidence is performed. Software tools are used to reveal hidden, deleted, swapped and corrupted files that were used including the dates, duration, log file etc. Low-level time lining is performed to trace a user’s activities and identity.

5. Reconstruction phase; which includes putting the pieces of a digital puzzle together, and developing investigative hypotheses.
6. Presentation phase; that involves presenting the digital evidence that was found to the physical investigative team.

3. The Need For Digital Forensic Investigation Models

It is important to understand the need of the “Digital Forensic Investigation Model” which is currently an active area of research in the academic world, which aims to ameliorate procedures followed in this field. The way Digital Forensic Science is implemented has a direct impact on

- The prevention of further malicious events occurring against the intended “target".
- The successful tracing back of the events that occurred which led to the crime, and determining the guilty parties involved.
- Bringing the perpetrators of the crime to justice.
- The improvement of current prevention mechanisms in place to prevent such an event from occurring again.
- Improving standards used by corporate security professionals to secure their respective corporate networks.
- How everyone “plugged" into this digital environment can increase their awareness about current vulnerabilities and prevention measures.

There has been a need for a standard methodology used for all Digital Forensics investigations. There have been many initiatives made to have models that have a general process to be followed for such investigations [8]. Research done by the scientific community has been fairly recent, and has concentrated mostly upon coming up with good models that can be practiced [9]. Yet, it can be safely said that these models are mainly ad-hoc and much needs to be accomplished in this particular domain.

4. KEY CHALLENGES

At the 2006 DFRWS conference, the keynote speech, “Challenges in Digital Forensics” was delivered by Ted Lindsey a computer scientist at the FBI [9]. In his speech, a number of the challenges were identified.
These are presented in Table 1.

Device diversity	Volume of evidence
Video and rich media	Whole drive encryption
Wireless	Anti-forensics
Virtualization	Live response
Distributed evidence	Usability & visualization

TABLE 1: Challenges in digital forensics - DFRWS 2006 keynote

These challenges as enumerated by Lindsey at DFRWS 2006 are a mix of: new technologies (e.g. wireless, whole drive encryption), situational technology trends (e.g. device diversity, volume of evidence, distributed evidence), and techniques (e.g. Live response, usability & visualization).
In 2005, the following list of challenges was presented by Mohay [10]:

- Education & certification
- Embedded systems
- Corporate governance and forensic readiness
- Monitoring the internet
- Tools
- Data volumes

In 2005 and 2004, Casey summarized the key challenges as:

- Counter forensics
- Networked evidence

- Keeping pace with technology
- Tool testing
- Adapting to shifts in law
- Developing standards and certification [11, 12]

5. Proposed Work: Systematic Digital Forensic Investigation Model (SRDFIM)

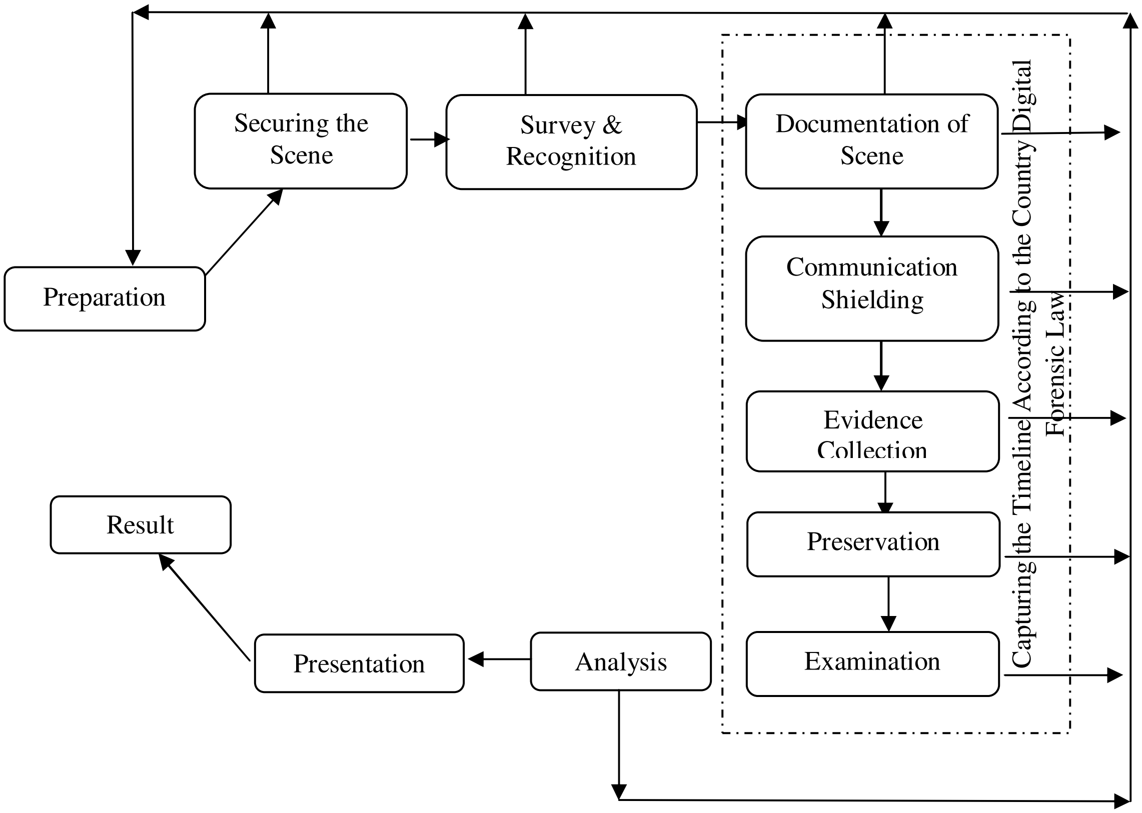


FIGURE2: Phases of Systematic Digital Forensic Investigation Model (SRDFIM)

5.1 Phase One - Preparation

The preparation phase occurs prior to the actual investigation. This involves getting an initial understanding of the nature of the crime and activities, prepare accumulating materials for packing evidence sources etc. It is very important to obtain the best possible assessment of the circumstances relating to the crime, prior to proceeding to the crime scene. A critical issue in the investigations involving digital devices is that the power runs out before evidence collection is over. The investigation should follow the various legal constraints and jurisdictional as well as organizational restrictions. This stage also involves obtaining search warrants, support from the management, required authorizations etc. before proceeding to the crime scene. The privacy rights of suspects should be taken into account. Legal notice must be provided to all concerned parties notifying about the forensic investigation. An appropriate strategy for investigation should be developed, having taken into account the nature of the incident and various technical, legal and business factors. Having a thorough preparation phase increases the quality of evidence and minimizes the risks and threats associated with an investigation.

5.2 Phase Two - Securing the Scene

This stage primarily deals with securing the crime scene from unauthorized access and preserving the evidence from being contaminated. There should be a formal protocol for handing over a crime scene in order to ensure that the chain of custody is properly followed. It will be difficult to judge how much at the crime scene actually the evidence is? The investigators should identify the scope of the crime and establish a perimeter. Ensuring the safety of all people at the scene and protecting the integrity of all evidence should also be the targets at this stage. The investigators should have absolute control of the scene and interference from unwanted people should be avoided. As the number of people at the crime scene increases, the possibilities for the contamination and destruction of evidence also increase. The crime scene investigation should follow Association of Chief Police Officers (ACPO), in conjunction with the National Hi-Tech Crime Unit (NHCTU) [13] guideline for securing the scene. Top priority should be given at this stage in minimizing the corruption of evidence. Any item that could be of evidence should not be tampered with. This phase plays a major role in the overall investigative process as it determines the quality of evidence.

5.3 Phase Three – Survey and Recognition

This stage involves an initial survey conducted by the investigators for evaluating the scene, identifying potential sources of evidence and formulating an appropriate search plan. In a complex environment, this may not be straightforward. In the case of Windows mobile devices, the major sources of evidence other than the device itself are the power adaptor, cradle, external memory cards, cables and other accessories. Since the information present in these devices can be easily synchronized with computers, any personal computer or laptop at the crime scene may also contain evidence. Evaluate the electronic equipments at the scene to determine whether any expert assistance is required in processing the scene. Identifying people in the scene and conducting preliminary interviews are extremely important. The owners or users of the electronic devices or system administrators can provide valuable information like the purpose of the system, security schemes, various applications present in the devices, user names, passwords, encryption details etc. Without violating the jurisdictional laws and corporate policies, the investigators must try to obtain the maximum information from the various people present in the scene. If it becomes necessary to search for items that are not included in the search warrant, appropriate amendments must be made to the existing warrant or a new warrant must be obtained, which includes the additional items. An initial plan for collecting and analyzing evidence must be developed at the end of the survey and recognition phase.

5.4 Phase Four - Documenting the Scene

This stage involves proper documentation of the crime scene along with photographing, sketching and crime-scene mapping. All the electronic devices at the scene must be photographed along with the power adaptors, cables, cradles and other accessories. If the digital or mobile device is in the on state, what is appearing on the screen should also be documented. A record of all visible data must be created, which helps in recreating the scene and reviewing it any time. This is particularly important when the forensic specialist has to do a testimony in a court, which could be several months after the investigation. Circumstances surrounding the incident, including those who reported the incident initially and at what date and time, should be included. It is necessary to keep a log of those who were present on the scene, those who arrived, those who left etc., along with the summary of their activities while they were at the scene. It is necessary to classify the people into separate groups like victims, suspects, bystanders, witnesses, other assisting personnel etc. and record their location at the time of entry. Documentation is a continuous loop back activity, required in all the stages of the investigation and required for maintaining proper chain of custody.

5.5 Phase five - Communication Shielding

This step occurs prior to evidence collection. At this stage, all further possible communication options of the devices should be blocked. Even if the device appears to be in off state, some communication features like wireless or Bluetooth may be enabled. This may result in overwriting the existing information and hence such possibilities should be avoided. In other situations where the device is in the cradle connected to a computer, synchronization mechanisms using ActiveSync might be enabled. This may also lead to the corruption of evidence. The best option after seizing a device is to isolate it by disabling all its communication capabilities. If the device is in the cradle, remove any USB or serial cable, which connects it to a computer.

5.6 Phase Six - Evidence Collection

Evidence collection of the digital or mobile devices is an important step and required a proper procedure or guideline to make them work. We can categorize evidence collection of the digital devices into two categories:

- Volatile Evidence Collection
- Non-Volatile Evidence Collection
-

5.6.1 Volatile Evidence Collection

Majority of the evidence involving mobile devices will be of volatile nature, being present in ROM. Collecting volatile evidence presents a problem as the device state and memory contents may be changed. The decision whether to collect evidence at the crime scene or later at a secured forensic workshop depends on the nature of the particular situation including the current power state. If the device is running out of battery power, the entire information will be lost soon. In that case, adequate power needs to be maintained if possible by using the power adaptor or replacing batteries. If maintaining the battery power seems doubtful, the contents of the memory should be imaged using appropriate tools as quickly as possible. A combination of tools must be used to obtain better results. If possible, an adequate power supply must be maintained by recharging the device or replacing the battery, whichever is appropriate. If it is not possible to provide sufficient power, the device must be switched off to preserve battery life and the contents of the memory. The presence of any malicious software installed by the user should also be checked at this stage.

5.6.2 Non-volatile Evidence Collection

This phase involves collecting evidence from external storage media supported by these devices, like MMC cards, compact flash (CF) cards, memory sticks, secure digital (SD) cards, USB memory sticks etc. Evidence from computers, which are synchronized with these devices, must be collected. Appropriate forensic tools must be used for collecting evidence to ensure its admissibility in a court of law. The integrity and authenticity of the evidence collected should be ensured through mechanisms like hashing, write protection etc. All power cables, adaptors, cradle and other accessories should also be collected. Care should be also taken to look for evidence of non-electronic nature, like written passwords, hardware and software manuals and related documents, computer printouts etc.

5.7 Phase Seven: Preservation

This phase includes packaging, transportation and storage. Appropriate procedures should be followed and documented to ensure that the electronic evidence collected is not altered or destroyed. All potential sources of evidence should be identified and labeled properly before packing. Use of ordinary plastic bags may cause static electricity. Hence anti-static packaging of evidence is essential. The device and accessories should be put in an envelope and sealed before placing it in the evidence bag. The evidence bag must be kept in a radio frequency isolation container to avoid further communications with any other device. All the containers holding these evidence bags must also be properly labeled. Adequate precautions are necessary as the sources of evidence could be easily damaged while transportation because of shock, excessive pressure, humidity or temperature. Afterwards the device can be moved to a secure location where a proper chain of custody can be maintained and examination and processing of evidence can be started. The evidence should be stored in a secure area and should be protected from electromagnetic radiations, dust, heat and moisture. Unauthorized people should not have access to the storage area. ***National Institute of Standards and Technology*** guideline highlights the need of proper transportation and storage procedures, for maintaining a proper chain of custody.

5.8 Phase Eight: Examination

This phase involves examining the contents of the collected evidence by forensic specialists and extracting information, which is critical for proving the case. Appropriate number of evidence back-ups must be created before proceeding to examination. This phase aims at making the evidence visible, while explaining its originality and significance. Huge volumes of data collected during the volatile and non-volatile collection phases need to be converted into a manageable size and form for future analysis. Data filtering, validation, pattern matching and searching for particular keywords with regard to the nature of the crime or suspicious incident, recovering relevant ASCII as well as non- ASCII data etc. are some of the major steps performed during this phase. Personal organizer information data like address book, appointments, calendar, scheduler etc, text messages, voice messages, documents and emails are some of the common sources of evidence, which are to be examined in detail. Finding evidence for system tampering, data hiding or deleting utilities, unauthorized system modifications etc. should also be performed. Detecting and recovering hidden or obscured information is a major tedious task involved. Data should be searched thoroughly for recovering passwords, finding unusual hidden files or directories, file extension and signature mismatches etc. The capabilities of the forensic tools used by the examiner play an important part in the examination phase. When the evidence is checked-out for examination and checked-in, the date, time, name of investigator and other details must be documented. It is required to prove that the evidence has not been altered after being possessed by the forensic specialist and hence hashing techniques like md5 must be used for mathematical authentication of data.

5.9 Phase Nine: Analysis

This step is more of a technical review conducted by the investigative team on the basis of the results of the examination of the evidence. Identifying relationships between fragments of data, analyzing hidden data, determining the significance of the information obtained from the examination phase, reconstructing the event data, based on the extracted data and arriving at proper conclusions etc. are some of the activities to be performed at this stage. ***The National Institute of Justice(2004)*** guidelines recommend timeframe analysis, hidden data analysis, application analysis and file analysis of the extracted data. Results of the analysis phase may indicate the need for additional steps in the extraction and analysis processes. It must be determined whether the chain of evidence and timeline of the events are consistent. Using a combination of tools for analysis will yield better results. The results of analysis should be completely and accurately documented.

5.10 Phase Ten: Presentation

After extracting and analyzing the evidence collected, the results may need to be presented before a wide variety of audience including law enforcement officials, technical experts, legal experts, corporate management etc. Depending on the nature of the incident or crime, the findings must be presented in a court of law, if it is a police investigation or before appropriate corporate management, if it is an internal company investigation. As a result of this phase, it should be possible to confirm or discard the allegations regarding the particular crime or suspicious incident. The individual results of each of the previous phases may not be sufficient to arrive at a proper conclusion about the crime. The results of examination and analysis must be reviewed in their entirety to get a complete picture. A report consisting of a detailed summary of the various steps in the process of investigation and the conclusions reached must be provided. In many cases, the forensic specialist may have to give an expert testimony in court. The complex terms involved in various stages of investigation process needs to be explained in layman’s terminology. The expertise and knowledge of the forensic examiner, the methodology adopted, tools and techniques used etc. are all likely to be challenged before a jury. Along with the report, supporting materials like copies of digital evidence, chain of custody document, printouts of various items of evidence etc. should also be submitted.

5.11 Phase Eleven - Result & Review

The final stage in the model is the review phase. This involves reviewing all the steps in the investigation and identifying areas of improvement. As part of the review phase, the results and their subsequent interpretation can be used for further refining the gathering, examination and analysis of evidence in future investigations. In many cases, much iteration of examination and analysis phases are required to get the total picture of an incident or crime. This information will also help to establish better policies and procedures in place in future.

6. Comparison With Existing Models

Table below gives a comparison of the activities in the proposed model with those in the major existing models described in the previous chapter. Some of the relevant activities in other models are incorporated in the proposed model. However there are many activities like communication shielding and bifurcation of evidence collection, which are unique for this model, as it is clear from the table.

ital Forensic odel	NIJ Law Enforcement Model	DRFWS Model	Abstract Digital Forensic Model	IDIP Model
			✓	✓
ene		✓		✓
gnition		✓	✓	✓
of Scene				✓
Shielding				
ce Collection				
idence Collection	✓	✓	✓	✓
		✓	✓	✓
	✓	✓	✓	✓
	✓	✓	✓	
	✓	✓	✓	✓
v				✓

TABLE 2: Mapping of Major Forensic Models to the Proposed Model

There may not always be a one-to-one mapping between the activities in the proposed model and other previous models. In some cases, though the process is similar, the terms used in other existing forensic models may differ. Table 2 gives a comparison of terminology used for different processes in the proposed model and various other models discussed in the previously.

NIJ Law Enforcement Model	DRFWS Model	Abstract Digital Forensic Model	D
--	--	Preparation	
--	Preservation	--	
--	Identification	Identification	
--	--	--	
--	--	--	
--	--	--	D
--	--	--	
--	--	--	
Collection	Collection	Collection	
--	Preservation	Preservation	
Examination	Examination	Examination	R
Analysis	Analysis	Analysis	
Reporting	Presentation	Presentation	
--	--	--	

TABLE 3: Mapping of Major Forensic Models to the Proposed Model

CONCLUSION

Motivated by the rapid increase in computer frauds and cyber crimes, this research work took the challenge to explore some of the open issues of digital forensic research. This paper starts with the discussion digital forensic technology then the discussion moves on to digital forensic investigation models. Some of the open problems of digital forensic research have been identified.

Then the proposed work provides Systematic Digital Forensic Investigation Model which is very use-full variety of digital forensic investigation.
The benefits of work are as follows:

- This will help in evidence dynamics and reconstruction of events by realizing the properties of Individuality, Repeatability, Reliability, Performance, Testability, Scalability, Quality and Standards in analysis of computer frauds and cyber crimes (CFCC).
- It will serve as benchmark and reference points for investigating cases of computer frauds and cyber crimes.
- It will help in the development of generalized solutions, which can cater to the need of rapidly changing and highly volatile digital technological scenario.
- The integrity and admissibility of digital evidence can be attained.

FUTURE SCOPE

In this study, work has been done in development of Systematic Digital Forensic Investigation Model. Following are few pointers for direction of future scope of research in these areas:

1. Application of the new model in variety of cases and improvement in light of feedback.
2. Identification of new constraints in terms of technological advancement will require model to be updated with time.

REFERENCES

1. Michael Noblett, Mark.M.Pollitt and Lawrence Presley. (2000) Recovering and Examining Computer Forensic Evidence, Forensic Science Communications, Volume 2, Number 4.

2. Gary L Palmer.(2001). A Road Map for Digital Forensic Research. Technical Report DTR-T0010-01, DFRWS. Report for the First Digital Forensic Research Workshop (DFRWS).

3. Kruse II, Warren and Jay, G. Heiser (2002) Computer Forensics: Incident Response Essentials. Addison-Wesley.

4. National Institute of Justice. (July 2001) Electronic Crime Scene Investigation. A Guide for First Responders.
Available from: http://www.ncjrs.org/pdffiles1/nij/187736.pdf.

5. Mark Reith, Clint Carr and Gregg Gunsch.(2002)An Examination of Digital Forensic Models International Journal of Digital Evidence, Fall 2002,Volume 1, Issue 3.

6. Digital Forensic Research Workshop (DFRWS) Research Road Map, Utica, NY. (2001) http://www.dfrws.org/archive.html

7. Brian Carrier and Eugene H Spafford,(2003) Getting Physical with the Investigative Process International Journal of Digital Evidence.Fall 2003,Volume 2, Issue 2.

8. M. M. Pollitt. An ad hoc review of digital forensic models. In Systematic Approaches to Digital Forensic Engineering, 2007, pages 43{54. University of Central Florida, USA, IEEE, April 10-12, 2007 2007.

9. Lindsey, T. Challenges in Digital Forensics. 2006
Available from: http://www.dfrws.org/2006/proceedings/Lindsey-pres.pdf.

10. Toward Models for Forensic Analysis, Sean Peisert, Matt Bishop, Sidney Karin, Keith Marzullo.Mohay, G. Technical Challenges and Directions for Digital Forensics. in 1st International Workshop on Systematic Approaches to Digital Forensic Engineering,. 2005.

11. Casey, E., State of the field: growth, growth, growth. Digital Investigation, 2004.

12. Casey, E., Digital arms race, The need for speed. Digital Investigation, 2005.

13. ACPO. Good Practise Guide for Computer based Electronic Evidence. 2006 Available from: http://www.acpo.police.uk/asp/policies/Data/gpg_computer_based_evidence_v3.pdf.

Secure E-Commerce Protocol

Khalid Haseeb khalid.haseeb@icp.edu.pk
Lecturer
Department of Computer Science
Islamia College University
Peshawar, 25000, Pakistan

Dr.Muhammad Arshad Muhammad.arshad@icp.edu.pk
Assistant Professor
Department of Computer Science
Islamia College University
Peshawar, 25000, Pakistan

Shoukat Ali shoonikhan@yahoo.com
Lecturer
F.G Degree College
Peshawar Cantt, 25000, Pakistan

Dr.Shazia Yasin shazia.khalid@icp.edu.pk
Associate Professor
Department of Physics
Islamia College University
Peshawar, 25000, Pakistan

Abstract

E-commerce has presented a new way of doing business all over the world using internet. Organizations have changed their way of doing business from a traditional approach to embrace e-commerce processes. As individuals and businesses increase information sharing, a concern regarding the exchange of money securely and conveniently over the internet increases. Therefore, security is a necessity in an e-commerce transaction. The purpose of this paper is to present a token based Secure E-commerce Protocol. The purpose of this paper is to present a paradigm that is capable of satisfying security objectives by using token based security mechanism.

Keywords: Trusted Third Party (TTP), Pretty Good Privacy (PGP), Secure Socket layer (SSL), Secure Electronic Transaction (SET).

1. INTRODUCTION

E-commerce refers to a wide range of online business activities for products and services. Security is the basic need to secure information on internet [1]. It also pertains to any form of business transaction in which the parties interact electronically rather than by physical exchanges or direct physical contact. A security objective is the contribution to security that a system or a product is intended to achieve. E-commerce has become a dynamic force, changing all kinds of business operations world-wide. E-commerce is conducted on global network i.e. Internet which is untrusted. So confidentiality is required during transmission and it must be kept secure against all type of threats The related concepts and business practices not only influence communications, the routines of daily life and personal relationships, they represent opportunities for initiating new international and domestic business ventures. However, as the Cyber is used increasingly as a platform for e-commerce transactions, security becomes a primary issue for Internet applications. Security has emerged as an increasingly important issue in the development of an e-commerce organization. The eradication of trust in e-commerce applications may cause prudent business operators and clients to forego the use of the Internet for now and revert back to traditional methods of doing business. Gaining access to sensitive information and replay are some common threats that hackers impose to E-commerce systems [2].

The successful functioning of E-commerce security depends on a complex interrelationship between several applications development platforms, database management systems, systems software and network infrastructure [3] . By doing online business, it is a facility of reaching to everyone. Exploring the opportunities challenges conventional notions of business competition through electronic flows of information and money [6]. Payment on Internet or network is a critical important chain of whole e-commerce, which contains the payment activity [4]. Security protection starts with the preservation of the confidentiality, integrity and availability of data and computer resources [5]. These three tenets of information security are sometimes represented in the Confidentiality, Integrity and Authentication Triad in the Figure 1.

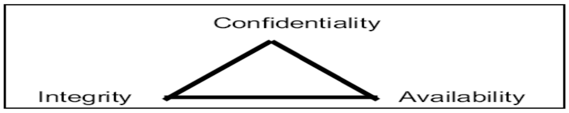


FIGURE 1: The Confidentiality, Integrity and Authentication Triad.

Including the elements of the Confidentiality, Integrity and Authentication Triad, the six security needs in E-commerce are:

i. Access Control.
ii. Privacy/Confidentiality.
iii. Authentication.
iv. Non Repudiation.
v. Integrity.
vi. Availability.

Access control ensures only those that legitimately require access to resources are given access [3].

Confidentiality is concerned with warranting that data is only revealed to parties who have a legitimate need, while privacy ensures that customers' personal data collected from their electronic transactions are protected from indecent and/or unauthorized disclosure [6]. Issues related to privacy can be considered as a subset of issues related to access control.

Authentication provides for a sender and a receiver of information to validate each other as the appropriate entity. This means having the capability to determine who sent the message and from where and which machine.

Non-repudiation is a property of the transaction that positively confirms that a particular client did indeed request the transaction in question without having the ability to deny making the request [4].

Integrity ensures that if the context of a message is altered, the receiver can detect it. It is possible that as a file, electronic mail, or data is transmitted from one location to another, its integrity may be compromised.

Availability as defined in an information security context ensures that access data or computing resources needed by the appropriate personnel are both reliable and available in a timely manner.

2. RELATED WORK

Several research papers have been presented discussing security aspects in E-commerce. E-commerce software packages should also work with Secure Electronic Transfer (SET) or Secure Socket Layer (SSL) technologies for encryption of data transmissions. (SSL) protocols, which allow for the transmission of encrypted data across the Internet by running above the traditional TCP/IP protocols. SSL protects the communication between a client and a server and provides authentication to both parties to secure communication. SSL provides point to point security. Storage of sensitive data in repositories or databases makes e-commerce system ideal target [7]. Hackers seem any target to data repositories due to availability of data on a single place. E-commerce has become a critical component in any business competitive strategy. Organizations are gaining opportunities and benefits such as global presence and improved competitiveness from web-based e-commerce. Algorithm provides the capability to generate and verify signatures. Signature generation makes use of a private key to generate a digital signature [8].

SSL allows many key exchange algorithms, but some algorithms such as Diffie-Hellman key exchange have no certificate concept [9].

3. PROBLEM DEFINITION

PGP has been considered to provide security to E-commerce [10]. But it is not a full proof solution because PGP is specifically used for E-mail security which can provide Authentication and Confidentiality, which are enough for E-mail security but not for E-commerce security. PGP can not deal with Reply and Man in the Middle security threats against E-commerce transaction. Figure 2 depicts only Authentication and Confidentiality to provide E-commerce security which are not enough.

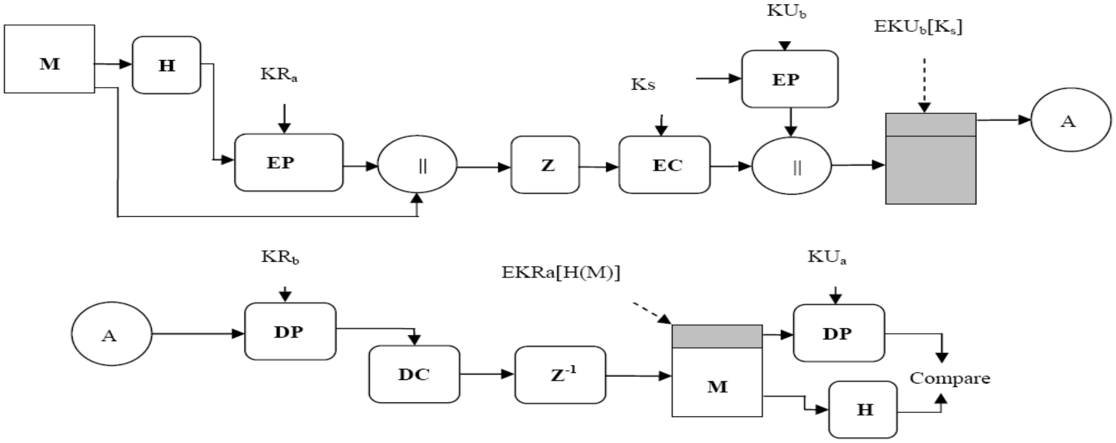


FIGURE 2: PGP Based E-commerce Cryptography [10]

Analyzing threats is difficult and time consuming but secure approach cannot be build without understanding the threats that can occur during communication and we cannot determine the appropriate technology for taking counter measures against these threats. We encounter those threats in the following categories that can break E-commerce security

i. Information disclosure threat
ii. Data Tampering threat
iii. Repudiation threat
iv. Replay threat
v. Man in the middle threat

The following table shows the security comparison of different E-commerce Security protocols.

E-commerce Protocols	Confidentiality	Non Repudiation	Integrity	Replay Attack	Man in the middle Attack
SSL	Yes	No	Yes	No	No
PGP	Yes	No	Yes	No	No
SET	Yes	No	Yes	No	No

TABLE 1: Security comparison of E-commerce protocols

To provide strong security framework, security requirements must kept in mind. Authentication, confidentiality and integrity are the main security objectives. For web and Internet related applications non repudiation, Reply and man in the middle threats are other major security objectives.

4. PROPOSED SOLUTION

Before commencing an E-commerce transaction, both parties must be registered by a TTP. TTP will provide transaction tokens to both the parties involved for sending data. TTP can be beneficial in solving many disputes that can occur during transaction between two parties. When both parties will get transaction tokens then both parties can communicate with each other and SEP provides protection against security threats.

The steps performed by SEP (shown in Figure 3) are:

i. At first customer would have to request TTP for the issuance of token.
$E_{KU\ (TTP)}$ [ID_A, Req_A, Time, K_{UA}, N_A]

ii. TTP will decrypt the customer request using its private key and respond to customer with a token. The token will be encrypted using the TTP private key.
T_A=$E_{KR\ (TTP)}$ [ID_A, Req_A , Time, K_{UA}, N_A]

iii. Customer will send token to merchant
$T_A \rightarrow M$

iv. When merchant received customer token then merchant would have to request for an issuance of token to TTP.
$E_{KU\ (TTP)}$ [ID_B, Time, K_{UB}, N_B]

v. TTP provides a token to merchant and encrypted using private
T_B=$E_{KR\ (TTP)}$ [ID_B, Time, K_{UB}, N_B]

vi. Merchant will send token to customer

$T_B \rightarrow C$

Now both parties have an authentic token and can communicate to each other in secure manner.

vii. Customer encrypts its ID, time and nonce N_A (generated in token) using its private key. Again encrypts it along with the new nonce N_1 (generated by customer side) using public key of the merchant and sends it to the merchant.

$E_{ku\ (B)}\ [N_1,\ E_{KR\ (A)}\ [ID_A,\ Time,\ N_A]]$

viii. Merchant encrypts its ID, time and nonce N_B (generated in token) using its private key. Again encrypts it along with the new nonce N_2 (generated by Merchant side) using the public key of the customer

$E_{ku\ (A)}\ [N_2,\ E_{KR\ (B)}\ [ID_B,\ Time,\ N_B]]$

ix. Customer respond with the nonce N_2 (generated by merchant) send in step 8 encrypted using the public key of merchant

$E_{ku\ (B)}\ [E_{KR\ (A)}\ [N_2]]$

Using these steps customer and merchant shares a lot of information to each other for the purpose to recognize each other and to solve future disputes in E-commerce transaction. SEP completes E-commerce transaction in secure manner.

5. PROTECTION AGAINST SECURITY ATTACKS

This section provides Protection against attacks. Secure E-commerce Protocol (SEP) covers security aspects in E-commerce as discuss below.

Authentication

Customer sends ID, nonce and time that will sign by private key of customer and then encrypted the whole package by public key of Merchant (step 7).

Merchant decrypts the package with its private key. After Decrypt the Customer Package merchant will access Customer ID. As the package is sign by private key of customer. So in way Merchant can determine that customer is Authentic

Non-Repudiation

There are two possible way to perform Non-Repudiation in proposed solution:

a) As both the customer and Merchant get their tokens from TTP , which will contain their IDs, Nature of request , time of issuance of token, their respective public keys and a nonce (generated by the customer and Merchant respectively). The trusted third party will keep a copy of the original request for the token send by the customer and merchant (step 1 and step 4) and a copy of the transaction tokens issued to them (step 2 and step 5). Therefore Non-Repudiation problem can be solved using the TTP.

b) In step 7 and 8, both customer and Merchant send some information to each other. This information

contains a subpart encrypted by using their private keys.

$E_{KR\ (A)}\ [ID_A,\ Time,\ N_A]$

$E_{KR\ (B)}\ [ID_B,\ Time,\ N_B]$

SEP uses this information as evidence to resolving Non Repudiation Problem.

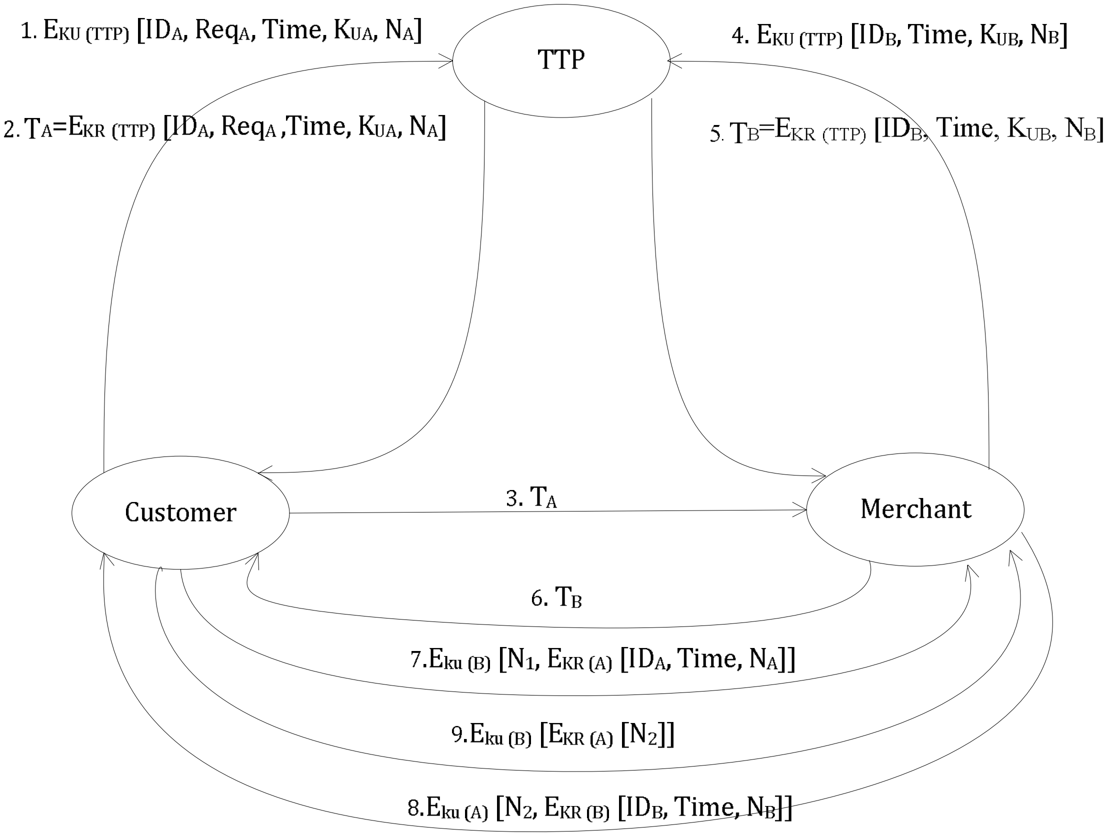

1. $E_{KU\ (TTP)}$ [ID_A, Req_A, Time, K_{UA}, N_A]
TTP
4. $E_{KU\ (TTP)}$ [ID_B, Time, K_{UB}, N_B]
2. T_A=$E_{KR\ (TTP)}$ [ID_A, Req_A ,Time, K_{UA}, N_A]
5. T_B=$E_{KR\ (TTP)}$ [ID_B, Time, K_{UB}, N_B]
Customer
3. T_A
Merchant
6. T_B
7.$E_{ku\ (B)}$ [N_1, $E_{KR\ (A)}$ [ID_A, Time, N_A]]
9.$E_{ku\ (B)}$ [$E_{KR\ (A)}$ [N_2]]
8.$E_{ku\ (A)}$ [N_2, $E_{KR\ (B)}$ [ID_B, Time, N_B]]

FIGURE 3: SEP Steps

Integrity

On the customer side the hash code is generated using SHA-1, which is then encrypted using the customer's private key. The encrypted hash code is combined with the original transaction message and sends towards merchant. The merchant side separates the hash code form the message, decrypts it using the customer's public key. At the same time, the merchant will also calculate the hash code of the received transaction message using the same SHA-1 algorithm. Transaction message will be received correctly if calculated hash code and decrypted hash code will be same.

Reply Attack

In case of key exchange a reply attack can take place, which is easily solved in the proposed solution. At first a reply attack can take place in step 1. The untrusted party can catch the token request send by the user and after some time reply it the trusted third party for getting a fake token. But as the token request contains ID, time and nonce, on this information trusted third party can easily figure out it as a replay attack and request generated by bad party will discard.

Man in the Middle Attack

The man in the middle attack works by involving three people in a communication session (server, client and third untrusted party).Third untrusted party sits between the client and the server on the network and analyzed traffic that from client to server and from server to client.

In proposed solution the trusted third party provides a token that contains ID, Public key, issuer name, Hash code, Nonce and token signed by trusted third private key. The client checks the token originality by checking the signature and name of the issuer.

6. IMPLEMENTATION

We have developed an algorithm to secure E-commerce transaction as discussed earlier. The algorithm is implemented by using the console application of .Net environment. The implementation process contains transactional entities. One is root entity second is customer entity and the third entity is merchant. Root entity act as an interface between other two entities. To achieve successful and protected communication root entity must be involved in transaction. The entities involved in transaction requests for authentic token through security mechanism SEP by using console environment to root entity .On other hand the root entity provides an authentic tokens to both transaction entities through SEP using console environment. The entities involved in transaction, requests for authentic token through security mechanism SEP by using console environment to root entity .On other hand the root entity provides an authentic tokens to both transaction entities through SEP security module using console environment.. To implement the proposed solution we used visual studio 2008 that runs on Microsoft operating system platform 64 bit computer. We used visual C# as a tool to implement proposed solution. Implementation is console based application designed to be used through text-only computer interface and used .Net framework 3.5 to provides a set of cryptographic objects, supporting hashing, encryption, and generating digital signatures. Figure 4 depicts the implementation process in detail.

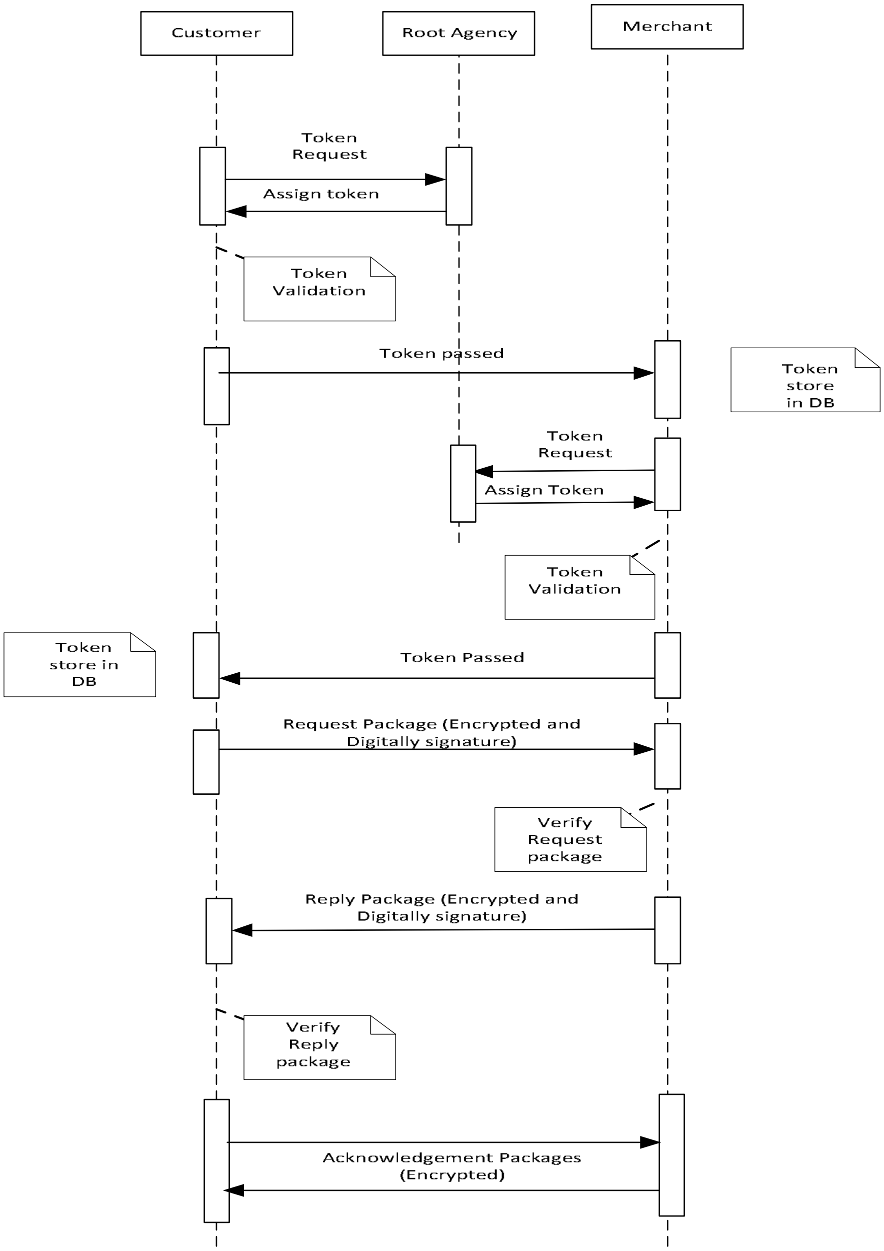
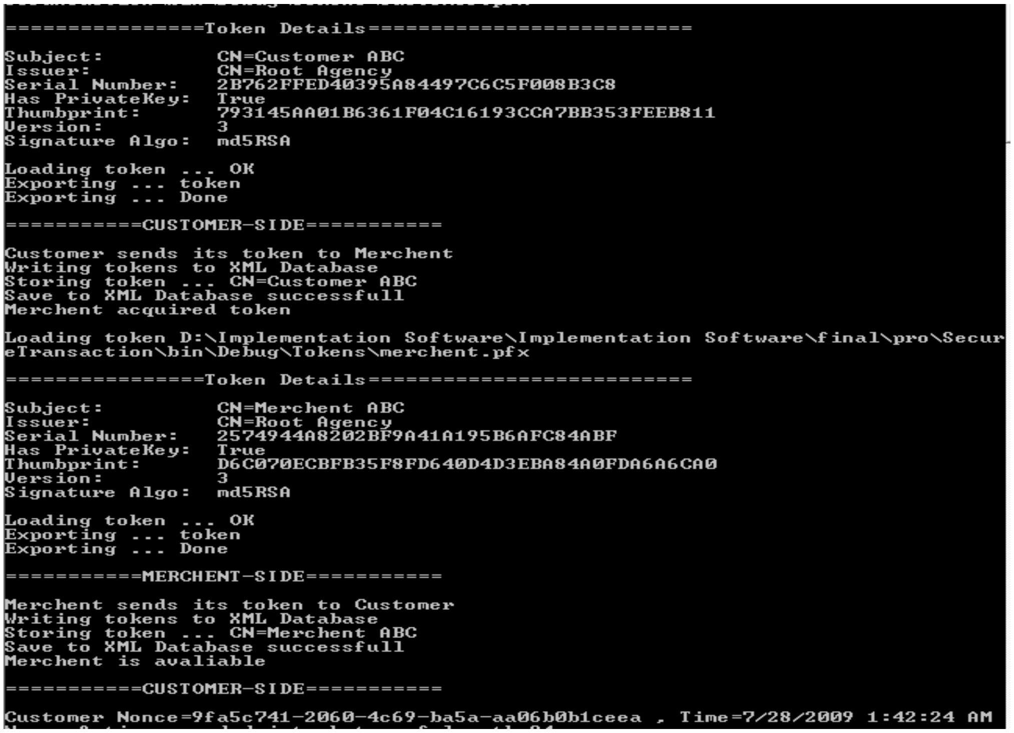


FIGURE 4: Implementation Sequence Diagram

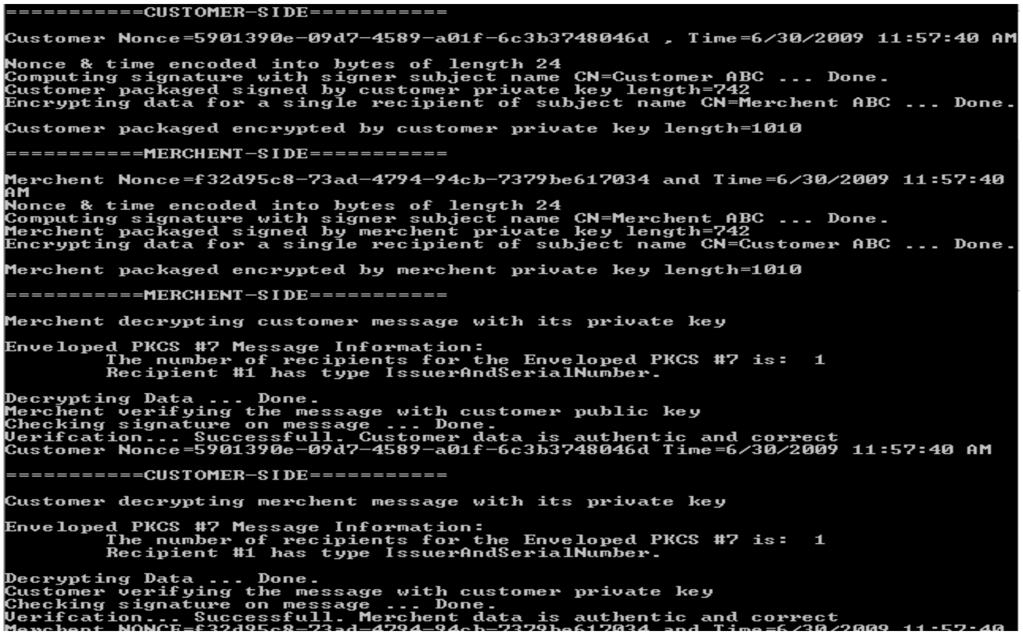
7. RESULTS

To secure transaction application generates tokens that are used by customer and merchant. Tokens have different attributes such as serial number, subject, hash code, issue name and public key. Customer and merchant first verify the authenticity of tokens and then perform communication in a secure domain shown in figure 5. Application encodes the package to transmit over the network and then decodes at receiving side to achieve original data. Application also provides authentication and integrity checks to customer and merchant packages to protect against threats shown in figure 6.



```
================Token Details========================

Subject:          CN=Customer ABC
Issuer:           CN=Root Agency
Serial Number:    2B762FFED40395A84497C6C5F008B3C8
Has PrivateKey:   True
Thumbprint:       793145AA01B6361F04C16193CCA7BB353FEEB811
Version:          3
Signature Algo:   md5RSA

Loading token ... OK
Exporting ... token
Exporting ... Done

===========CUSTOMER-SIDE===========

Customer sends its token to Merchent
Writing tokens to XML Database
Storing token ... CN=Customer ABC
Save to XML Database successfull
Merchent acquired token

Loading token D:\Implementation Software\Implementation Software\final\pro\Secur
eTransaction\bin\Debug\Tokens\merchent.pfx

================Token Details========================

Subject:          CN=Merchent ABC
Issuer:           CN=Root Agency
Serial Number:    2574944A8202BF9A41A195B6AFC84ABF
Has PrivateKey:   True
Thumbprint:       D6C070ECBFB35F8FD640D4D3EBA84A0FDA6A6CA0
Version:          3
Signature Algo:   md5RSA

Loading token ... OK
Exporting ... token
Exporting ... Done

===========MERCHENT-SIDE===========

Merchent sends its token to Customer
Writing tokens to XML Database
Storing token ... CN=Merchent ABC
Save to XML Database successfull
Merchent is avaliable

===========CUSTOMER-SIDE===========

Customer Nonce=9fa5c741-2060-4c69-ba5a-aa06b0b1ceea , Time=7/28/2009 1:42:24 AM
```

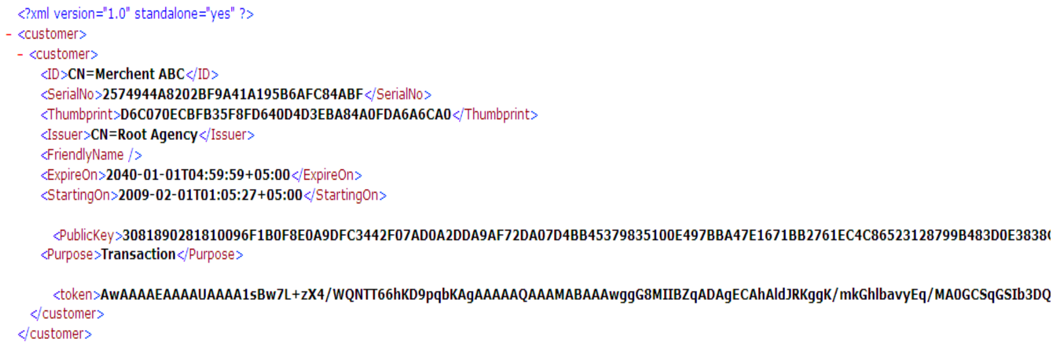
FIGURE 5: Tokens Generation and Exchanging between Transactional Entities



```
===========CUSTOMER-SIDE===========

Customer Nonce=5901390e-09d7-4589-a01f-6c3b3748046d , Time=6/30/2009 11:57:40 AM

Nonce & time encoded into bytes of length 24
Computing signature with signer subject name CN=Customer ABC ... Done.
Customer packaged signed by customer private key length=742
Encrypting data for a single recipient of subject name CN=Merchent ABC ... Done.

Customer packaged encrypted by customer private key length=1010

===========MERCHENT-SIDE===========

Merchent Nonce=f32d95c8-73ad-4794-94cb-7379be617034 and Time=6/30/2009 11:57:40
AM
Nonce & time encoded into bytes of length 24
Computing signature with signer subject name CN=Merchent ABC ... Done.
Merchent packaged signed by merchent private key length=742
Encrypting data for a single recipient of subject name CN=Customer ABC ... Done.

Merchent packaged encrypted by merchent private key length=1010

===========MERCHENT-SIDE===========

Merchent decrypting customer message with its private key

Enveloped PKCS #7 Message Information:
        The number of recipients for the Enveloped PKCS #7 is:  1
        Recipient #1 has type IssuerAndSerialNumber.

Decrypting Data ... Done.
Merchent verifying the message with customer public key
Checking signature on message ... Done.
Verifcation... Successfull. Customer data is authentic and correct
Customer Nonce=5901390e-09d7-4589-a01f-6c3b3748046d Time=6/30/2009 11:57:40 AM

===========CUSTOMER-SIDE===========

Customer decrypting merchent message with its private key

Enveloped PKCS #7 Message Information:
        The number of recipients for the Enveloped PKCS #7 is:  1
        Recipient #1 has type IssuerAndSerialNumber.

Decrypting Data ... Done.
Customer verifying the message with customer private key
Checking signature on message ... Done.
Verifcation... Successfull. Merchent data is authentic and correct
```

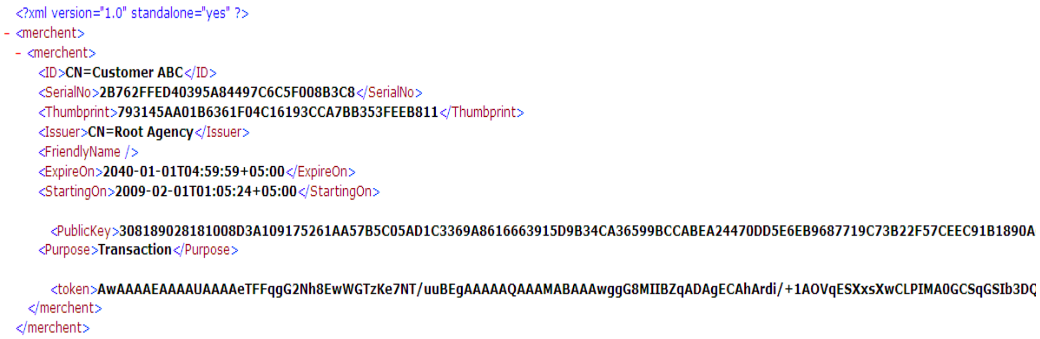
FIGURE 6: Encoding and Decoding Packages**.**

When customer and merchant exchange tokens to each other the application store both tokens in XML data files to eliminate non-repudiation problem in future shown in figure 7 and figure 8.



```
  <?xml version="1.0" standalone="yes" ?>
- <customer>
  - <customer>
      <ID>CN=Merchent ABC</ID>
      <SerialNo>2574944A8202BF9A41A195B6AFC84ABF</SerialNo>
      <Thumbprint>D6C070ECBFB35F8FD640D4D3EBA84A0FDA6A6CA0</Thumbprint>
      <Issuer>CN=Root Agency</Issuer>
      <FriendlyName />
      <ExpireOn>2040-01-01T04:59:59+05:00</ExpireOn>
      <StartingOn>2009-02-01T01:05:27+05:00</StartingOn>

        <PublicKey>3081890281810096F1B0F8E0A9DFC3442F07AD0A2DDA9AF72DA07D4BB45379835100E497BBA47E1671BB2761EC4C86523128799B483D0E3838
      <Purpose>Transaction</Purpose>

        <token>AwAAAAEAAAAUAAAA1sBw7L+zX4/WQNTT66hKD9pqbKAgAAAAAQAAAMABAAAwggG8MIIBZqADAgECAhAldJRKggK/mkGhlbavyEq/MA0GCSqGSIb3DQ
    </customer>
  </customer>
```

FIGURE 7: Customer XML file



```
  <?xml version="1.0" standalone="yes" ?>
- <merchent>
  - <merchent>
      <ID>CN=Customer ABC</ID>
      <SerialNo>2B762FFED40395A84497C6C5F008B3C8</SerialNo>
      <Thumbprint>793145AA01B6361F04C16193CCA7BB353FEEB811</Thumbprint>
      <Issuer>CN=Root Agency</Issuer>
      <FriendlyName />
      <ExpireOn>2040-01-01T04:59:59+05:00</ExpireOn>
      <StartingOn>2009-02-01T01:05:24+05:00</StartingOn>

        <PublicKey>308189028181008D3A109175261AA57B5C05AD1C3369A8616663915D9B34CA36599BCCABEA24470DD5E6EB9687719C73B22F57CEEC91B1890A
      <Purpose>Transaction</Purpose>

        <token>AwAAAAEAAAAUAAAAeTFFqgG2Nh8EwWGTzKe7NT/uuBEgAAAAAQAAAMABAAAwggG8MIIBZqADAgECAhArdi/+1AOVqESXxsXwCLPIMA0GCSqGSIb3DQ
    </merchent>
  </merchent>
```

FIGURE 8: Merchant XML file

8. CONCLUSION

There are many issues involved in securing E-commerce Transaction e.g. Privacy, Integrity Access Control, Confidentiality and Non Repudiation. These issues are still ongoing research problem. The Internet, which is the primary medium used for conducting E-commerce transactions, is not designed to handle transactions securely. In this paper an approach has been suggested, which covers Authentication, Integrity and Non Repudiation security objective in a secure manner. In this paper Secure E-commerce Protocol is proposed to provide protection against attacks. SEP presents security mechanism to increase the level of security objectives using simple cryptographic techniques.

9. REFERENCES

[1] William Stallings, “Cryptography and Network Security”, 3rd edition, Prentice Hall,2003

[2] D. Berlin, "Information Security Perspective on Intranet," presented at Internet and E-Commerce Infrastructure, 2007.

[3] S. R. S. KESH, AND S. NERUR, "A Framework for Analyzing E-Commerce Security," *Information Management and Computer Security*, vol. 10, no. 4, no. pp. 149-158.

[4] X.Sahi and P.C. Wright, “ E-Commercializing Business Operations” Communication of ACM, Feburary,2003 vol.46. no.2 page 83-87.

[5] C. BARNES, "Hack Proofing Your Wireless Networks," Syngress Publishing, Rockland, 2002.

[6] P. RATNASINGHAM, "Trust in Web-Based Electronic Commerce Security," *Information Management and Computer Security*, vol. 6, no. 4, no. pp. 162-166, 1998.

[7] Anup K. Ghosh “E-Commerce security: No Silver Bullet” IFIP Conference Proceedings; Vol. 142, P: 3 – 16, 1998

[8] P. C. O. A.J Menezes, and S.A. Vanstone, *Handbook of Applied Cryptography*: CRC Press, 1996.

[9] L. X. QIN Zhiguang, GAO Rong, "A survey of E-commerce Security," *Electronic Science and Technology of China* vol. 2, no. 3, Sept 2004.

[10] N. M. A. Al-Slamy, "E-Commerce Security," *IJCSNS International Journal of Computer Science and Network Security*, vol. 8, no. 5, May 2008.

[11] Dale Barr, “Public Key Infrastructure”, TECHNOLOGY AND PROGRAMS DIVISION Volume 11, Number 3, December 2004

[12] Cetin K. Koc, "Next Generation E-Commerce Security" Information Security Laboratory December 2, 1999

Diacritic Oriented Arabic Information Retrieval System

Khalid S. R. Aloufi koufi@taibahu.edu.sa
College of Computer Science and Engineering,
Taibah University,
Madinah, KSA

Abstract

Arabic language support in search engines and operating systems is improved in recent years. Searching in the Internet is reliable and can be compared to the excellent support for several other languages, including English. However, for text with diacritics there are some limitations. For this reason, most Information retrieval (IR) systems remove diacritics from text and ignore it for its complexity. Searching text with diacritics is important for some kinds of documents, such as those of religious books, some newspapers and children stories. This research shows the design and development of the system that overcome the problem. The proposed system considers diacritics. The proposed system includes the design complexity in the retrieving algorithm rather than the information repository, which is database in this study. Also, this study analyses the results and the performance. Results are promising and performance analysis shows methods to enhance design and increase the performance. The proposed system can be integrated in search engines, text editors and any information retrieval system that include Arabic text. Performance analysis of the proposed system shows that this system is reliable. The proposed system is applied on database of Hadeeth, which is religious book includes the prophet action and statements. The system can be applied in any kind of data repository.

Keywords: Search Engine, Information Retrieval Systems, Diacritics, Arabic Language, information Retrieval Performance Analysis

1. INTRODUCTION

In the early days of the Internet Arabic letters were not defined. However, when the Unicode standard becomes applicable in the Internet browsers and the hyper text markup language (HTML), several non Latin languages have been supported.

Arabic section in the Hex reference of the Unicode standardization that include characters, such as letters, symbols and diacritics Ranges from 0600 to 06FF [6].

The Arabic letters in Unicode range from 0621 to 063A and from 0641 to 064A [6]. The Arabic diacritics range from 0618 to 061A and from 064D to 0656 [6]. In Unicode, There are 36 Arabic letter and 11 diacritics.

Every spoken language has its own features that are applied in reading, writing, listening and speaking. Arabic language is root based language. Arabic language consists of 28 letters. Each letter is pronounced with different vowels depending on the diacritics used. Some of the 28 letters are written with different shapes depending of their order in the word. These features are important for information retrieval systems, either for sound processing or pattern recognition. This study develops an information retrieval methodology for Arabic language.

The features of the any spoken language increase the information find-ability when considered in those concerned information retrieval systems. Any language with diacritics can get applied by the result of this study. The language features is included in the information systems analysis and design to increase the retrieval reliability.

There are present difficulties for Arabic users in searching for information in the Internet using search engines [2]. The amount of information returned is far less than available.

Current search engines are failing to support non Latin languages in the same level of Latin language support [10]. The design of search engine philosophy considers the features of Latin languages but it is not working with non Latin languages such as Arabic [2].

There are different methodologies for AIRS. Methodologies can be classified in two categories. The first category makes no change to the text. The second category removes all diacritics from the text.

The second category cannot be used with text sources that require being with diacritics. Diacritics are important from some sources because changing diacritics for similar words might change the meaning. Usually, as mentioned earlier this is important for some text sources, such as religious and educational books for children.

Compared to the second category, the first category increases the complexity of database design and the retrieval algorithm. However, this requires further investigation and AIRS development. This study keeps the diacritics as in the original document as in the first category of the methodologies. The complexity of database design is out of the scope of this study. The database mainly is the repository of the information of Arabic text with diacritic. The main contribution of this research is to investigate the basic approach of retrieving diacritized text.

The methodology and approach of this study was not found to be applied by any study according to the knowledge of this research. However, several studies removed diacritics from text, which applied in information retrieval system of Quran [7] [1] [9] [10].

The paper is organized as follows. The next section describes the system model. Third section is the section for discussing the results. The paper finding and further research suggestions are summarized in the section Conclusion and Future work. This paper ends with the references used in this research.

2. THE SYSTEM MODEL

This section presents the Arabic information retrieval system (AIRS). This system uses the Database as the information repository. Database is one of the examples of data repositories used by search engines [11].

The SQL is the language that supports reading, writing and other functions with databases. However, SQL is found to not fully support non Latin languages, such as Arabic [4]. The SQL commands such as LIKE and regular expression command does not support diacritics and multi byte characters [4]. For this reason this study propose AIRS simplified model.

The system model consists of four processes, which are input processing, input terms, searching and result set.

Input processing is the process of defining the characters of word. The proposed model assumes single word without diacritics. Usually the user is expected to enter the word without diacritics. Input terms are the step of the definition of all the possible words with diacritics. Searching is the SQL query to search for all the words. Result set is the last process to return the group of records from the database.

The following algorithm shows the above processes:

Variables:

Term: entered by user

Generated terms: contains words that will be forwarded to the search engine.

The algorithm:

1. *User enters the Term.*
2. *Generate all possible Terms*
3. *Search for generated term*
4. *Return result set for all generated terms*
5. *finish*

Assuming the user will enter the word $x_1x_2x_{3,}$ the algorithm execute as follows:

1. User enters the term $x_1x_2x_3$.
2. The generated terms will be $x_1x_2x_3$,x_1-x_2x_3,x_1x_2-x_3 and x_1-x_2-x_3.
3. Search for all the generated terms in step 2
4. The result set is returned
5. finish

The user enters a word without diacritics to search for. The system generates all the possible words with diacritics using the simple collection generation as shown in the algorithm. Any "-"is counted if it is any diacritics only because the system uses regular expression. After that, the system in step 3 search for the generated words in the database. Step 4 will return the search match of any of the generated terms in one query result without any repetition of the records returned in the result set. Searching is a result set of the SQL query for all the generated terms. SQL query replaces any dash "-"with any character, mainly for diacritics.

The searching algorithm is developed using JAVA programming language [3]. The database is designed using MySQL [5]. The operating system used is Windows 7 Home premium. Processor if Intel ® Core™2 Do CPU P9300 @ 2.26GHz 2.27GHz and the Ram is 3.00 GB. System type is 64-bit Operating System.

This research is applied as information retrieval of database of Hadeeth. The information of the Hadeeth can be organized according to the section found in most Hadeeth books.

Each Hadeeth consists of Sanad and Matin. The Hadeeth book in this study is mukhtasar Saheeh Muslim [8].

The Hadeeth book is organized in chapters, sections and items. Each item is single Hadeeth. Each Chapter consists of several Sections and each section contains a group of Hadeeth. Chapter is called Book or Ketab in Arabic. Section is called Door or Bab in Arabic.

3. RESULTS AND PERFORMANCE ANALYSIS

The section presents the experiments results and performance analysis and applied improvement methods. Each experiment returns a number of generated words, the number of returned results and the time required.

Each experiment includes the generated words, the number of the results returned for this word, the time required to get the result set. Table 1 presents one experiment example.

Table 2 summarizes all the experiments performed on AIRS in this study. The table shows the word, the number of letter for each word, the number of generated words, the waiting time, number of words without results, number of words with results and the total number of returned results.

Word	Number of Results
رسول	3
ر_سول رس_ول رسو_ل ر_سو_ل رس_و_ل ر_س_و_ل	0
ر_س_ول	1768
Time	1553 *ms*

TABLE 1: search for the word رسول

The mathematical notations used in this study are as follows. The number of generated words is n_t. The waiting time is w_t. The total number of returned records is n_r.

Equation (1) computes the time required to get a result for all generated words which have no results, where x_{nwrt} is a constant; n_t is the total number of generated words. From the experiments, x_{nwrt} is found to be 38.7 *ms* for each word without returned result.

Computing the time required to get a record is performed by Equation (2), where x_{nwr} is a constant, n_r is the total number of returned records. From the experiments, x_{nwr} is found to be approximately 0.6 *ms*. The waiting time can be calculated as a function of the time required to search for a result of a word and the time requiered to get a result.

The total waiting time is computed using equation (3), where n_r is the total number of returned records and n_t is the total number of generated words.

$$t_{nwrt} \quad = x_{nwrt}.n_t, \text{ , where } x_{nwrt} = 38.7\ ms \qquad (1)$$

$$t_{nw} \quad = x_{nwr}.n_r \text{ , where } x_{nwr} = 0.6 \qquad (2)$$

$$w_t \quad = t_{nwr} + t_{nwrt} = x_{nwr} \cdot n_r + x_{nwrt} \cdot n_t = 0.6 \cdot n_r + 38.7 \cdot n_t \qquad (3)$$

Total number of records	Number of words with results	Number of words without results	Waiting Time	Number of Generated Words	Number of letters	Word
1771	2	6	1553	8	4	رسول
2073	3	1	982	4	3	قال
22	1	7	382	8	4	خالد
0	0	16	722	16	5	هريره
451	2	14	872	16	5	هريرة
0	0	64	2353	64	7	المدينه
94	1	63	3217	64	7	المدينة
0	0	64	2117	64	7	الاسلام
53	1	63	2221	64	7	الإسلام
0	0	64	2110	64	7	ألإسلام
0	0	64	2790	64	7	ألاسلام
349	2	2	488	4	3	أحد
120	3	1	256	4	3	احد
5	1	3	165	4	3	صلى
1	1	3	167	4	3	صلي
0	0	8	286	8	4	شجره
23	1	3	209	4	3	عجل
13	1	7	296	8	4	شجرة
3	1	15	524	16	5	قيامه
89	1	15	614	16	5	قيامة
55	1	7	318	8	4	خرجت
0	0	4	164	4	3	حتى
4	1	3	165	4	3	حتي
486	3	1	486	4	3	إذا
49	2	2	217	4	3	اذا
0	0	64	2971	64	7	الايمان
17	1	63	2171	64	7	الإيمان
0	0	64	2150	64	7	ألإيمان

TABLE 2: Summery of a group of experiments

Figure 1 shows the time to search for words that has no result. Figure 2 shows the time required to return record from database. Figure 3 shows the time required for generated words when n_t is 1.

The comparison between figure 1 and figure 2 shows that time consumed in searching is much higher than the time required for getting the results from the information repository.

The comparison between figure 2 and figure 3 shows that the time required for getting the results increases as the number of returned results increases without regards of the number of letters of the word.

Figure 4 shows the time required for generated words when n_t is 8. Figure 5 shows that the w_t increase by a factor of searching time, which is 38.7 *8. Figure 5 shows the time required for searching and getting results of generated words when n_t is 8.

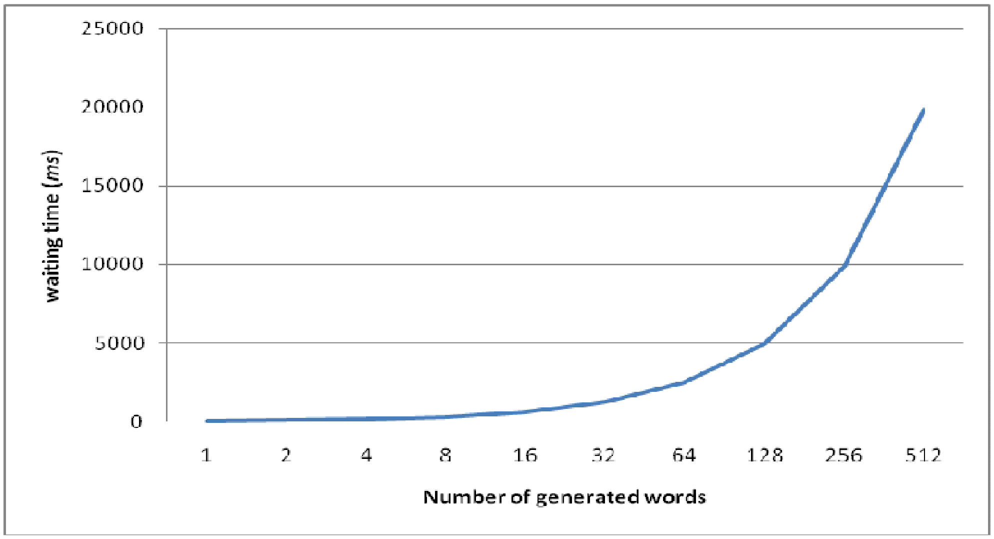


FIGURE 1 : the time required to search for words that has no result.

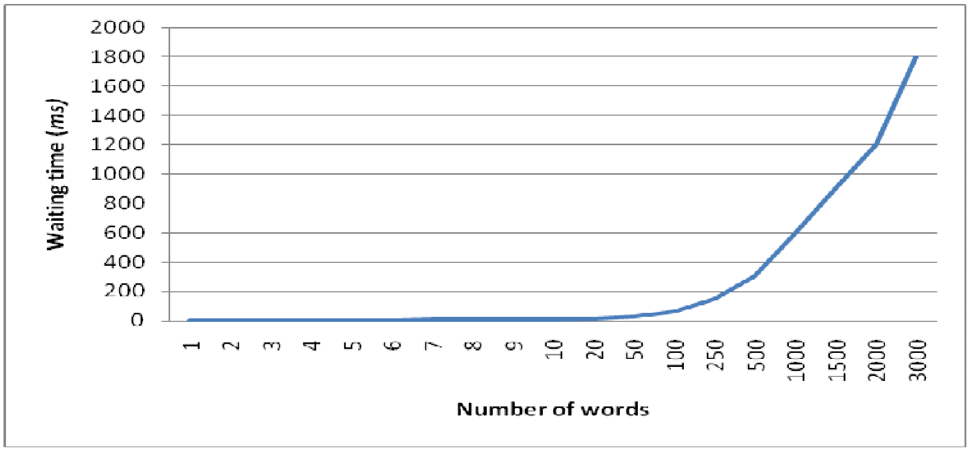


FIGURE 2 : the time required to return record from database.

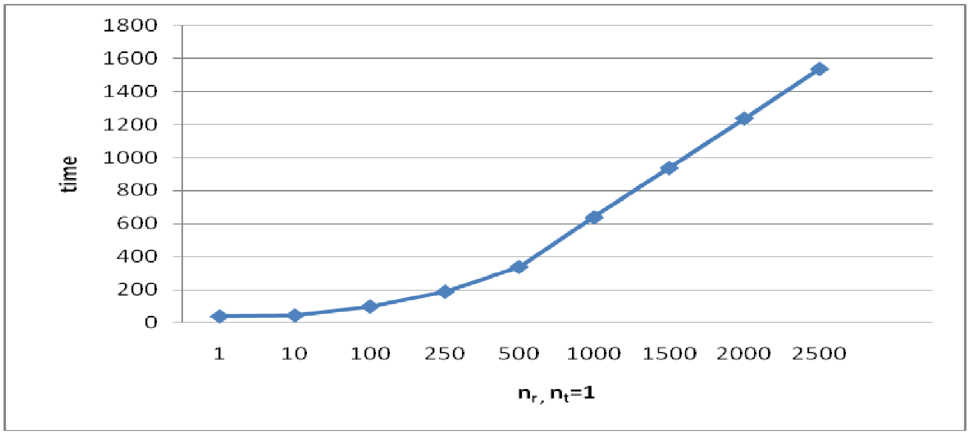


FIGURE 3 : The time required for generated words when n_t is 1.

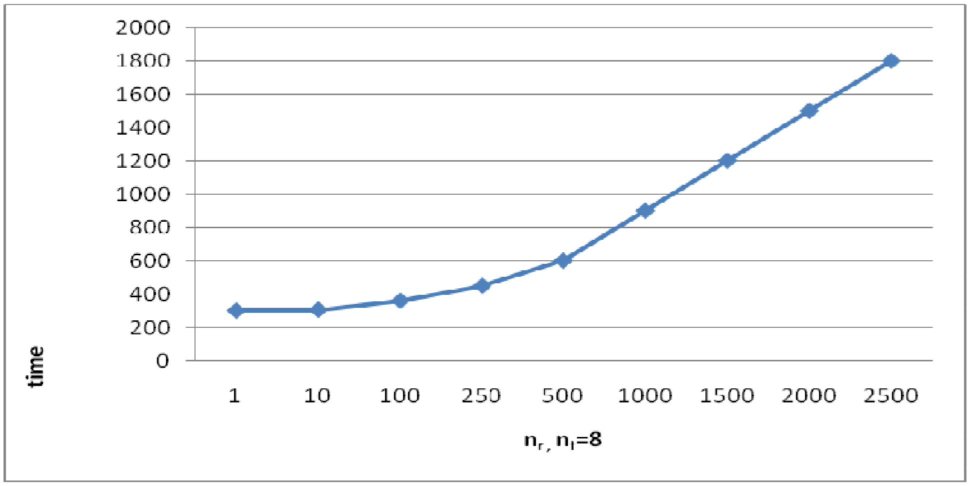


FIGURE 4 : The time required for generated words when n_t is 8.

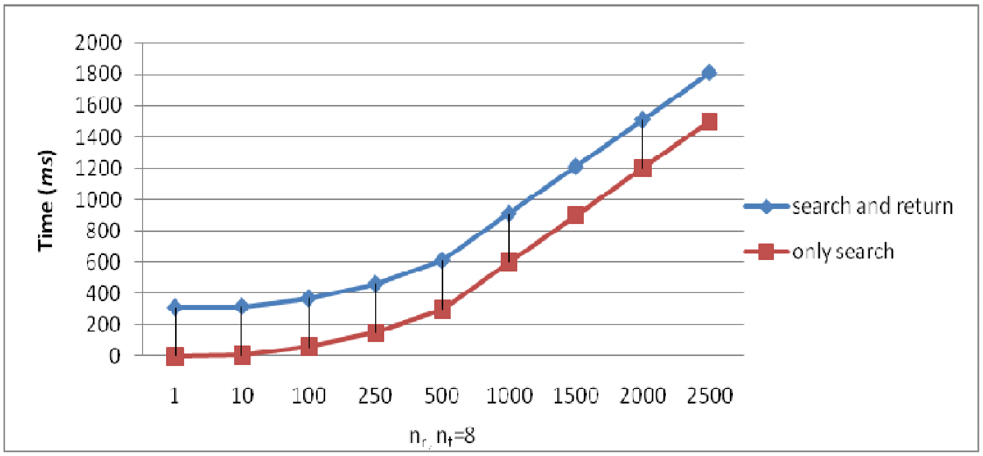


FIGURE 5 : The time required for searching and getting results of generated words when n_t is 8.

4. PERFORMANCE DEVELOPMENT

The system performance can be increased by decreases the waiting time when excluding the words that has no results. The time required to search for a word with no result is found to be 38.7 *ms.*

The average time to return one record is 0.605063 *ms.* In some cases, which is expected, some results were performed with high performance even with a large number of words without results. These results have low number of returned results and can be considered as words with no results as an assumption in this study.

According to Equation (3), there is a waiting time increase of 38.7 *ms* for each search. The worst case is small number of result or no result for the search.

The best case is where there is a group of results for each search. The small number of result can be defined as the number of results with waiting time close to the waiting time for searching for the same number of generated words with no results.

According to figure 5, there is 8 generated words. The waiting time increases as the number of returned words increases. The increase wating time is constant becasuse of searching is constant with 8 * 38.8.

Figure 6 shows that the percentage of the time used for searching is decreasing as the number of the returned results increases. This can lead to a conclusion that the percentage of searching time is much less than the returning time when the returned results is increasing. However, when the returned results are decreasing, most of the waiting time is in searching.

When n_t is 512 words , figure 7 shows that more than 90 % of the waiting time is searching either for large or small number of returned results.

Earlier figures of figure 3 and figure 4 shows that the waiting time increases as the number of generated words increases. By equation (1), figure 8 shows exponential increase of wating with the increase of the number of genreated words.

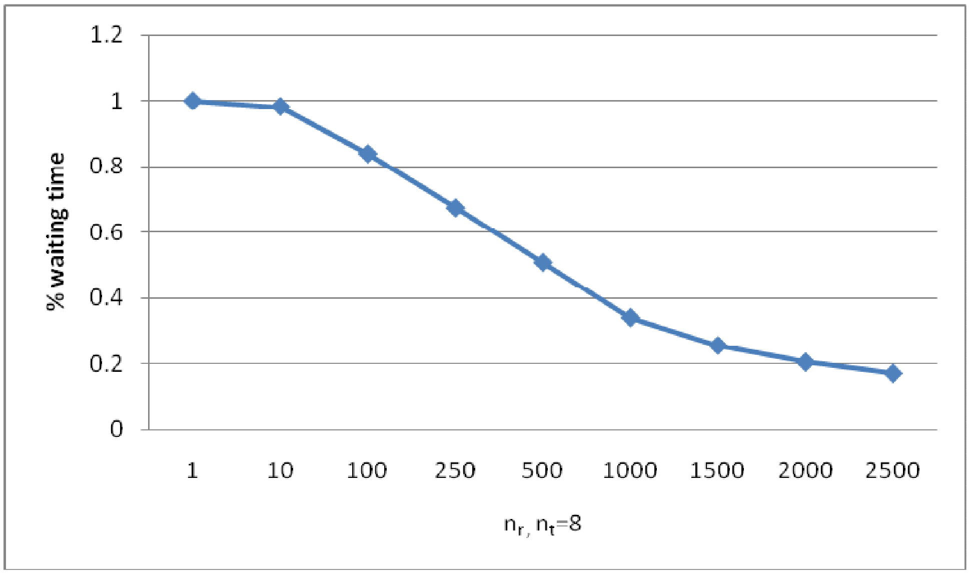


FIGURE 6: the % w_t for different n_r ,n_t=8

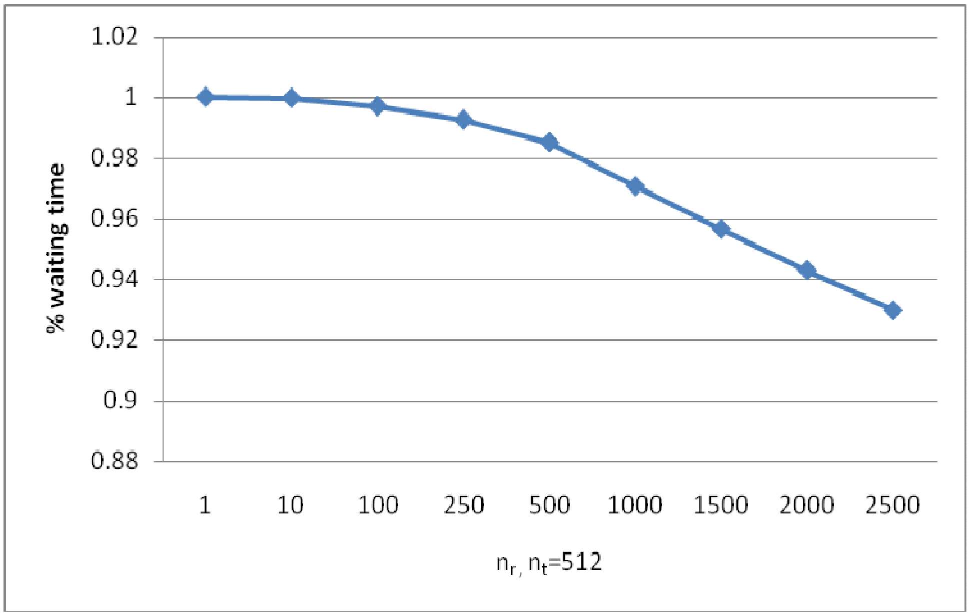


FIGURE 7: the % w_t for different n_r ,n_t=512

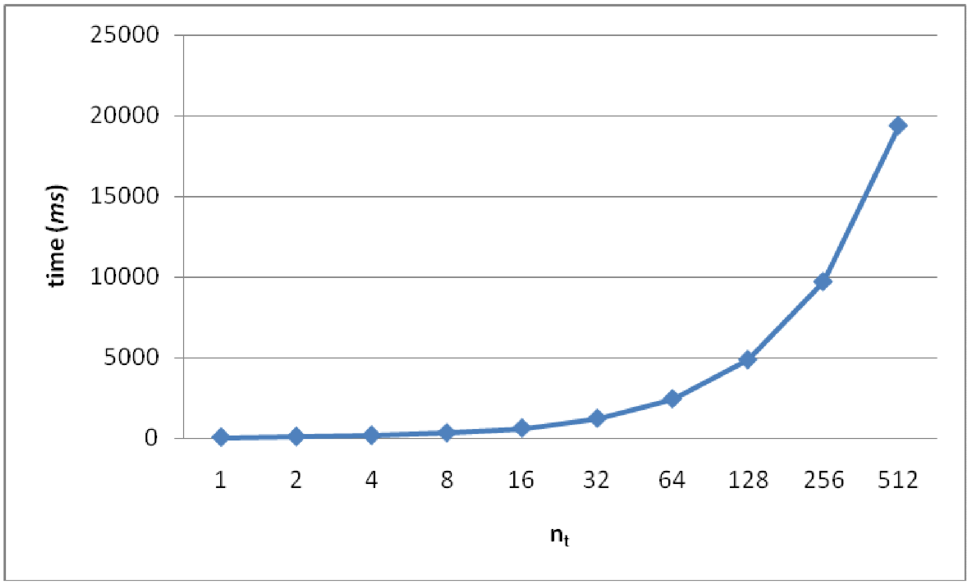


FIGURE 8: the w_t for different n_t

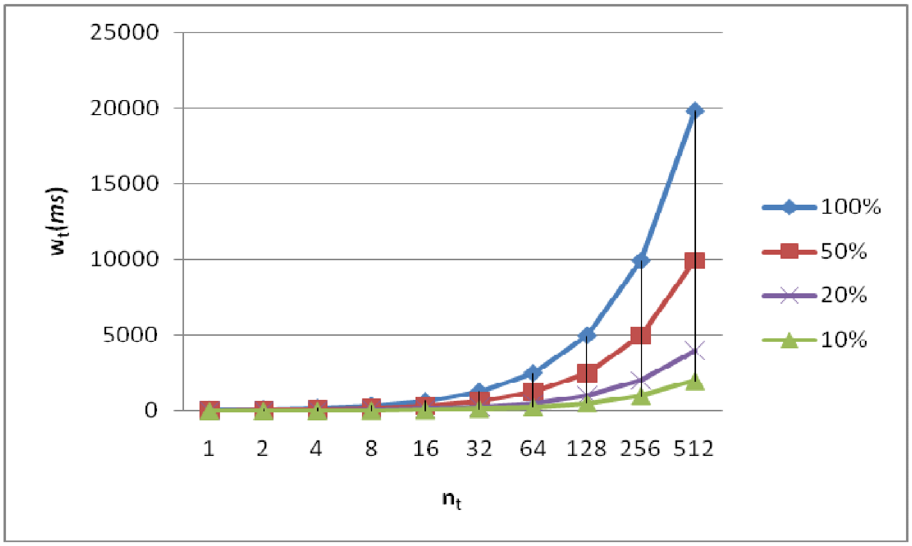


FIGURE 9: the w_t for different n_t

In conclusion, the percntage of waiting time used for search is increasing as the number of generated words increases. Not having every search return results, it is performance development advantage by excluding the words that have no results.

The system performance can be increased by having a list of words with no results to decrease waiting time. Figure 9 shows the w_t increases as the n_t increases. If 50%,20%,10% of the generated words has no results, 50%,20%,10% of the w_t is saved, consequently.

The detailed result is listed in table 3. The system will gain a great perfromance by exluding the words with no results. There is no tradeoff by using a table to list the excluded words with no results because this will be small table and time for searching is assumed to be zero time.

Furthermore in perfomance analysis, if a word has no result at all, the AIRS can be developed to exclude another table for words from the first step befor other steps befor generating other words. In general AIRS can be developed to work according the following algorithm:

```
Variables:
term: entered by user
t1: table of excluded terms
t2: table for exuded generate terms
Generated terms: contains terms that will be forwarded to the search engine.
The algorithm:
    1. User enters the Term.
    2. If the term is in t1, then return no results and move to step 7
    3. Generate all possible Terms
    4. Remove any term found in t2
    5. Search for generated term
    6. Return result set for all generated terms
    7. finish
```

Number of letters	n_r	% w_t , 10% of n_r with results	% w_t , 20% of n_r with results	% w_t , 50% of n_r with results	% w_t , 100% of n_r with result
1	1	3.87	7.74	19.35	38.7
2	2	7.74	15.48	38.7	77.4
3	4	15.48	30.96	77.4	154.8
4	8	30.96	61.92	154.8	309.6
5	16	61.92	123.84	309.6	619.2
6	32	123.84	247.68	619.2	1238.4
7	64	247.68	495.36	1238.4	2476.8
8	128	495.36	990.72	2476.8	4953.6
9	256	990.72	1981.44	4953.6	9907.2
10	512	1981.44	3962.88	9907.2	19814.4

TABLE 3: % w_t , different percentages of n_r with results

5. PERFORMANCE ANALYSIS

Some words can be without meaning but returns results because it is part of other words. This is the result of using regular expressions. For example the word حتي is not meaningful in Arabic but because it can be part of other words, there were a result set for it. The word حتى is meaningful but there was no result set for it.

The search term, for example, قال has some of the possible generated words such as قَال , قال قُال , قَالْ , قالْ , قّال , قالْ , قال , قال , قَالَ , قَال , قالَ , قَال , قالَ , قال , .. etc. There are 11 possible diacritics and this means this will results in 1331 different terms of قال. However, because the system uses regular expression, there will be only 4 words which are ق-ا-ل ,قا-ل ,ق-ال ,قال, where the dash or "-" is any possible diacritic.

Also, for performance reasons, some Arabic information retrieval system evaluates some Arabic letters to be equal, such as ا, أ, and إ.

Some words cannot be found in Arabic because the combination of diacritics does not exist and this is not a problem of processing because the system uses regular expression.

6. CONCLUSION AND FUTURE WORK

In conclusion, AIRS is a system model to retrieve information from Arabic text that includes diacritics. The system design, analysis and performance development is presented in this study. Results shows that the system overcomes the problem found in current information retrieval systems. Results show that the performance can be improved by extra algorithm steps.

The developed system assumes the user will not enter any diacritic. The user could select from the possible inputs to refine the search and the system considers the order of results. The system uses the discrete processing of input characters of the search term.

It is expected that some users may be interested in writing some diacritic for exact matches of the terms. The system can be developed for this purpose.

Future studies will include the addition of the stemming and lemmatization to the system, such that the searched term will be refereed to its lemma using a stemming engine. This will include more results for a search action. However, this will increase the number of terms that will be searched for each search action**.**

Future studies will include the addition of VSP model to the system. However, this will increase the number of terms that will be searched for each search process. Performance issues will meet challenges and will need advance information retrieval system to minimize words with no weight or no records at all.

7. REFERENCES

1. Hammo , Bassam, Mahmoud EL-Haj, Azzam Sleit (2008), Enhancing Retrieval Effectiveness of Diacritisized Arabic Passages Using Stemmer and Thesaurus: *The 19th Midwest Artificial Intelligence and Cognitive Science Conference* (Cincinnati, OH, USA).

2. Lazarinis , Fotis, Jesus Vilares Ferro, John Tait (2007)*,* Improving Non-English Web Searching (iNEWS07), *SIGIR Forum* 41(2) 72-76

3. Oracle (2010),http://www.java.com(accessed 17 April 2010).

4. Sudeshna Sarkar (2007), Regular Expression Matching for Multi-script Databases, *Bulletin on the Technical Committee on Data Engineering* 30(1) 17-29.

5. Sun Microsystems (2010), MySQL 5.5 Reference Manual (2010). Available at: www.mysql.com (accessed 16 Mar 2010).

6. The Unicode Consortium (2006), *Unicode Standard, Version 5.0*, Addison-Wesley, 5th edition.

7. Thabet , N. (2004), Stemming the Qur'an, *Proceedings of the Workshop on Computational Approaches to Arabic Script-based Languages*.

8. Zaki Aldeen Almonthery (2003), Mukhtasar Saheeh Muslim.

9. Alhajjar , A., Mohammad Hajjar, Khaldoun Zreik (2009), Classification of Arabic Information Extraction methods, *2nd International Conference on Arabic Language Resources and Tools*, Cairo, Egypt.

10. Beitzel, S., U. Syed, E. Jensen, O. Frieder and D. Grossman (2006), "On the Development of Name Search Techniques for Arabic", *Journal of the American Society for Information Science and Technology*, 57(6), pp.728– 739.

11. Carol Lundquist, Ophir Frieder, David O. Holmes and David Grossman (1999), parallel relational database management system approach to relevance feedback in information retrieval, Journal of the American Society for Information Science (JASIS), 50(5);413-426.

An Ant Algorithm for Solving QoS Multicast Routing Problem

A. Younes a_y_hamed@yahoo.com
Computer Science Department,
Faculty of Science, Sohag University,
Sohag, Egypt

Abstract

Many applications require send information from a source to multiple destinations through a communication network. To support these applications, it is necessary to determine a multicast tree of minimal cost to connect the source node to the destination nodes subject to delay constraints. Based on the Ant System algorithm, we present an ant algorithm to find the multicast tree that minimizes the total cost. In the proposed algorithm, the k shortest paths from the source node to the destination nodes are used for genotype representation. By comparing the results The expermintal results show that the algorithm can find optimal solution quickly and has a good scalability.

Keywords: Multimedia Communication; Multicast Routing; Multicast Tree; Ant Colony Algorithms; Bandwidth, Delay and Cost.

1. INTRODUCTION

The QoS multicast routing (QMR) problem concerns the search of optimal routing trees in the distributed network, where messages or information are sent from the source node to all destination nodes, while meeting all QoS requirements. This problem is NP completes [1]. Over the past decades, many unconstrained or simple constrained multicast routing algorithms have been developed. Typical approaches include (1) applying Dijkstra algorithm to find the shortest path, (2) seeking the minimum network cost using Steiner tree routing algorithm, and (3) finding multicast trees that the paths between source node and the destination nodes are connected and their cost is minimized. A state of the art review and analysis can be found, see [1]- [3].

There are many studies that apply genetic algorithms (GA) and ant algorithms to solve the QMR problems (with different types of QoS constraints) are increasing. In [4] – [7], a heuristic GA is used to solve the QMR problems. The algorithm acquires the solution by representing a multicast tree as a chromosome so as to save the coding spaces and reduce the decoding operations (compared with the binary coding mechanism). However, these approaches cannot be expanded. If one or more nodes are added into the network, the system needs to scan all nodes again to acquire the optimum solution. That is, previous network information cannot be transferred to the expanded network.

A number of efficient heuristic algorithms given in [7] – [9], consider a number of rigid QoS criteria, such as bandwidth, delay, delay constraint, and packet loss rate. Chu [10], presented a model that treats these constraints separately, add more constraints such as delay jitter and packet loss rate, and take network expansion into account.

In [11], an efficient algorithm based on ant system is used for generating a low-cost multicast tree subject to delay constraints. The algorithm starts with a backup-paths-set from the source node to each destination nodes using Dijkstra Kth shortest path algorithm. Then transform the formed procedure of the multicast tree to the Graph, and use AS to the QoS problems: when a ant move from the node i to the node j depend on the corresponding probabilities function, and update the Pheromone on Graph when every iteration finished.

In the last years, the genetic algorithms (GA) are gaining an increasing interest for solving complex problems in the networking field, as network design [13] and unicast routing [14]. GA for multicast routing without constraints was presented by [15] and [16], while authors in [17] and [18] addressed the constrained problem taking into account the QoS level provided for real-time applications in single multicast sessions. Luca and Lugi [19], presented an approach for group multicast routing by genetic algorithm. Chen [12], proposed a new multicast routing optimization algorithm based on Genetic Algorithms, which find the low-cost multicasting tree with bandwidth and delay constraints.

In this paper, we propose an efficient algorithm based on ant system for generating a low-cost multicast tree subject to delay constraints. The proposed algorithm uses a genetic algorithm given in [4], to find the kth shortest paths from the source node to each destination nodes. Then we use the Ant System to solve the QoS problems: when an Ant moves through a shortest path it depends on the corresponding probabilities function and update Pheromone on that path after finishing each iteration. The experimental results show the comparison between the proposed ant algorithm and the genetic algorithm, [12]. Simulation results show our algorithm has features of well performance of cost, fast convergence and stable delay.

The rest of the paper is organized as follows: Section 2 presents the problem description and formulation. Sections 3 describe our Ant-System based QOS multicasting algorithm followed by time complexity of the algorithm. Simulation results and comparison with other reported heuristics are presented in Section4. Section 5 concludes the paper.

2. PROBLEM DESCRIPTION AND FORMULATION

A network is usually represented as a weighted directed graph *G*=(*N,E*), where *N* denotes the set of nodes and *E* denotes the set of communication links connecting the nodes. |*N*| and |*E*| denote the number of nodes and links in the network respectively. We consider the multicast routing problem with bandwidth and delay constraints from one source node to multi-destination nodes. Let $X = \{n_0,\ u_1, u_2, ...u_m\} \in N$ be a set of from source to destination nodes of the multicast tree. Where n_0 is source node, and $U = \{u_1\ ,\ u_2\ \ldots\ u_m\}$ denotes a set of destination nodes. Multicast tree $T = (N_T\ ,\ E_T\ )$, where $N_T \subseteq N$, $E_T\ \subseteq E$, there exists the path $P_T\ (n_0\ ,\ d)$ from source node n_0 to each destination node $d \in U$ in *T*. *e*(*i*,j) is a link from node i$\in N$ to node $j \in N$. Three non-negative real value functions are associated with each link *e*($e \in E$): cost *C*(*e*), delay *D*(*e*), and available bandwidth *B*(*e*). The link cost function, *C*(*e*), may be either monetary cost or any measure of the resource utilization, which must be optimized. The link delay, *D*(*e*), is considered to be the sum of switching, queuing, transmission, and propagation delays. The link bandwidth, *B*(*e*), is the residual bandwidth of the physical or logical link. The link delay and bandwidth functions, *D*(*e*) and *B*(*e*), define the criteria that must be constrained.

The cost of the path P_T *is* defined as the sum of the cost of all links in that path and can be given by

$$C(P_T) = \sum_{e \in P_T} C(e) \tag{1}$$

The total cost of the tree *T* is defined as the sum of the cost of all links in that tree and can be given by

$$C(T) = \sum_{e \in E_T} C(e) \tag{2}$$

The total delay of the path $P_T(n_0,d)$ is simply the sum of the delay of all links along $P_T(n_0,d)$:

$$D(P_T) = \sum_{e \in P_T(n_0,d)} D(e), \qquad d \in U \tag{3}$$

The delay of multicast tree *T* is the maximum value of delay in the path from source node n_0 *to* each destination node $d \in U$.

$$D(T) = \max(\sum_{e \in P_T(n_0,d)} D(P_T), \qquad d \in U) \tag{4}$$

The bandwidth of the path $P_T(n_0,d)$ is defined as the minimum available residual bandwidth at any link along the path:

$$B(P_T) = \min(B(e), e \in P_T) \tag{5}$$

The bandwidth of the tree *T* is defined as the minimum available residual bandwidth at any link along the tree:

$$B(T) = \min(B(e), e \in E_T) \tag{6}$$

Assume the minimum bandwidth constraint of multicast tree is *B*, and the maximum delay constraint id is *D*, given a multicast demand *R*, then, the problem of bandwidth-delay constrained multicast routing is to find a multicast tree *T*, satisfying:

1. Bandwidth constraint: $B\,(T) = B$.
2. Delay constraint: $D\,(T) = D$.

Suppose *S*(*R*) is the set, *S*(*R*) satisfies the conditions
above, then, the multicast tree *T* which we find is:

$$C\,(T) = \min\,(C\,(Ts),\ Ts \in S(R))$$

3. THE PROPOSED ANT ALGORITHM

Assuming n_0 is source node, and $U = \{u_1, u_2 \ldots u_m\}$ denotes a set of destination nodes, the smallest bandwidth constraint, and by the algorithm for finding the *k* shortest paths in reference [4], we can find the candidate route set from source node to each destination node i (i.e. $P_i = \{p_1, p_2, \ldots\ldots\ldots, p_n\}$). The proposed ant algorithm can be performed as the following steps:

<u>Algorithm: Ant algorithm for multicast routing</u>

```
1. Initialize network nodes.
   a. Define the source node s and the destination nodes $U= \{u_1, u_2 \ldots u_m\}$
b. Set NC =0 (NC is a loop counter.), and put m ants to s
2. For each destination node $u_i \in U$,
3. Let $Pi$ be the set of the shortest paths for the destination node $u_i$ ( by using [4]).
4. Assign an initial value $\tau_k = 0$ ; to the pheromone intensity of every $p_k$, k=1,2,...n,
5. Begin the first tour;
6. Let m ants move from s to $u_i$ on $P_i$ equally (the ants number in each path $p_k$ is equal).
7. Compute the pheromone amount left by $x$ ants at $p_k$ ($\Delta\tau_k$) by using the following equation:
```

$$\Delta\tau_k^{total} = \frac{Q}{C_k} * x; \qquad (7)$$

Where C_k is the cost of the path p_k and is computed by Eq. (1).

8. Update the local pheromone τ_k ;

$$\tau_k = (1-\rho)\tau_k + \Delta\tau_k^{total}; \qquad (8)$$

Where $\rho \in (0, 1]$ is the evaporation rate.

9. Begin a new tour
10. Set NC=NC+1;
11. Compute the corresponding probabilities function f_k for each p_k as follows:

$$f_k = \begin{cases} \dfrac{[\tau_k]^\alpha * [\eta_k]^\beta}{\sum\limits_{j \in n} [\tau_j]^\alpha * [\eta_j]^\beta}; & k \in n \\ 0 & otherwise \end{cases} \qquad (9)$$

Where $\eta_k = \dfrac{1}{d_k}$; d_k is computed by using Eq. (3), and α, β denote the information accumulated during the movement of ants and the different effects of factors in the path selection.

12. Compute $\Delta\tau_k$ by using Eq. (7)
13. Update the global pheromone τ_k by using Eq. (8)
14. Repeat from step 9 until NC_{max}
15. Compare between the values of τ_k to get the best path for the destination u_i (p_{ui}).
16. End For
17. Collect the all best path (p_{ui}) to get the multicast tree.

4. EXPERIMENTAL RESULTS

In this section, we show the effectiveness of the above algorithm by applying it on two examples and compare the results which obtained by the proposed ant algorithm with the results of which obtained by [12].

The parameters setting in the proposed algorithm as follows: ants number m = 30, $\rho = 0.5$, α=β=1, and NC_{max}=20 (iteration numbers).

4.1 First Example

We consider a network with 8 nodes taken from [12]. Each link represented by a triple-group (B, *D*, *C*), given its value randomly as shown in Fig. 1.

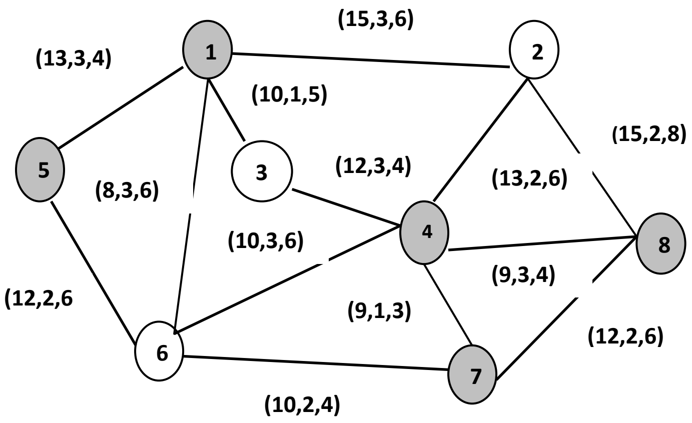


FIGURE 1: Network Topology Structure

Assuming the source node n_0 is node 1, destination node set *U*= {4, 5, 7, 8} as shown in the above figure. By the algorithm for finding the *k* shortest paths in reference [4] with smallest bandwidth constraint B=10, we can find the candidate route set from source node 1 to each destination node, as shown in Table 1.

Destination node	The shortest paths
4	1 2 8 7 6 4
	1 3 4
	1 5 6 4
	1 2 4
	1 5 6 7 8 2 4
5	1 5
	1 2 4 6 5
	1 2 8 7 6 5
	1 3 4 6 5
7	1 3 4 2 8 7
	1 3 4 6 7
	1 2 4 6 7
	1 2 8 7
	1 5 6 7
	1 5 6 4 2 8 7
8	1 5 6 4 2 8
	1 3 4 2 8
	1 3 4 6 7 8
	1 5 6 7 8
	1 2 8
	1 2 4 6 7 8

TABLE 1: The candidate route set from source node 1 to each destination node

We find the multicast tree as shown in Fig.2 with cost=41.

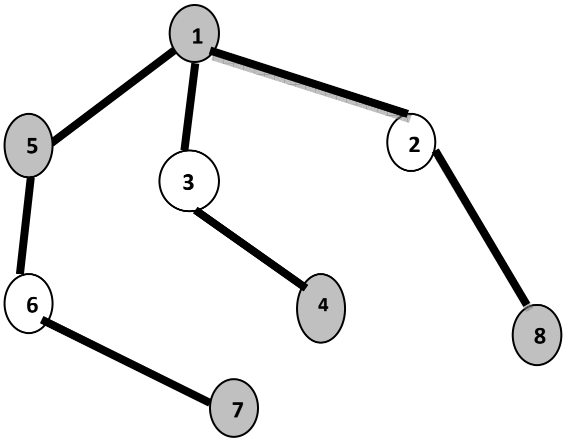


FIGURE 2: The Multicast Tree obtained by the proposed Ant Algorithm

Figure 3(a, b, c, and d)) shows the number of ants on each path of the destination 4, 5, 7, and 8 respectively.

The following figures show the best path which represents the candidate route from the source node 1 to the destination nodes. The horizontal axis represents the tour number and the vertical axis represents the number of ants.

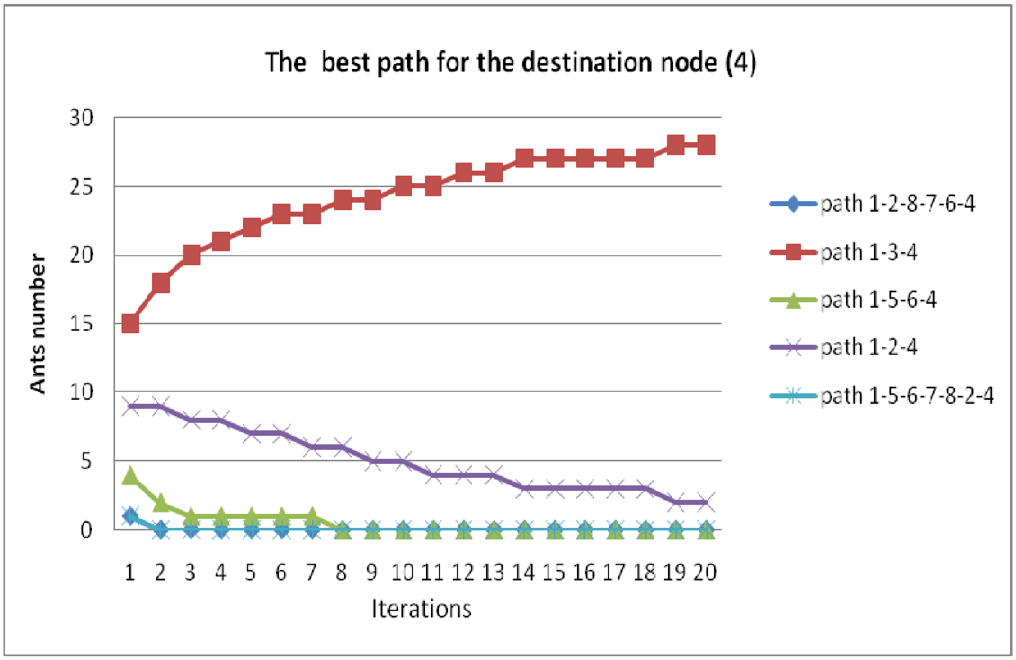


FIGURE 3(a): The iteration number and the number of Ants for the destination 4.

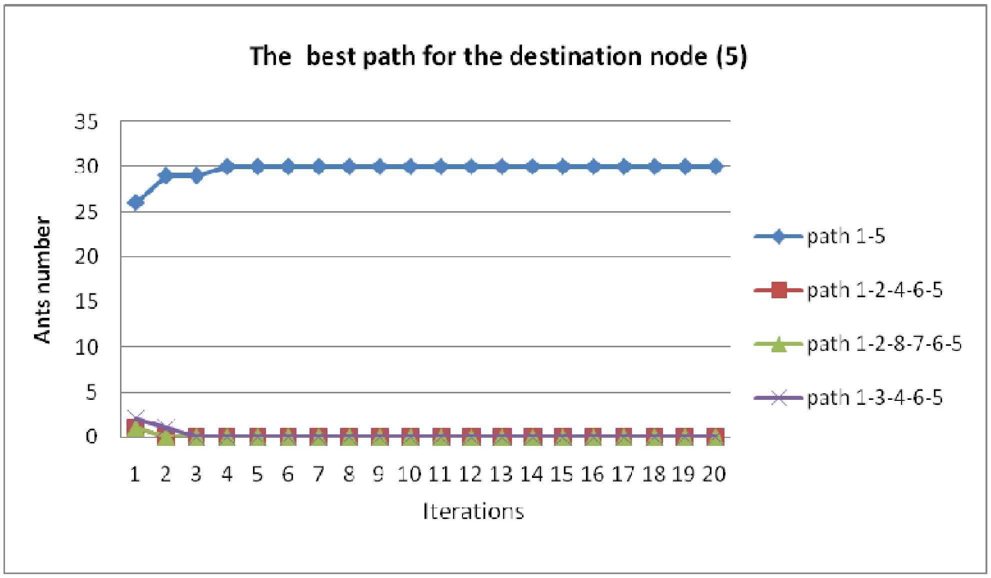


FIGURE 3(b): The iteration number and the number of Ants for the destination 5.

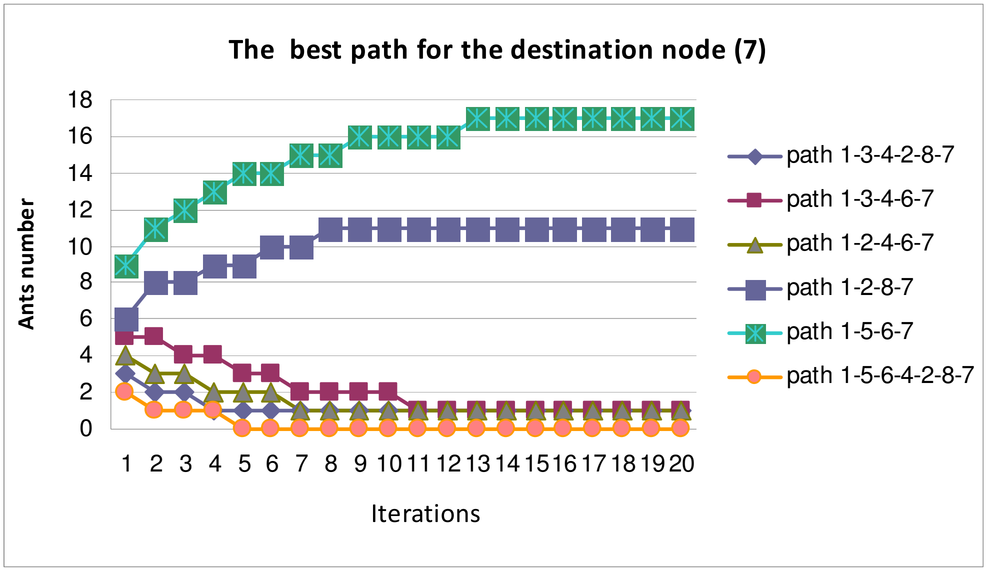


FIGURE 3(c): The iteration number and the number of Ants for the destination 7.

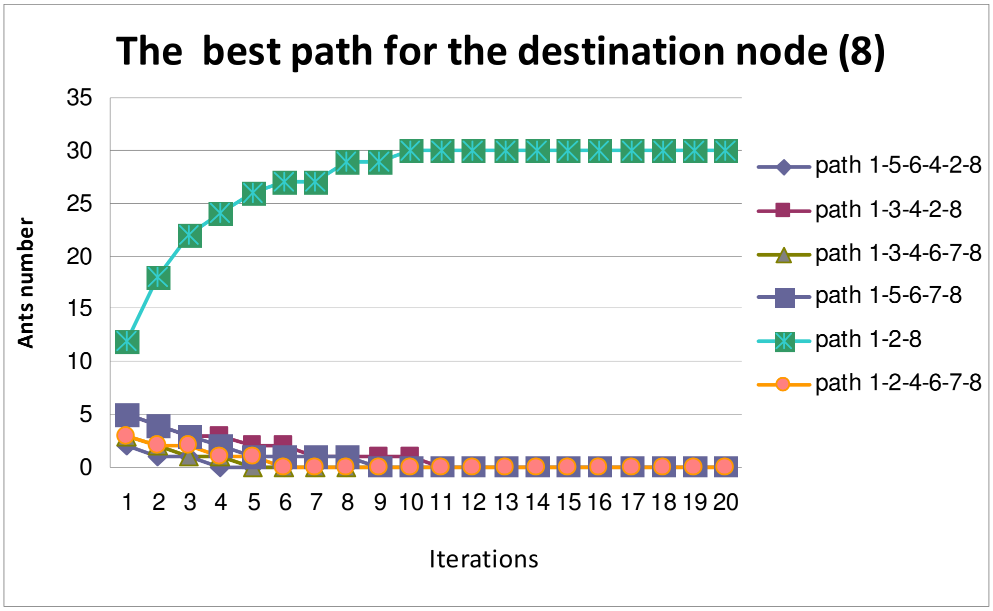


FIGURE 3(d): The iteration number and the number of Ants for the destination 8.

From the above figures, if we consider the figure 3(d) as an example we note that: the number of ants in the path 1-2-8 increases from 11 to 30 during iteration 1 to iteration 20. But the number of ants on the other paths is decreasing to 0. This means that, the path 1-2-8 is the best candidate route from the source node 1 to the destination node 8.

Figure 4 represents the multicast tree which obtained by the genetic algorithm, [12].

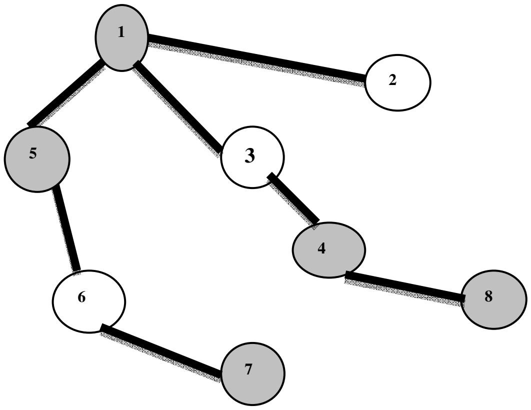


FIGURE 4: The Multicast Tree obtained by [12].

By comparing the Multicast tree obtained by the proposed Ant algorithm, given in Fig. 2 and the other one which obtained by using genetic algorithm [12], given in Fig. 4, we noted the following:

1. The bandwidth B of the path 1->3->4->8 in the tree obtained by [12] equal to 9 according to Eq. 5 which is not 10 as it is imposed.
2. The path 1->2 isn't true, because the node 2 does not represent the destination node.

Hence, the multicast tree obtained by [12] is not correct, based on the parameters imposed.

4.2 Second Example

We consider a network with 8 nodes taken from [10]. Each link represented by a triple-group (D, B, *C*), given its value randomly as shown in Fig.5 and compare the results with [10].

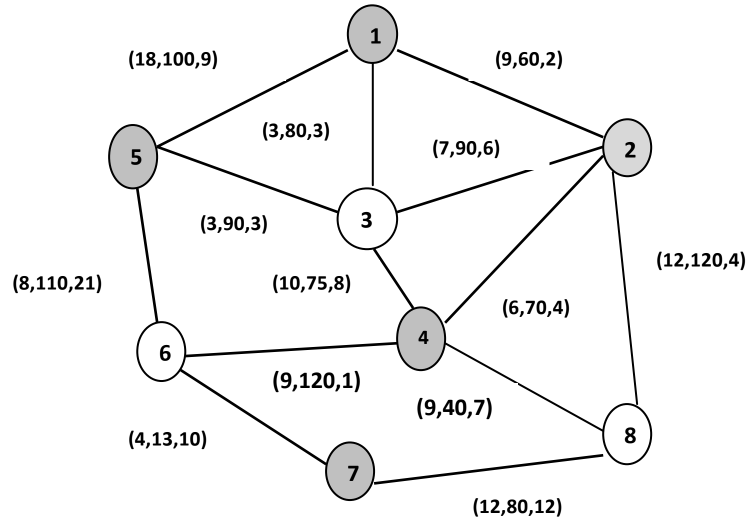


FIGURE 5: **Network Topology Structure**

Assuming the source node n_0 is node 1, destination node set U= {2, 4, 5, 7} as shown in the above figure. By the algorithm for finding the *k* shortest paths in reference [4] with smallest bandwidth constraint B=70, we can find the candidate route set from source node 1 to each destination node, as shown in Table 2.

Destination node	The shortest paths
2	1 3 4 2
	1 5 3 2
	1 5 3 4 2
	1 3 5 6 4 2
	1 3 2
	1 5 6 7 8 2
	1 5 6 4 2
	1 5 6 4 3 2
	1 3 5 6 7 8 2
4	1 5 3 4
	1 5 3 2 4
	1 3 5 6 4
	1 5 6 4
	1 3 2 4
	1 3 4
5	1 5
	1 3 4 6 5
	1 3 5
	1 3 2 4 6 5
7	1 3 5 6 7
	1 3 4 6 7
	1 5 6 7
	1 3 4 2 8 7
	1 3 2 8 7
	1 5 3 4 6 7

TABLE 2: The candidate route set from source node 1 to each destination node

We find the multicast tree as shown in Fig.6 with cost=63.

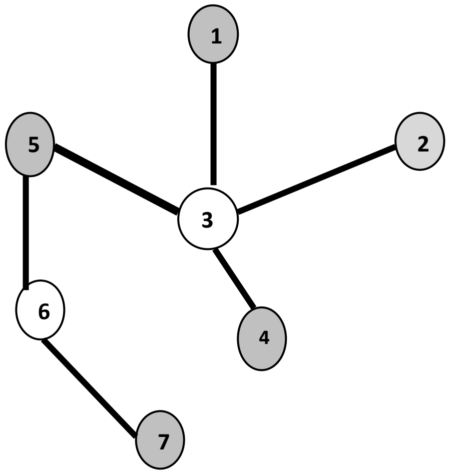


FIGURE 6: The Multicast Tree obtained by the proposed Ant Algorithm

The multicast tree obtained by [10] is shown in Fig. 7.

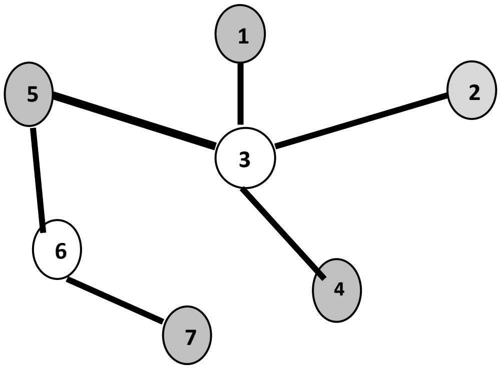


FIGURE 7: The Multicast Tree obtained by [10]

By comparing the previous results we observe that the multicast tree obtained by the proposed Ant algorithm is quite similar to the multicast tree obtained by [10].This means that the proposed Ant algorithm is working properly.

5. CONCLUSION

This paper presented an Ant algorithm for solving QoS multicast routing problem based on bandwidth and delay constraints. The proposed algorithm uses the k^{th} shortest paths algorithm [4], to construct the route set. Then, we have a set of paths for each destination nodes; the Ants moving through the paths depending on the corresponding probabilities function and update the Pheromone on the paths after finishing each iteration. Simulation results show that the proposed algorithm has features of well performance of cost, fast convergence and stable delay. The algorithm can guarantee the requirement of multimedia group communication for quality of service.

6. REFERENCES

1. L. H. Sahasrabuddhe, and B. Mukherjee, *"Multicast Routing Algorithms and Protocols: A Tutorial", IEEE Network*, pp. 90-102, January, February 2000.

2. B. Wang, and J. C. Hou, *"Multicast Routing and Its QoS Extension: Problems, Algorithms, and Protocols," IEEE Network*, pp. 22-36, January/February 2000.

3. H. F. Salama, D. S. Reeves, and Y. Viniotis, *"Evaluation of Multicast Routing Algorithms for Real-Time Communication on High-Speed Networks," IEEE Journal on Selected Areas in Communications*, Vol. 15(3): 332-345, 1997.

4. A. Younes, *"A Genetic Algorithm for Finding the K Shortest Paths in a Network*", Egyptian Informatics Journal, Vol.10(2), 2010.

5. Z. Wang, and B. Shi, *"Solution to QoS Multicast Routing Problem Based on Heuristic Genetic Algorithm," Journal of Computer*, 2001, Vol. 24(1): 55-61, 2001.

6. X. Zhou, C. Chen, and G. Zhu, "A Genetic Algorithm for Multicasting Routing Problem," International Conference on Communication Technology, Vol. 2, pp. 1248-1253, 2000.

7. Z. Wang, and J. Crowcroft, *"Quality of Service for Supporting Multimedia Applications," IEEE Journal on Selected Areas in Communications*, Vol. 14(7): 1228-1234, 1996.

8. L. Guo and I. Matta, *"QDMR: An Efficient QoS Dependent Multicast Routing Algorithm,"* Proceedings of the Fifth IEEE Real-Time Technology and Applications Symposium, pp. 213-222, 1999.

9. W. Wu, *"Multicast routing Algorithm Based on Multiple Qualities of Services," Applied Electronic Technologies"*, Vol. 266(8), 2000.

10. Chao-Hsien Chu, *"A Heuristic Ant Algorithm for Solving QoS Multicast Routing Problem"*, Proceedings of the Evolutionary Computation Vol. 2, 2002.

11. Lin Huang, Haishan Han and Jian Hou, *"Multicast Routing Based on the Ant System",*Applied Mathematical Sciences, Vol. 1(57): 2827–2838, 2007.

12. Hua Chen, Baolin Sun, *" Multicast Routing Optimization Algorithm with Bandwidth and Delay Constraints Based on GA",* Journal of Communication and Computer, Vol. 2(5): 2005.

13. L. Atzori and A. Raccis, *"Network Capacity Assignment for Multicast Services Using Genetic Algorithms"*, IEEE Communications Letters, vol. 8(6): 403-405, June 2004.

14. C.W. Ahn and R.S. Ramakrishna, *"A genetic algorithm for shortest path routing problem and the sizing of population"*, IEEE Transaction on evolutionary computation, vol. 6(6): Dec. 2002.

15. R.H. Hwang, W.Y. Do, and S.C. Yang, "*Multicast Routing Based on Genetic Algorithms",* Journal of information science and engineering, vo1.16, pp.885-901, 2000.

16. R. Bhattacharya, P. Venkateswaran, S.K. Sanyal, R. Nandi, , *"Genetic algorithm based efficient outing scheme for multicast networks",* IEEE International Conference on Personal Wireless Communications (ICPWC 2005), pp. 500 - 504, Jan 2005

17. L. Chen, Z. Yang, Z. Xu, *"A degree-delay-constrained genetic algorithm for multicast routing tree"*, The Fourth International Conference on Computer and Information Technology (CIT), pp. 1033 -1038, September 2004.

18. M. Hamdan and M.E. El-Hawary, *"Multicast routing with delay and delay variation constraints using genetic algorithm"*, Canadian Conference on Electrical and Computer Engineering, vol. 4, pp. 2363 - 2366, May 2004.

19. Luca Sanna Randaccio and Luigi Atzori, *"A Genetic Algorithm Based Approach for Group Multicast Routing"*, Journal of Networks, Vol. 1(4): , 2006.

INSTRUCTIONS TO CONTRIBUTORS

The *International Journal of Computer Science and Security (IJCSS)* is a refereed online journal which is a forum for publication of current research in computer science and computer security technologies. It considers any material dealing primarily with the technological aspects of computer science and computer security. The journal is targeted to be read by academics, scholars, advanced students, practitioners, and those seeking an update on current experience and future prospects in relation to all aspects computer science in general but specific to computer security themes. Subjects covered include: access control, computer security, cryptography, communications and data security, databases, electronic commerce, multimedia, bioinformatics, signal processing and image processing etc.

To build its International reputation, we are disseminating the publication information through Google Books, Google Scholar, Directory of Open Access Journals (DOAJ), Open J Gate, ScientificCommons, Docstoc and many more. Our International Editors are working on establishing ISI listing and a good impact factor for IJCSS.

The initial efforts helped to shape the editorial policy and to sharpen the focus of the journal. Starting with volume 5, 2011, IJCSS appears in more focused issues. Besides normal publications, IJCSS intend to organized special issues on more focused topics. Each special issue will have a designated editor (editors) – either member of the editorial board or another recognized specialist in the respective field.

We are open to contributions, proposals for any topic as well as for editors and reviewers. We understand that it is through the effort of volunteers that CSC Journals continues to grow and flourish.

IJCSS LIST OF TOPICS

The realm of International Journal of Computer Science and Security (IJCSS) extends, but not limited, to the following:

- Authentication and authorization models
- Computer Engineering
- Computer Networks
- Cryptography
- Databases
- Image processing
- Operating systems
- Programming languages
- Signal processing
- Theory
- Communications and data security
- Bioinformatics
- Computer graphics
- Computer security
- Data mining
- Electronic commerce
- Object Orientation
- Parallel and distributed processing
- Robotics
- Software engineering

CALL FOR PAPERS

Volume: 5 - **Issue:** 3 - May 2011

i. Paper Submission: May 31, 2011

ii. Author Notification: July 01, 2011

iii. Issue Publication: July /August 2011

CONTACT INFORMATION

Computer Science Journals Sdn BhD
M-3-19, Plaza Damas Sri Hartamas
50480, Kuala Lumpur MALAYSIA

Phone: 006 03 6207 1607
006 03 2782 6991

Fax: 006 03 6207 1697

Email: cscpress@cscjournals.org

CSC PUBLISHERS © 2011
COMPUTER SCIENCE JOURNALS SDN BHD
M-3-19, PLAZA DAMAS
SRI HARTAMAS
50480, KUALA LUMPUR
MALAYSIA

PHONE: 006 03 6207 1607
006 03 2782 6991

FAX: 006 03 6207 1697
EMAIL: cscpress@cscjournals.org