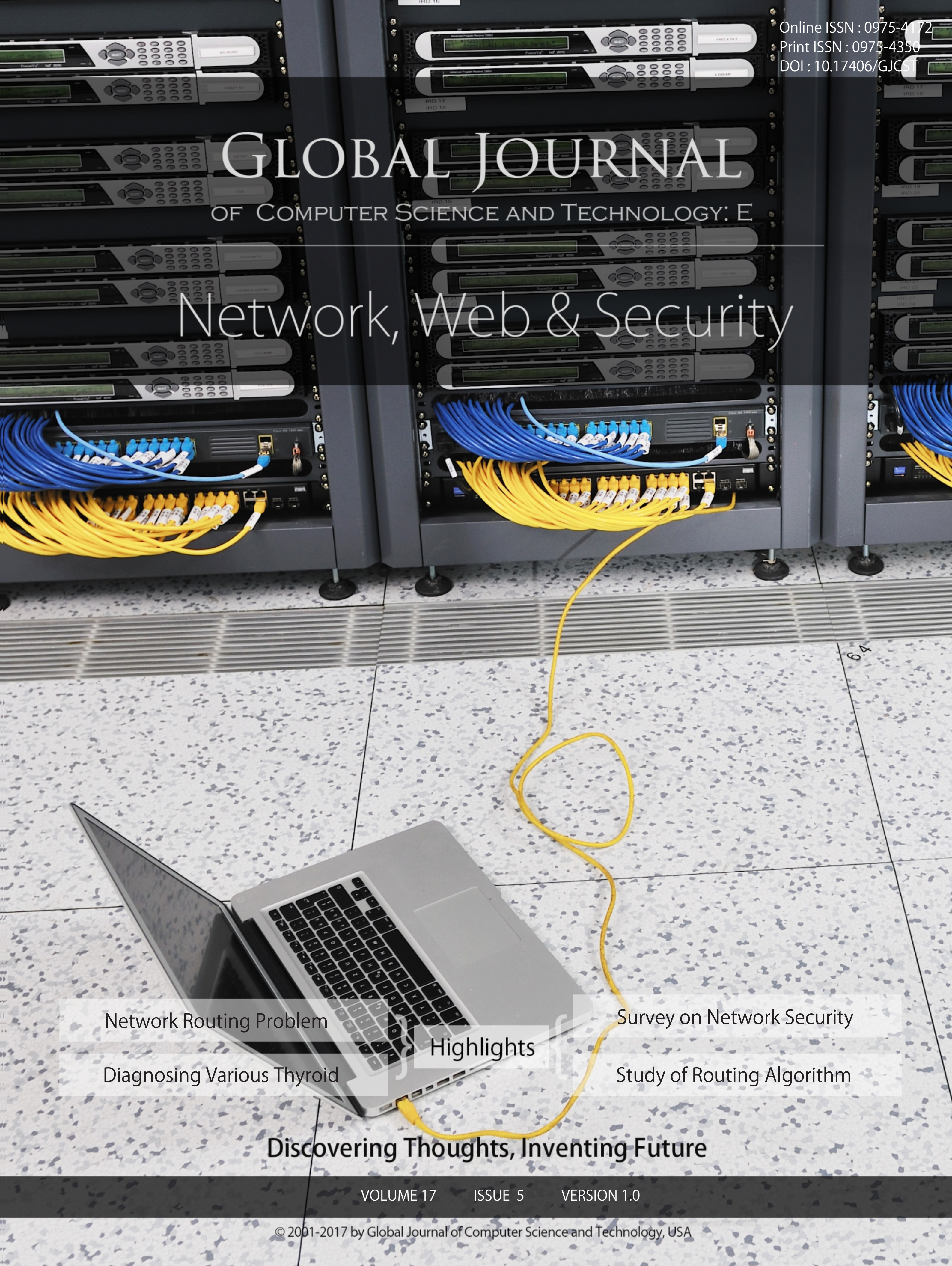
Online ISSN : 0975-4172
Print ISSN : 0975-4350
DOI : 10.17406/GJCST



Global Journal

of Computer Science and Technology: E

Network, Web & Security

Highlights

- Network Routing Problem
- Diagnosing Various Thyroid
- Survey on Network Security
- Study of Routing Algorithm

Discovering Thoughts, Inventing Future

VOLUME 17 ISSUE 5 VERSION 1.0

Global Journal of Computer Science and Technology: E
Network, Web & Security

Global Journal of Computer Science and Technology: E
Network, Web & Security

Volume 17 Issue 5 (Ver. 1.0)

Open Association of Research Society

Incorporation No.: 0423089
License No.: 42125/022010/1186
Registration No.: 430374
Import-Export Code: 1109007027
Employer Identification Number (EIN):
USA Tax ID: 98-0673427

Global Journals Inc.

*(A Delaware USA Incorporation with "Good Standing"; **Reg. Number: 0423089**)*

Sponsors: *Open Association of Research Society*
Open Scientific Standards

Publisher's Headquarters office

Global Journals® Headquarters
945th Concord Streets,
Framingham Massachusetts Pin: 01701,
United States of America
USA Toll Free: +001-888-839-7392
USA Toll Free Fax: +001-888-839-7392

Offset Typesetting

Global Journals Incorporated
2nd, Lansdowne, Lansdowne Rd., Croydon-Surrey,
Pin: CR9 2ER, United Kingdom

Packaging & Continental Dispatching

Global Journals Pvt Ltd
E-3130 Sudama Nagar, Near Gopur Square,
Indore, M.P., Pin:452009, India

Find a correspondence nodal officer near you

To find nodal officer of your country, please email us at *local@globaljournals.org*

eContacts

Press Inquiries: *press@globaljournals.org*
Investor Inquiries: *investors@globaljournals.org*
Technical Support: *technology@globaljournals.org*
Media & Releases: *media@globaljournals.org*

Pricing (Excluding Air Parcel Charges):

Yearly Subscription (Personal & Institutional)
250 USD (B/W) & 350 USD (Color)

Editorial Board

Global Journal of Computer Science and Technology

Contents of the Issue

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 17 Issue 5 Version 1.0 Year 2017
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Enchancing Qos in Manets using Preemptive AOMDV

By Mahak Singla & Dr. Paramjeet Singh

Abstract- MANETS is network of mobile devices. They communicate without the presence of any central device. Since nodes are mobile in nature the network has to face many problems like unpredictable link properties, security, battery life and route maintenance that affects the quality of Service (QoS) of the network. Lot of work has been done to increase the QoS of MANETS. In this paper also we will discuss about a new proposed algorithm to increase QoS of the network in terms of throughput and end to end delay.

Keywords: AOMDV, reactive, preemptive, priority, QoS.

GJCST-E Classification: C.1.4, C.1.3

ENCHANCINGQOSINMANETSUSINGPREEMPTIVEAOMDV

Enchancing Qos in Manets using Preemptive AOMDV

Mahak Singla [α] & Dr. Paramjeet Singh [σ]

Abstract- MANETS is network of mobile devices. They communicate without the presence of any central device. Since nodes are mobile in nature the network has to face many problems like unpredictable link properties, security, battery life and route maintenance that affects the quality of Service (QoS) of the network. Lot of work has been done to increase the QoS of MANETS. In this paper also we will discuss about a new proposed algorithm to increase QoS of the network in terms of throughput and end to end delay.

Keywords: AOMDV, reactive, preemptive, priority, QoS.

I. Introduction

MANETs are useful in all those areas where wired networks have failed like in battlefields, disaster operations [1]. Transmission Control Protocol (TCP) provides the reliable data delivery both within and across the MANET. MANETs have low bandwidth as they use batteries to maintain energy efficiency required for maximizing the life of nodes.

AOMDV is an extension of AODV routing protocol whereas AODV is an extension of Dynamic Source Routing (DSR).

DSR → AODV → AOMDV

These protocols follow Reactive topological routing where there exist no pre-established routing tables unlike that is made in Proactive routing. In reactive topology in the process of destination discovery, the active route to reach the target destination is unknown [2]. Every node from source to destination forward the RREQ packet to their neighboring nodes so that packet reach the desired destination.

The basic difference between AODV and AOMDV is that AOMDV is helpful in computing disjoint and multiple loop free paths .This makes AOMDV much better than AODV.

This paper is divided into 3 parts: first part contains basic information about MANETs and required routing protocols, second includes proposed algorithm and the third part consists of the simulation results.

II. Quality of Service

Various techniques have been surveyed on different routing protocols that support QoS in MANET and affect QoS delivery across the network. QoS consists of DiffServ and IntServ. IntServ are integrated services since they are not scalable so are not used in MANETS. The DiffServ are Differentiated Services works on boundary nodes but MANET is boundary less. So we need to provide proper QoS in MANETs.

III. Proposed Algorithm

In this paper we will discuss about the new proposed algorithm Preemptive AOMDV(PAOMDV). This algorithm is based on 3 main factors priority and bandwidth.

a) Priority Assignment of Nodes

The question here arises is that how to provide priority to the nodes. It's a very simple and important task. The nodes that are new to the network will be given highest priority as the older nodes can lead to deadlock and can lead to low bandwidth.

b) Bandwidth

Suppose we assign by default the bandwidth of network (Bn) =11. So while searching for the route to destination, source node will pass the RREQ message to the neighboring node having bandwidth(Bnn) >=11. As in fig. 1 Source node S has 3 neighbors, if bandwidth from S to node 1 (Bs1)<11, then S will preempt its route and search for new one. Bs2 >11 and Bs3>11 so source has two options to reach the destination.

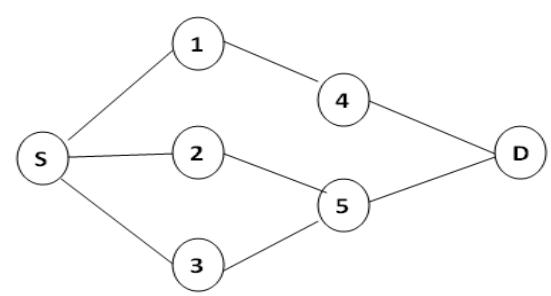


Fig.1: Simple MANET Network

Now S will send RREQ to both node 2 and node 3 and the above process will repeat for both the nodes till the destination is reached.

Author α σ: GZSCCET, MRRSSTU, Bathinda, 151001, India.
e-mails: er.mahak@yahoo.com, param2009@yahoo.com

Global Journal of Computer Science and Technology (E) Volume XVII Issue V Version I Year 2017

c) Preemption

Route is required to be preempted whenever the Bnn< Bn. Thus, selection of route further depends on preemptiveness. The route that is preempted least number of times is the first to be accepted for data transmission. In case nodes are preempted equal number of times then route with minimum hop count is selected. If both are same then any random path is selected.

For this we have added two new fields in the routing table, bandwidth and priority respectively as shown in table1 below:

Table1: Routing Table for the proposed PAOMDV

Dest.	Seq. num	Advertised Hop count	Route list					
			Next_ hop1	Last_ Hop1	Hop_ Count1	Timeout 1	Node_ Bandwith1	Node_ Priority1
			Next_ hop2	Last_ Hop2	Hop_ Count2	Timeout 2	Node_ Bandwith2	Node_ Priority2

i. *Algorithm*

Step 1: Send RREQ from source to sink.

Step 2: If a route exists, add it to the routing table otherwise resend the request.

Step 3: While sending RREQ, keep a check on bandwidth of the requested nodes Bnn and available bandwidth $Bw_{avail.}$

a. If $Bw_{avail} \geq$ Bnn, then pass ahead the RREQ message and record the updated value $Bw_{avail} = Bw_{avail} - Bnn$.
b. Otherwise discard.

Step 4: When destination is discovered, then choose the route with least/ minimum number of preemptions.

Step 5: While sending RREP packet from sink to source node for choosing the path, data regarding number of hop counts and number of preemptions is seen.

a. Least preemptive route is selected, else
b. When preemption is same at all flows then route with minimum hop count is selected, else
c. If both of them are same, then any random path will be selected.

IV. Simulation

The simulation is carried out using Network Simulator 2 (NS2) in two scenarios. Scenario 1 includes 18 nodes whereas scenario 2 includes 25. Results in both scenarios prove that PAOMDV is better than AOMDV.

Table 2: Simulation Parameters

No. of nodes	18
Area	3000m*1000m
Traffic	CBR
Transport Layer	UDP
Motion	Random
Speed	10m/s
Simulation Time	125
Packet Size	520

a) Results and Analysis

Scenario 1: At 18 nodes

Table 3: Simulation Results for AOMDV

Pause Time	Throughput	ETE Delay	PDR
50	49.15	0.00731	1.96
75	53.48	0.00469	2.15
100	65.10	0.00226	2.79
125	67.16	0.00214	2.95

Table 4: Simulation Results for PAOMDV

Pause Time	Throughput	ETE Delay	PDR
50	80.27	0.00617	3.38
75	81.51	0.00171	3.45
100	86.01	0.00064	3.90
125	86.17	0.00076	3.92

Scenario 2: At 25 nodes

Table 5: Simulation Results for AOMDV

Pause Time	Throughput	ETE Delay	PDR
50	88.27	0.00423	3.51
75	87.72	0.00286	3.52
100	91.21	0.00153	3.90
125	92.89	0.00166	4.08

Throughput vs Pause Time: Fig.2 clearly shows that the throughput of PAOMDV is greater than AOMDV. The performance of protocol increases as its throughput increases with time.

Delay vs Pause Time: Fig.3 shows that PAOMDV is better than AOMDV as in modified protocol high priority data goes from shorter path by preempting low priority flow.

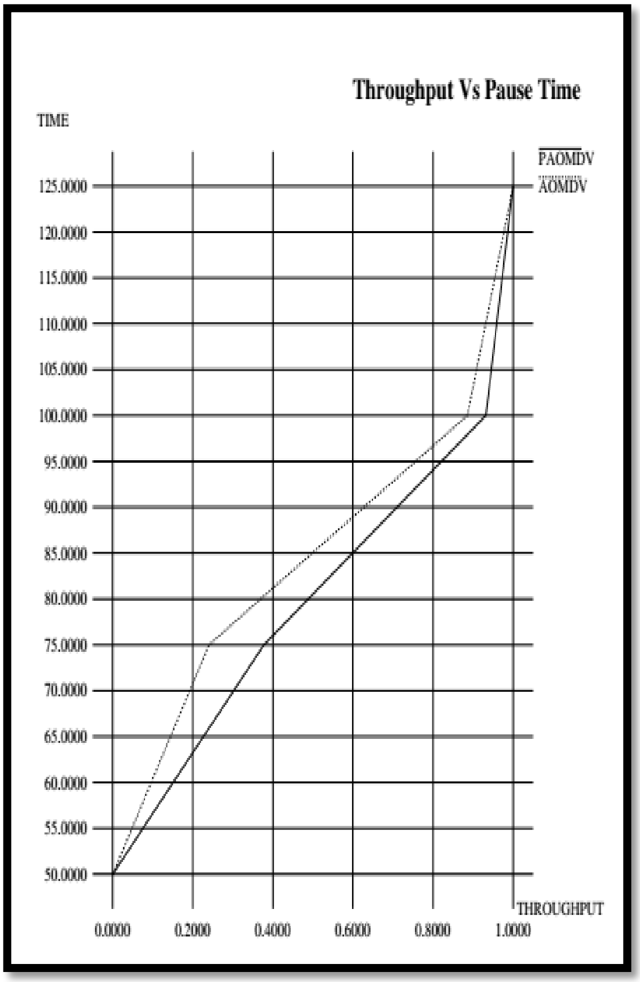


Fig. 2: Throughput vs Pause Time (sec)

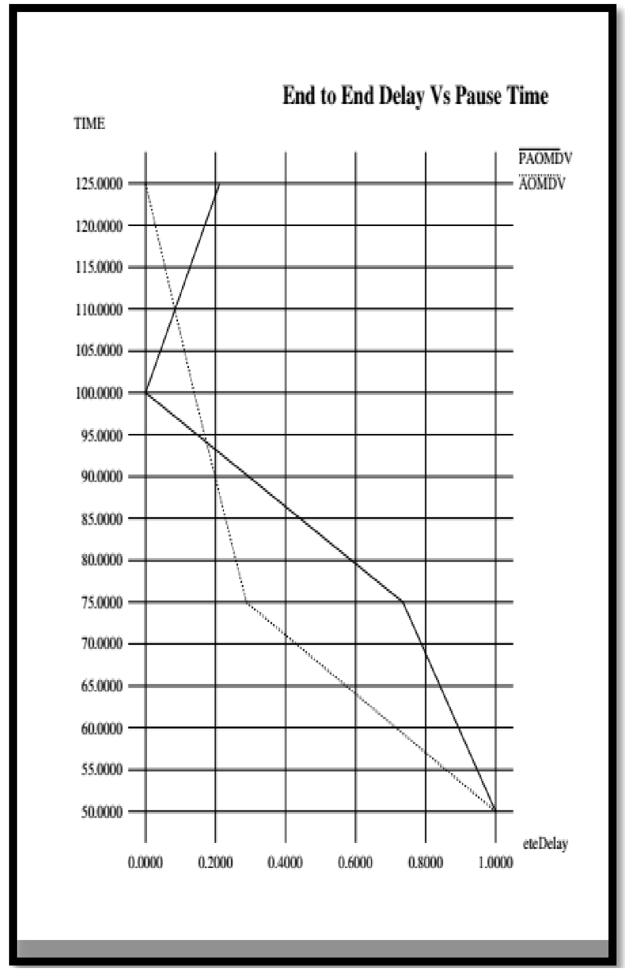


Fig. 3: End to End Delay vs Pause Time(sec)

The fig.4 and fig.5 clearly proves PAOMDV better than AOMDV in both throughput and end to end delay.

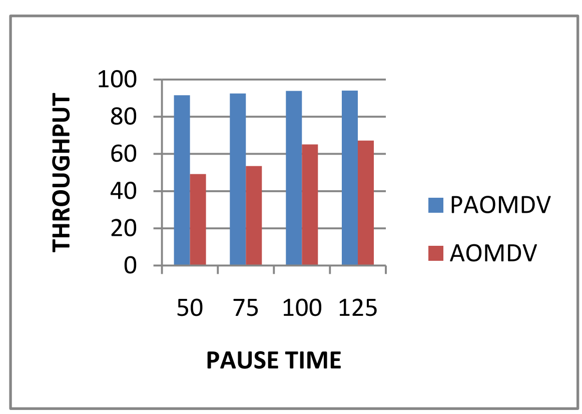


Fig. 4: Throughput vs Pause Time (sec)

Global Journal of Computer Science and Technology (E) Volume XVII Issue V Version I Year 2017

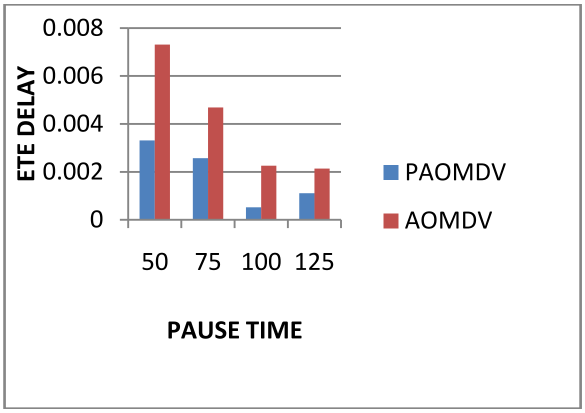


Fig. 5: End to End Delay vs Pause Time (sec)

V. Conclusion

Providing a best QoS from source to destination is the objective of our modified QoS AOMDV protocol called PAOMDV. The constraints are the number of preemption required and maximum priorities using link probability for transmission of data. The study of this scenario has shown comparison of PAOMDV and AOMDV routing protocol is done using the performance metrics like end to end delay, throughput to show that the former outperforms the latter to be better performing protocol.

Références

1. P.PERIYASAMY and E.KARTHIKEYAN, " a Novel Approach To Enhance the Quality of Aomdv Routing Protocol for Mobile Ad Hoc Networks," vol. 69, no.2, pp. 394 404, 2014.
2. N. Tiwari and S. Shibu, "Load Balancing Congestion Control Techniques in Mobile Ad hoc Network : A Survey," vol. 3, no. 2, pp. 2652–2659, 2014.
3. Dr. MadhumitaDash and Mrs Ricky Mohanty, "Quality- Of- Survey Routing Solutions forMobile Ad HocNetworks: A Review," *IOSR J. Electron. Commun. Eng.*, vol. 9, no. 2, pp. 29–36, 2014.
4. K. Fall and K. Varadhan, "The ns Manual (formerly ns Notes and Documentation)" *VINT Proj.*, no. 3, p. 434, 2011.
5. R. Kumar, M. Misra, and A. K. Sarje, "A Proactive Load-Aware Gateway Discovery in Ad Hoc Networks for Internet Connectivity," *Int. J. Comput. Networks Commun.*, vol. 2, no. 5, pp. 120–139, 2010.
6. K. S. Madhusudhananagakumar, Aghila, and G., "A Survey on Black Hole Attack Detection in MANET Using AODV Protocol," *Int. J. Comput. Appl.*, vol. 34, no. 7, pp. 23–30, 2011.
7. A. Modi and D. Rathod, "Improve Performance of AOMDV Protocol in," vol. 1, no. 11, 2015.
8. F. De Rango, P. Fazio, S. Member, and F. Conte, "A New Distributed Application and Network Layer Protocol for VoIP in Hostile Environments."
9. T. B. Reddy, I. Karthigeyan, B. S. Manoj, and C. S. R. Murthy, "Quality of service provisioning in ad hoc wireless networks: A survey of issues and solutions," *Ad Hoc Networks*, vol. 4, no. 1, pp. 83–124, 2006.
10. N. Simulator, "This Installation of Network Simulator 2 on the Ubuntu 16 . 04 Live CD UDisk," 2011.
11. K. N. Sridhar and M. C. Chan, "Channel-aware packet scheduling for MANETs," *2008 IEEE Int. Symp. A World Wireless, Mob. Multimed. Networks, WoWMoM2008*, 2008.
12. P. P. White, "RSVP and integrated services in the internet: A tutorial," *IEEE Commun. Mag.*, vol. 35, no. 5, pp. 100–106, 1997.
13. Seema, Y. Singh, and V. Siwach, "Quality of Service in MANET," *Int. J. Innov. Eng. Technol.*, vol. 1, no. 3, pp. 28–31, 2012.
14. R. Braden, D. Clark, and S. . Shenker, "RFC1633: Integrated Services in the Internet Architecture: an Overview," *IETF RFC 1633, July*, pp. 1–28, 1994.

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 17 Issue 5 Version 1.0 Year 2017
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Effort Expectancy, Performance Expectancy, Social Influence and Facilitating Conditions as Predictors of Behavioural Intentions to use ATMS with Fingerprint Authentication in Ugandan Banks

By Nyesiga Catherine, Dr. Kituyi Mayoka Geofrey, Musa B. Moya & Grace Aballo

Makerere University Business School

Abstract- The purpose of this study was to examine the relationship between Performance Expectancy, Effort Expectancy, Social Influence, Facilitating Conditions and Behavioural intentions to use fingerprint biometrics authentication for ATMs. However much developed countries have adopted and used fingerprint biometrics authentication for ATMs, it is still ignored in undeveloped countries in particular thus the motivation for the study. A cross sectional field survey methodology was used to collect data from 211 ATM users. Quantitative data was collected using self-administered questionnaires from four banks; KCB, Barclays Banks, Stanbic Bank and Centenary Bank from Kampala City in Uganda. The Questionnaire was tested for validity and reliability found out to be valid with CVI above 0.7 and reliable (cronbach alpha>0.6), the data collected was analysed using SPSS. The study used descriptive statistics to examine the relationships.

Keywords: behavioural intentions to use, ATMS, fingerprint authentication.

GJCST-E Classification: C.2.5, C.2.1

Effort Expectancy, Performance Expectancy, Social Influence and Facilitating Conditions as Predictors of Behavioural Intentions to use ATMS with Fingerprint Authentication in Ugandan Banks

Nyesiga Catherine [α], Dr. Kituyi Mayoka Geoffrey [σ], Musa B. Moya [ρ] & Grace Aballo [ω]

Abstract- The purpose of this study was to examine the relationship between Performance Expectancy, Effort Expectancy, Social Influence, Facilitating Conditions and Behavioural intentions to use fingerprint biometrics authentication for ATMs. However much developed countries have adopted and used fingerprint biometrics authentication for ATMs, it is still ignored in undeveloped countries in particular thus the motivation for the study. A cross sectional field survey methodology was used to collect data from 211 ATM users. Quantitative data was collected using self-administered questionnaires from four banks; KCB, Barclays Banks, Stanbic Bank and Centenary Bank from Kampala City in Uganda. The Questionnaire was tested for validity and reliability found out to be valid with CVI above 0.7 and reliable (cronbach alpha>0.6), the data collected was analysed using SPSS. The study used descriptive statistics to examine the relationships. Correlation and regression analysis were also used to determine the relationships between the study variables. The findings of the study indicated that there are significant positive relationships between Performance Expectancy, Effort Expectancy, Social Influence, Facilitating Conditions and Behavioural intentions to use ATMs with fingerprint authentication. Therefore Effort Expectancy, Performance Expectancy, Social Influence and Facilitating conditions are predictors of Behavioural Intentions to Use ATMs with Fingerprint Authentication in Ugandan Banks. The researchers made recommendations that banks should sensitize customers about the benefits of fingerprint biometrics authentication for ATMs, should ensure they implement systems that are secure, easy to use and reliable.

Keywords: behavioural intentions to use, ATMS, fingerprint authentication.

I. Introduction

The introduction of technology such as the ATM has enabled banks to improve service delivery (Olatokun & Igbinedion, 2009). Currently, ATMs are being used to perform a number of functions, ranging from traditional cash dispensing, cash deposits, account transfers, mini statements and even payment of bills. The adoption of ATMs has enabled customers to access their accounts any time and day of the week in the shortest time possible (Das & Jhunu, 2011). However, the ATM has its own limitations (Selvaraju & Sekar, 2010). For example, there are information security flaws are reflected in the form of “ATM frauds” (Adepoju & Alhassan, 2010). The ATM frauds problem is global in nature (Adeoti, 2011) and its consequences have been felt in Uganda as well (Namutebi, 2013). It is estimated that information security attacks have resulted in financial losses to banks (Jain, Prabhakar & Chen, 1999). As the ATM technology is advancing, fraudsters are devising different skills to beat the security of ATM operations. Various forms of fraud are perpetuated, ranging from ATM card theft, skimming, pin theft, card reader techniques and forced withdrawals (Luftman et al, 2006). Managing the risk associated with ATM fraud as well as reducing its impact is an important issue that faces financial institutions as fraud techniques have become more advanced with increased occurrences.

The ATM insecurity situation is not different from Uganda. An increasing number of Ugandans are losing money from their accounts through ATMs (Bank of Uganda, 2015). For example four Bulgarians were convicted for ATM Fraud in Uganda (Kasoma, 2012).Since January 2013 customers' money has been stolen from at least 20 banks through ATM (Chimp reports, 2015). Among these, include Centenary bank, Global Trust, Finance Trust, Stanbic bank, Orient bank, KCB, Barclays among others. Therefore, there is the need to enhance the ATM security system to overcome these challenges by adopting fingerprint based authentication for ATMs. Biometric technology has recently attracted more and more attention as a viable solution to enhancing ATM transaction security (Musleh & Ba, 2012). Given that the process is automated, biometric decision making is very fast, taking only a few seconds in real time in most cases (Emuoyibofarhe et al., 2011). According to Emuoyibofarhe et al. (2011), biometrics could provide a more secure, easier to use alternative to PIN. Ideally, biometrics prove the claimed identity of the card holder, cannot be forgotten, have very high variability and cannot be transferred or stolen.

Author α σ ρ Ѡ: (PhD), Makerere University Business School.
e-mail: cnyesiga@mubs.ac.ug

Biometric systems have replaced card/PIN in many physical access security systems, but do not have widespread use in self-service terminals, particularly ATMs (Pat & Knudsen, 2005).Fingerprint biometrics is a preferred choice for enhancing ATM transaction security. According to Jain (1999), fingerprint biometrics are reliable since majority of the population in the world have fingerprints and every human being has a unique fingerprint, they also require only a small amount of storage and offer more accuracy when compared to other biometrics. Fingerprint acquisition, operations and maintenance are relatively inexpensive in nature, and they are permanent in nature; their characteristics do not change over the course of time. They are formed in the fetal stage and it remains structurally unchanged.

Despite the strengths of fingerprint biometric authentication systems, Ugandan banks are still using the traditional method which is password-based authentication only using cryptographic techniques (BoU Report, 2015; Kasoma, 2012). In a conventional cryptographic system, the user authentication is possession based (BoU Report, 2015). Furthermore, the weakness of such authentication systems cannot assure the identity of the maker of a transaction; it can only identify the maker's belongings (that is cards) or what he remembers (passwords or PINs) (Awotunde, Tolorunloju & Adewunmi-Owolabi, 2014). Therefore, encouraging adoption of fingerprint authentication for ATMS in Uganda remains a virgin research area.

Studies establishing the importance of Effort Expectancy, Performance Expectancy, Social Influence and Facilitating conditions in enhancing technology adoption exist (Venkatesh and Balla, 2008; Chau, Stephens & Jamieson, 2004; Davies, 1989). However, there is no specific research done to encourage adoption of fingerprint authentication for ATMs in Ugandan Banks. Previous literature investigated users' acceptance of E-Health, E learning portals and E-commerce (Harby, Qahwaji and Kamala, 2010) But all these studies seem to overlook the adoption of fingerprint authentication for ATMs which is an increasingly important mechanism to verify user identity in the banking industry. This is basically a knowledge gap that this study intends to fill.

Consequently, the study sought to examine the determinants of behavioral intentions to adopt fingerprint authentication for ATMs based on the unified theory of acceptance and use of technology (UTAUT) proposed by Venkatesh, Morris, Davis and Davis (2003).

This study is significant since it provides critical literature on the influence of Effort Expectancy, Performance Expectancy, Social Influence and Facilitating conditions on bank customers' behavioral intentions to use ATMs with Fingerprint Authentication in Uganda. It has been noted by Parket al.(2007) that there is need to test constructs in the IT adoption and acceptance models in different cultural settings since they play a significant role in impacting IT acceptance.

II. Problem Statement

The security of the current ATM technology in Ugandan banks has been compromised leading to a lot of interest from banks regarding Closed Circuit Television (CCTV) security solutions for ATMs, deploying security guards at ATMs and sensitizing their customers about ATM security (BoU Report, 2015). Despite, these efforts, there have been complaints by users of ATM facilities in banking industry in Uganda on the fraudulent activities being carried out in their accounts that necessitated this study. ATM fraudsters use high-end techniques to rob Ugandans of hard-earned cash (Masaba, 2013). Presently in Uganda, ATM crimes have become a threat not only to customers, but also to bank operators (BoU Report, 2015). Moreover, the security layout of ATMs in Uganda is still at password-based authentication only using cryptographic techniques (BoU Report, 2015; Kasoma, 2012). Furthermore, the weakness of such authentication systems cannot assure the identity of the maker of a transaction; it can only identify the maker's belongings (that is cards) or what he remembers (passwords or PINs) (Awotunde, Tolorunloju & Adewunmi-Owolabi, 2014).Therefore, biometrics-based authentication systems that use physiological and/or behavioral traits are good alternatives to traditional methods. These systems have not been used to enhance ATM security in Uganda banks (BoU Report 2015) yet they are more reliable (biometric data cannot be lost, forgotten, or guessed) and more user-friendly (there is nothing to remember or carry) (Uludag, 2006). Recently, fingerprint authentication is the most popular authentication in developed countries (Ndife et al., 2013). Therefore, it becomes imperative to embrace a more robust technique like fingerprint biometric authentication, that is, to integrate encryption key with fingerprint biometrics for easy identification and authentication of users to reduce the propensity to ATM security limitations in Ugandan banks. Hence the need to examine predictors of Behavioural Intentions to Use ATMs with Fingerprint Authentication in Ugandan Banks.

III. Objectives of the Study

1) To examine the relationship between Performance Expectancy and Behavioural Intention to use fingerprint biometrics based authentication for ATMS in Uganda.
2) To examine the relationship between Effort Expectancy and Behavioural Intention to use fingerprint biometrics based authentication for ATMS in Uganda.
3) To examine the relationship between Social Influence and Behavioural Intention to use

fingerprint biometrics based authentication for ATMS in Uganda.

4) To study the relationship between Facilitating Conditions and and behavioural intention to use fingerprint biometrics based authentication for ATMS in Uganda.

a) Hypothesis

H1: Performance expectancy has a positive influence on the Behavioral intention to use fingerprint-based authentication for ATMs in Uganda.

H2: Effort expectancy has a positive influence on the Behavioral intention to use fingerprint authentication based ATMs in Uganda.

H3: Social influence has a positive influence on the Behavioral intention to use fingerprint-based authentication for ATMs in Uganda.

H4: Facilitating conditions has a positive influence on Behavioral intention to use fingerprint-based authentication for ATMs in Uganda.

IV. Related Literature

a) ATM PIN based Authentication

People use the ATM for transactions such as cash withdrawal, balance inquiry, mini statement and statement request (Emuoyibofarhe et al., 2011). ATM is the most convenient way to access the accounts and funding transactions. According Ravikumar (2013) ATMs have two input devices (a card reader and keypad) and four output devices (display screen, cash dispenser, receipt printer, and speaker). An invisible communications mechanism to the client links the ATM directly to an ATM host network (Thyagarajan, 2006). The ATM functions much like a PC given that it comes with an operating system and specific application software for the user interface and communications (Fengling, Jiankun, Xinhuo, Yong &Jie, 2005).

The ATM uses magnetic strip cards and PINs to identify account holders. The ATM forwards information read from the client's card and the client's request to a host processor, which routes the request to the client's financial institution. If the cardholder is requesting cash, the host processor signals for an electronic funds transfer (EFT) from the customer's bank account to the host processor's account (Leigh, 2013). Once the funds have been transferred, the ATM receives an approval code authorizing it to dispense the cash. This communication, verification, and authorization can be delivered in several ways (Thyagarajan, 2006). Leased line, dial-up, or wireless data links may be used to connect to the host system. In this case, the PIN is an important aspect in protecting an individual's ATM transaction account. This PIN is shared between a user and the system and can be used to authenticate or identify the user to the system (Babatunde & Akinyokun, 2013). Therefore, the ATM system authentication of the customer is based only on the PIN he/she supplies (Ravikumar, 2013).

b) ATM PIN based Limitations

The limitations of the PIN based ATM authorization process include theft, unauthorized access, forgetfulness, card swallowing and damages due to bending (Das & Jhunu, 2011; Sunday, 2012; Akinyemi, Omogbadegun & Oyelami, 2010). The potential for the theft of PIN by unsuspecting criminals is a major disadvantage to the operation of ATM. While fraudsters place card readers, called skimmers, over the authentic reader to transfer numbers and codes, password voyeurs use spy cameras to collect access codes (Babatunde & Akinyokun, 2013). Burglars also use cloning devices to gain access into customer's account. Forgetfulness is mostly experienced when user makes frequent attempts to protect his or her PIN from people's guess and in the process, end up forgetting it (Subh & Vanithaasri, 2012). Occasionally, an ATM may malfunction resulting in swallowing of card, which may pose a number of inconveniences to the user. Damaging may be because of injuries caused to cards in wallets or hip pockets with no adequate attention or care (Babatunde & Akinyokun, 2013).

c) Fingerprint Biometrics as a Means for Enhancing ATM Transaction Security

Among all the biometrics, fingerprint based identification is one of the most mature and proven technique and has been the most widely used during the 20th century. Because fingerprint-based authentication offers several advantages over other authentication methods, there has been a significant surge in the use of finger print biometrics for user authentication in recent years (Akwaja, 2010). At the time of transaction, fingerprint image is acquired at the ATM terminal using high resolution fingerprint scanner. The choice of fingerprint for this research is premised on the fact that it is the most popular biometrics mode for its uniqueness (no two people with identical print) and consistency (it may change in scale but not in relative appearance) (Awotunde, Tolorunloju & Adewunmi-Owolabi, 2014). It also enjoys high availability (it is naturally fixed on all individuals) and universality (possess by every individual irrespective of gender, age or race) (Fatai, Awotunde, & Matluko, 2014; Jeroen, Ileana, Koen & Emile, 2011; Wang, Hu & Phillips, 2007). In addition, fingerprint cannot be forged, stolen, misplaced or forgotten and in cases of damages, it reproduces in short interval of time (Iwasokun, 2012; Iwasokun, Akinyokun, Alese & Olabode, 2012; Fengling, Jiankun, Xinhuo, Yong & Jie, 2005; Das & Jhunu, 2011). Fingerprint technologies are also supported by numerous and existing fast computing devices, high recognition rate and speed, explosive growth of network and Internet transactions and the heightened awareness of the need for ease-of-use as an essential ingredient of reliable security (Babatunde & Akinyokun, 2013).

Fingerprint recognition is an active research area nowadays (Maltoni, Maio, Jain & Prabhakar, 2009). An important component in fingerprint recognition systems is the fingerprint matching algorithm. According to the problem domain, fingerprint matching algorithms are classified in two categories: fingerprint verification algorithms and fingerprint identification algorithms. The aim of fingerprint verification algorithms is to determine whether two fingerprints come from the same finger or not. On the other hand, the fingerprint identification algorithms search a query fingerprint in a database looking for the fingerprints coming from the same finger.

Since security measures at ATM centers play a critical and contributory role in preventing attacks on customers, several authors have used fingerprint to shift from PIN to biometric based security (Kuykendall & Lee, 2003). Das and Jhunu (2011) and Yun and Jia(2010) focused on vulnerabilities and the increasing wave of criminal activities occurring at ATMs and presented a prototype fingerprint authentication for enhancing security. The systems adopt the same measure as the current work by formulating modules for fingerprint enrolment, enhancement, feature extraction and database and matching.

Subh and Vanithaasri (2012) proposed a highly authenticated biometric security system. The work is similar to the current work with its use of conventional fingerprint static points (features and minutiae points) for authentication during ATM access. The static points of fingerprint were considered for increased matching scores against the distortions and non-linear deformations. Consecutive steps processed include preprocessing and key points generation (KPG). KPG is based on the iterative process of evaluating the costs of each fingerprint and iris simultaneously using the cryptosystem features for identification of valid users from the database. The work however lacks the strength to exclude false feature and minutiae points from its extracted list.

Santhi and Kumar (2012) proposed an ATM security enhancing method with secured Personal Identification Image (PII) process. A detailed study on various existing biometric systems is also presented stating the strengths and limitations. In the same manner of the current research, they used the characteristic features of fingerprint to overcome the limitations of the PIN based ATM authentication. However, the proposed method lacks adequate implementation and evaluation to back-up the performance claim. Bhosale and Sawant (2012) and Ibiyemi, Obaje and Badejo (2012) present innovative models for biometric ATMs, which replaces card system with biometric technology. The proposed systems hybridize feature-based fingerprint, iris and PIN to provide reliable and fool-proof ATM authentication.

Singh, Tripathi, Agarwal and Singh (2011), through a formal verification of existing models, have proposed for ATM transaction through fingerprint with the help of Real Time Constraint Notation (RTCN). The technology is related to the current work by utilizing the uniqueness of epidermis of fingers for user's identification. In addition, in a way similar to the current work, the user is expected to keep the finger on a sensory pad, which reads the ridges of epidermis of finger and try to match it with available data of the finger with the bank. The relative advantages of the technology over Sequence Diagrams (SDs), Finite State Machine (FSM) in areas of branching, state information and composing SDs are presented.

d) Predictors of Behavioral Intentions to use ATMs with Fingerprint Authentication

Performance Expectancy: Performance expectancy refers to the extent/degree to which an individual believes that using the system will help him/her to attain gains in job performance (Venkatesh et al. 2003). This factor is similar to perceived usefulness from TAM and is recognized to be a fundamental attribute in influencing individual's attitude towards using any system (Chau, Stephens & Jamieson, 2004). Ho, Stephens & Jamieson (2003) further define performance expectancy as the degree to which a person believes that using a particular biometric system would fulfill the organization's security access requirements in a particular domain. According to Venkatesh et al.'s (2003) studies, Performance expectancy is found to uniquely, significantly and positively influence one's behavioral intension to accept and use an IT system. Performance expectancy can be explained by security (confidentiality, integrity and availability of information used), reliability (the probability that the system remains successful in achieving its intended objectives) and identity assurance (the assurance that only authorized individuals are given access) (Ho et al. 2003). Therefore, in this study security, reliability and identity assurance explained the performance expectancy of the intention to use fingerprint-based authentication.

Effort Expectancy: Venkatesh et al., (2003) define effort expectancy as the level of easiness related while using any system. This means that effort expectancy refers to the effort needed to use the system, whether it is simple or complicated. User-friendly technology could be easily accepted and adopted by users. Most users prefer technology that provide them flexibility, usefulness, and ease of use. According to Giesing (2003) effort expectancy is a factor that is highly significant in influencing intention to use. In the present context, effort expectancy refers to the perception of ease using fingerprint-based authentication in ATMs. Clodfelter (2010) explains that three constructs from the existing models capture the concept of effort expectancy: perceived ease of use (TAM/TAM2), complexity (MPCU), and ease of use (IDT). Ho et al. (2003) say fingerprints are easy to use in authentication since there is no need to remember, hide, replace or repair. Therefore, If users expect ATMs to perform excellently with the fingerprint authentication system, they are more likely to use the system.

Facilitating Conditions: Facilitating conditions are defined as the degree to which an individual perceives that organizational and technical infrastructure exist to support use of the system (Venkatesh et al., 2003). In the context of this study, it referred to the objective factors like infrastructures and resources that influence intention to use fingerprint-based authentication in ATMs. Venkatesh et al (2013) argue that there is a positive relationship between facilitating conditions and behavioral intention to use and adoption of technology. However, the relationship was moderated by Age and experience with the result being stronger for older workers with increasing experience. For the case of this study, people will be willing to use ATMs with fingerprint based authentication if they believe the infrastructure and resources exit to support use of the system.

Social Influence: Social influence is defined as the degree to which an individual perceives that important others (such as relatives, peers and subordinate) believe that he or she should use the new system (Venkatesh et al., 2003). According to Pietro et al. (2012), word of mouth is influenced by reference groups and it includes friends and IT experts, which in turn play a major role in the adoption of communication technologies. Social influence can be either subjective norm, social factors, or image. Image refers to the improvement of solitary image or class in social system using the apparent new system (Venkatesh et al., 2003). Constructs of subjective norms (Ration action theory, planned theory, and decomposed planned theory and Technology acceptance model 2), social factors (PC utilization model) and image (innovation diffusion theory) were influential in formation of the social influence variable (Giesing, 2003). For the case of this study, subjective norm measured social influence. A person's subjective norm is determined by his or her perception that salient social referents think he/she should or should not perform a particular behavior (Ajzen and Fishbein, 1980). A person is motivated to comply with the referents even if he/she does not favour the behaviour. The referents may be superiors like parents, employers or teachers or peers like friends, workmates or classmates. This study considered that most users tend to have their decision making reliant on others' suggestions, therefore social influence should play a more important role. Venkatesh et al. (2003) explains that the relationship between social influence and behavioral intention to use is strong, hence the following hypothesis.

Venkatesh et al. (2003) recommended that future research applies and examines the applicability of the Unified Theory of Adoption and use of Technology (UTAUT) constructs in different contexts hence this study examined the influence of Effort expectancy, Performance expectancy, Social influence and Facilitating conditions on Behavioural intentions to Use which helped to understand the predictors of Behavioural intentions to Use ATMs with Fingerprint Authentication in Ugandan Banks.

Measurement of Variables: The items used to measure performance expectancy, effort expectancy, social influence and behavioural intention were adapted from Venkatesh et al(2003).In the context of this study, factors such as security, reliability and identity assurance were used to measure performance expectancy of the intention to use fingerprint-based authentication as suggested by Ho et al. (2003). Complexity and ease of use were used to measure effort expectancy (Clodfelter, 2010). Social influence variable was measured by subjective norm (Venkatesh et al., 2003) and facilitating conditions was measured by technical infrastructures and resources that encourage the usage of fingerprint-based authentication in ATMs.

V. Methodology

a) *Research Design*

A cross- sectional field survey research design was adopted and thus quantitative research techniques were used during data collection. A cross-sectional field survey research design was used, given that researchers are able to collect data on beliefs, practices or situations from a random sample of subjects in the field using survey questionnaires (Bhattacherjee, 2012). Questionnaires used were tested for reliability and validity before the survey.

b) *Study Population, sample size and Sampling technique*

ATM users were the population for this study. Due to the large sizes of population and limited financial, human and time resource resources, this study was not able to cover all the banks but only used accessible population. This is in line with Amin (2005) definition of accessible population referring to it as the portion of the population to which the researcher has reasonable access. In this study customers of Stanbic Bank, Barclays Bank, KCB and Centenary Bank were the access population. The four banks were selected over the rest considering the maturity of the banks, big numbers of customers, exposure of the customers and the fact that they have faced fraudulent activities. A total of 275 questionnaires were administered to ATM users (respodents) who were selected using convenience sampling from the four banks and 211 questionnaires were returned. This sample is in line with Roscoe's (1970) rule of thumb that states that a sample size between 30 and 500 is sufficient. Data were analyzed and then presented in the tables. The study used descriptive statistics, correlation and regression analyses. According toJanssens et al.(2008), descriptive statistics is important because it provides a simple way of presentation of results, and it is easy to understand the results when presented

c) Validity and reliability tests

Validity tests determine how well a research instrument used measures the concept for which it was intended (Miller, 2010). Content Validity Index was used to test for validity of the questionnaires (Saha, 2008). Two questionnaires were developed with a five point likert scale of Not relevant, Somewhat relevant, Quite relevant, Relevant and Very relevant and distributed to 4 experts to test for content validity. The experts were asked to indicate the extent to which each variable was valid and investigated what they were intended to measure. The result showed a content validity of 0.85 which was an evidence of good content validity according to Polit et al (2007). Whereas reliability tests measure the consistence and stability of a research instrument. Cronbach Alpha Coefficient was used to test for reliability (Carcary, 2008). The researcher used Cronbach Alpha Coefficient (Cronbach, 1951) to measure reliability. Questionnaires were administered to thirty respondents to check for the reliability of the questionnaires. The questionnaire items were analyzed using Cronbach's Alpha reliability test in SPSS software as shown in Table 1

Table 1: Reliability Statistics

Variable	Number of Items	Cronbach's Alpha
Performance Expectancy	3	0.821
Effort Expectancy	4	0.701
Social Influence	4	0.821
Facilitating Condition:	3	0.691
Behavioral Intention	5	0.707

Findings in Table 1 show that all items under each of the variables measured were found to have a coefficient of 0.691 and above which according to Nunnaly (1978) is acceptable in research.

VI. Ethical Considerations

Informed Consent: The researcher ensured prospective research participants were fully informed about the procedures and risks involved in research and they gave their consent to participate.

Respect, confidentiality and privacy: The researcher assured participants of the confidentiality and privacy of the information provided. More to that, participants were not asked to write names on the questionnaires. Research participants were given freedom to choose how much information about themselves they would reveal and under what circumstances. So the researcher was so careful when recruiting participants for a study and only those that were willing were given the questionnaires.

a) Findings

This section entails of the analysis of the data collected on the study variables and the interpretation of the analysis based on the research objectives and questions.

b) Background Characteristics

The background characteristics that were analyzed included; age and level of education.

Age

Table 2: Age of Respondents

Age Groups	Frequency	Percent
18-28 years	81	38.4
29-39 years	72	34.1
40-50 years	54	25.6
Over 51 years	4	1.9
Total	211	100.0

Results in Table 2 show that the respondents in the age category 18-28 years contributed the majority of respondents with (Freq=81, % =38%). This was followed by 29-39 years category with (Frq = 72, % = 34%). 40-50 years category followed with (Freq = 54, % = 25%) while above 51 years category was the last with (Freq = 4, % = 2%)

Academic qualification level of respondents

Table 3: Academic Qualification

Qualification	Frequency	Percent
Certificate	8	3.8
Diploma	31	14.7
Bachelor's degree	108	51.2
Master's degree	43	20.4
Post graduate	21	10.0
Total	211	100.0

The results in Table 3 show that most of the participants (bank customers) in the study (Freq = 108, % = 51%) were bachelor's degree holders. This was followed by those who were master's degree holders (Freq = 43, % = 20%) and diploma had (Freq = 31, % = 15%). Post graduate had (Freq = 21, % = 10%) whereas certificate holders scored less with (Freq = 8, % = 4%).

VII. Descriptive Statistics

a) *Performance Expectancy*

Table 4: Descriptive Statistics for performance expectancy for bank customers

Code		Mean	Std. Deviation	Meaning
PE1	I think a fingerprint authentication for ATM will improve identity assurance	4.4313	.61626	Agree
PE2	I think fingerprint authentication based ATM will be useful in carrying out transactions	4.2322	.69564	Agree
PE3	I think fingerprint authentication based ATM will improve security of money in the system	4.5403	.60320	Agree

Findings in Table 4 show that there are positive perceptions on performance expectancy in regards to PE1 (mean = 4.5403), PE2 (mean = 4.4313) and PE3 (mean = 4.2322). All the means are 4 and above, an indication that performance expectancy influences the adoption and use of biometric fingerprint technology for ATMs in Uganda.

b) *Effort Expectancy*

Table 5: Descriptive Statistics for Effort Expectancy

Code		Mean	Std. Deviation
EE1	I think my interaction with the fingerprint authentication based ATM will be clear and understandable.	4.218	0.71704
EE2	I think the fingerprint authentication based ATM will be easy to use	4.2701	0.80357
EE3	I think learning to operate the fingerprint authentication based ATM will be easy for me.	4.2559	0.73088
EE4	I will not need high effort to use fingerprint authentication based ATM	4.3223	0.77486

Results in Table 5 show that here are positive perceptions on effort expectancy in regard to EE1 (Mean = 4.3223), EE2 (mean = 4.2701), EE3 (Mean = 4.2559) and EE4 (mean = 4.2180). All the means are 4 and above, an indication that effort expectancy influences the adoption and use of biometric fingerprint technology for ATMs in Uganda.

c) *Social influence*

Table 6: Descriptive Statistics for Social Influence

Code	Factor	Mean	Std. Deviation	Meaning
SI1	I think people who are important to me will recommend me to use fingerprint authentication based ATM	3.6398	0.82412	Agree
SI2	I think the use of fingerprint authentication based ATM will elevate my class	3.6682	0.97291	Agree
SI3	I think my peers will expect me to use fingerprint authentication based ATM	3.7014	0.88959	Agree
SI4	I think people who influence my banking behavior will recommend me to use fingerprint authentication based ATM	3.9289	0.88354	Agree

Results in Table 6 show that there are positive perceptions on social influence in regards to SI1 (Mean= 3.9289), SI2 (Mean = 3.7014), SI3 (Mean = 3.6682) and SI4 (Mean = 3.6398). All the means are 3.6 and above, an indication that social influence influences the adoption and use of biometric fingerprint technology for ATMs in Uganda.

d) *Facilitating Conditions*

Table 7: Descriptive Statistics for facilitating conditions

Code	Factor	Mean	Std. Deviation	Meaning
FC1	I think my bank has the hardware and software required for implementation of the fingerprint authentication based ATM	3.5735	0.90399	Agree
FC2	I think my bank has enough money to implement and maintain a fingerprint authentication based ATM	3.8768	0.7892	Agree
FC3	I think my bank has a team in charge of championing Information Technology innovations.	3.9858	0.76519	Agree
FC4	I think a banking policy will be established to encourage use of fingerprint authentication based ATMs.	3.872	0.85508	Agree

Findings in Table7 indicate that there are positive perceptions on facilitating conditions in regards to FC3 (Mean =.3.9858), FC2 (Mean = 3.8768), FC2 (Mean =.3.8720), FC4 (Mean=3.8720) and FC1 (Mean = 3.5735). All the means are 3.5 and above, an indication that facilitating conditions influence the adoption and use of biometric fingerprint technology for ATMs in Uganda.

e) *Behavioural intention to use*

Table 8: Descriptive Statistics for Behavioural intention to use

Code	Factor	Mean	Std. Deviation	Meaning
BI1	I will take time to help others learn how to use fingerprint authentication based ATM	3.6872	0.93441	Agree
BI2	I think fingerprint based authentication will be a basis for future ATMs	4.1991	0.70926	Agree
BI3	I intend to use the fingerprint authentication based ATM in future	4.2986	0.7111	Agree
BI4	I am open to learning how to use fingerprint authentication based ATM	4.4171	0.7148	Agree
BI5	I think fingerprint authentication based ATMs will be interesting to use	4.3412	0.7414	211

Findings in Table 8 show that there are positive perceptions on behavioral intention to adopt in regards to BI4 (Mean = 4.4171), BI5 (Mean = 4.3412), BI3 (Mean = 4.2986), BI3 (Mean = 4.1991) BI1 (Mean = 3.6872). All the means are 3.6 and above an indication that bank customers are willing to use ATMs with fingerprint authentication now and in future and would also recommend and help their friends to use them.

VIII. Normality Test

Normality test of the study variables involved the use of PP plots, QQ plots, and Histogram. The PP and QQ plots showed most of the data points are on and close to the straight line an indication that the study variables were fairly and normally distributed as shown in Figures 1 to 10. The histogram in figure 11 shows that most of the bar charts are within the normal curve, an indication that the data are fairly and normally distributed for all variables being measured.

IX. Relationship between Study Variables

a) *Correlation and Regression*

Hypothesis 1: Results in tables 12 and 13 of correlation and regression outputs indicated a significant positive relationship between Performance Expectancy and Behavioural Intention(Beta = .230** $p < 0.01$, r=.316** $p < 0.01$) to use fingerprint biometrics based authentication for ATMS in Uganda. Therefore, the hypothesis that performance expectancy has a positive influence on the Behavioral intention to use fingerprint-based authentication for ATMs in Uganda was supported.

Hypothesis 2: Results in tables 12 and 13 ofthe correletation and regression outputs indicated a significant positive relationship between Effort Expectancy and Behavioural Intention (Path Beta = .230** P < 0.01, r = 304** p < 0.01) to use fingerprint biometrics based authentication for ATMS in Uganda. Therefore, the hypothesis that effort expectancy has a positive influence on the Behavioral intention to use fingerprint authentication based ATMs in Uganda was accepted.

Hypothesis 3: Results in tables 12 and 13 of the correletation and regression outputs indicated a significant positive relationship between Social Influence and Behavioural Intention (Beta = .153* P < 0.01, r = .271** p < 0.01) to use fingerprint biometrics based authentication for ATMS in Uganda. Therefore, the hypothesis that social influence has a positive influence on the Behavioral intention to use fingerprint-based authentication for ATMs in Uganda was accepted.

Hypothesi 4: Results in tables 12 and 13 of the correletation and regression outputs indicated a significant positive relationship between Facilitating Conditions and and behavioural intention (Beta = .254**, P < 0.01, .387**, p < 0.01) to use fingerprint biometrics based authentication for ATMS in Uganda. Therefore, the hypothesis that facilitating conditions has a positive influence on Behavioral intention to use fingerprint-based authentication for ATMs in Uganda was accepted.

Table 9: Zero order Correlation matrix for the study variables

Variable	PEXP	EEXP	SOINF	FCON	BINT
PEXP	1				
EEXP	0.128	1			
SOINF	0.019	.198**	1		
FCON	.255**	.217**	.284**	1	
BINT	.316**	.304**	.271**	.387**	1

*Source: **. Correlation is significant at the 0.01 level (2-tailed).*

Findings in Table 9 show a significant F value an indication that there is a significant linear relationship between the study variables.

Table 10: Hierarchical multiple linear Regression for Behavioral intention

	Model 1		Model 2		Model 3		Model 4		Model 5	
	B	Beta	B	Beta	B	Beta	B	Beta	B	Beta
Constant	4.207**		2.910**		2.081**		1.651**		1.397**	
Age	-.027	-.051	-.007	-.014	-.030	-.055	-.027	-.050	-.008	-.015
Gender	.023	.025	-.024	-.026	-.044	-.047	-.042	-.046	-.068	-.074
Qualification	.002	.005	-.024	-.049	-.026	-.053	-.019	-.040	-.030	-.063
Bank	.030	.059	.011	.022	-.066	.011	.008	.016	.003	.007
Service duration	-.040	-.075	-.028	-.053	-.032	-.060	-.034	-.663	-.041	-.078
Performance expectancy			.328**	.315**	.288**	.277**	.287**	.276**	.239**	.230**
Effort expectancy					.260**	.285**	.219**	.241**	.187**	.205**
Social influence							.154**	.281**	.108*	.153*
Facilitating conditions									.221**	.254**
R square	.018		.108		.186		.231		.283	
Adjusted R square	-.006		.082		.082		.200		.251	
R square change	.018		.090		.090		.045		.052	
F- Change	.736		20.610		19.402		11.885		14.562	
Sig F Change	.597		.000		.000		.001		.000	
F	.736		4.107		6.610		7.579		8.807	
Sig	.597		.001		.000		.000		.000	

Findings in Table 10 show a significant F value an indication that there is a significant linear relationship between the study variables.

X. Discussion

This study focused on examining factors for adoption of fingerprint based authentication for ATMs in Uganda. Variables of performance expectancy, effort expectancy, social influence, facilitating conditions were identified as factors influencing behavioral intention to use fingerprint based authentication for ATMs in Uganda.

Results from the study indicated that there is a significant positive relationship between Performance Expectancy and Behavioural Intention to use fingerprint biometrics based authentication for ATMS in Uganda. Thus if ATM users believe using an ATM with fingerprint authentication is useful, will improve identity assurance and security of their money while carrying carrying out transactions, it will then improvr thisr behavioral intentions to use.Therefore, the findings coincide with (Ho et al. 2003) who argue that performance Expectancy significantly and positively influences one's behavioral intention to accept and use a system. Venkatesh et al. (2003) also agrees that there is a positive relationship between performance Expectancy and behavioral intention to use. Chua et al., (2004) postulates that performance expectancy factor is similar to perceived usefulness from TAM and is recognized to be a fundamental attribute in influencing individual's attitude towards using any system.

Also results from the study indicated that there is a significant positive relationship between Effort Expectancy and Behavioural Intention to use fingerprint biometrics based authentication for ATMS in Uganda. This implied if people believe that interaction with the fingerprint authentication based ATM will be clear and understandable and easy to use, it will improve their behavioral intentions to use. This is in line with Giesing (2003) who posits that effort expectancy is a factor that is highly significant in influencing behavioral intention to use. Clodfelter (2010) also explains that the extent to which an individual perceives the system to be easy to use has been found to significantly affect intention to use. Venkatesh et al., (2003) and Ho et al., (2003) also explain that there is a positive relationship between effort expectancy and behavioral intention to use.

Thirdly, results suggested a significant positive relationship between Social Influence and Behavioural Intention to use fingerprint biometrics based authentication for ATMS in Uganda. This implies that if ATM users believe that people who are important to them will recommend them to use fingerprint authentication based ATM, use of fingerprint authentication based ATM will elevate their class and peers will expect them to use fingerprint authentication based ATM it will will improve their Behavioural Intentions to use. This is in agreement with an argument by Venkatesh et al. (2003) that the relationship between social influence and behavioral intention to use is strong. Pietro et al. (2012) argue that person's subjective norm is determined by his or her perception that salient social referents think he/she should or should not perform a particular behavior. Also Giesing (2003) explains that social influence influences behavioral intention to use.

Finally, results from the previous chapter indicated that there is a significant positive relationship between Facilitating Conditions and behavioural intention to use fingerprint biometrics based authentication for ATMS in Uganda. Thus it seems necessary to provide required resources, information and also continous support to encourage users. The findings of this study concur with Venkatesh et al., (2003) who argue that there is a significant positive relationship between facilitating conditions and behavioral intention to use a certain system. Venkatesh et al. (2003) also explain that there is positive relationship between facilitating conditions and behavioral intention to use.

The study's theoretical contribution is that it provides critical literature on the influence of performance expectancy, effort expectancy, social influence and facilitating conditions on bank clients' behavioral intentions to use ATMs with fingerprint authentication. To the practitioners, the study provides recommendations on how to enhance ATM users' behavioral intentions to use ATMs with fingerprint authentication.

XI. Conclusion

The study established positive relationships between performance expectancy, effort expectancy, social influence, facilitating conditions and behavioral intention to use ATMs with fingerprint biometric based authentication. This is an indication that performance expectancy, effort expectancy, social influence, facilitating conditions have the ability to influence ATM users' behavioral intentions to use ATMs with fingerprint authentication.

XII. Recommendations

Banks should implement fingerprint based authentication systems for ATMs that improve identity assurance, reliability (up all the times customers need to access their money) and secure so that customers will be willing to use them hence high rates of adoption. More to that, Banks should also make sure they implement fingerprint biometrics based authentication systems for ATMs that are user friendly in order to improve ease of use of ATMs with fingerprint biometric based authentication since users are more willing to easy systems. Finally, Facilitating conditions such information, continued support, right hardware and software should be purchased and put in place by banks in order to encourage use ATMs with fingerprint authentication. More to that, clients should be sensitized on how to use those systems

XIII. Limitation of the Study

Considering that data was mostly collected from banks, the researcher faced a problem of people fearing to share information. However, this was solved by the researcher seeking permission from management and explaining to the respondents the purpose of the information they provided.

XIV. Areas of Further Research

Future researchers should consider studying the role played by the moderating factors: Gender, Age, Experience and Voluntariness while studying factors for adoption of fingerprint based authentication for ATMs.

This research only put into consideration Barclays, KCB, Stanbic and Centenary banks in Kampala City, future research should also bring more banks on board considering all the regions in Uganda.

References Références Referencias

1. Adeoti, J. O. (2011). Automated Teller Machine (ATM) Frauds in Nigeria: The Way Out. *Journal of Social Science, 27*(1): 53-58.
2. Adepoju, A. S. & Alhassan, M. E. (2010).Challenges of Automated Teller Machine (ATM) Usage and Fraud Occurrences in Nigeria - A Case Study of Selected Banks in Minna Metropolis.
3. Ajzen, I. and Fishbein, M. (1980). Understanding Attitudes and Predicting Social Behavior, Engle wood Cliffs, *New Jersey: Prentice Hall.*
4. Awotunde, J. B., Tolorunloju, J. R. & Adewunmi-Owolabi, F. T. (2014). Fingerprint Authentication System: Toward Enhancing ATM Security. *International Journal of Applied Information Systems (IJAIS),* Vol. 7, No.7, 27-32.
5. Bank of Uganda (2015). Bank Fraud - A Challenge to Uganda's Banking Industry. Kampala: *Bank of Uganda.*
6. Chau, A., Stephens, G. and Jamieson, R. (2004) "Biometrics Acceptance –Perceptions of Use of Biometrics", 2004. *Australasian Conferenceson Information Systems (ACIS)*, paper 28.
7. Chipreports (2015). Uganda ATM Fraud Sends Customers Over .The Edge. Retrieved 18 July 2015 from http://chimpreports.com/11328-uganda-atm-fraud-sends-customers-over-the-edge/
8. Cronbach, L., J. (1951). "Coefficient alpha and the internal structure of tests". *Psychometrika*16 (3): 297–334.
9. Das, S. S. & Jhunu, D. (2011).Designing a biometric strategy (fingerprint) measure for enhancing ATM security in Indian e-banking system. *International Journal of Information and Communication Technology Research*, 197-203.
10. Davis, D. (1989). "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology", *MIS Quarterly*, Vol. 13, No. 3, pp. 319-340.
11. Emuoyibofarhe, O. J., Fajuyigbe, O., Emuoyibofarhe, O. N. & Alamu, F. O. (2011).A Framework for the Integration of Biometric In to Nigerian Banking ATM System. *International Journal of Computer Applications*, Volume 34– No. 4, 0975–8887.
12. Fatai, O. W., Awotunde, J. B. & Matluko, O. E (2014). A novel system of fingerprint recognition approach for immigration control, *IOSR Journal of Computer Engineering (IOSR-JCE) 2278-8727*, Vol. 16, Issue 3, Ver. III (May-Jun. 2014), 39-42.
13. Giesing, I. (2003)."User Perceptions Related To Identification Through Biometrics Within Electronic Business". *Master's Thesis*. South Africa: University of Pretoria.
14. Ho, G., Stephens, G. and Jamieson, R. (2003) "Biometric Authentication Adoption issues". *Australasian Conference on Information Systems*, pp. 1-12.
15. Jain, A. K., Prabhakar, S. & Chen, S. (1999). Combining multiple matchers for a high security Fingerprint verification system. *Pattern Recognition Letters, 20*, 1371-1379.
16. Jain, A., Maltoni, D., Maio, D., & Wayman, J. (2005). Biometric Systems Technology, Design and Performance Evaluation. London: Spring Verlag.
17. Kasoma, A. (2012). ATM fraud: Is your money safe? The Independent, Retrieved 18 July 2015 from http://www.independent.co.ug/business/business-news/ 6437-atm-fraud-is-your-money safe.#sthash.
18. Luftman, J., Kempaiah, R. & Nash, E. (2006). Key issues for IT executives 2005. *MIS Quarterly Executive, 5*(2): 81–99.
19. Miller E. J. (2006). Participatory Design Methods for C2 Systems, Air Force Research Laboratory/HECS.
20. Musleh, M. M. M. & Ba, I. I. (2012). Improving information security in e-banking by using biometric fingerprint: A case of major bank in Malaysia, *International Journal of Computer Science and Information Security*, Vol. 10, No. 3, March 2012, 7.
21. Namutebi, V. M. (2013). Automated Banking Systems and Customer Satisfaction: A Case Study of Stanbic Bank, Charm Towers Branch. A research report submitted in partial fulfillment of the requirement for the award of the Degree of Bachelor of Commerce, *Makerere University.*

22. Ndife, A., Ifesinachi, E. O., Okolibe, A. U. & Nnanna, D. K. (2013). An enhanced technique in ATM risk reduction using automated biometrics fingerprint in Nigeria. *International Journal of Scientific Engineering and Technology*, November 2012, No. 2, Issue No. 111132-1138.
23. Nunnaly, J. (1978). Psychometric theory. *New York: McGraw-Hill.*
24. Olatokun, W. M. & Igbinedion, L. J. (2009). The Adoption of Automatic Teller Machines in Nigeria: An Application of the Theory of Diffusion of Innovation. *Issues in Informing Science and Information Technology*, Vol. 6, 373-393.
25. Selvaraju, N. & Sekar, G. (2010), A method to improve the security level of ATM banking systems using AES algorithm, *International Journal of Computer Applications*. June 2010 Vol. 3 No. 6.
26. Uludag, U. (2006). *Secure Biometric Systems*. A Dissertation Submitted to Michigan State University in partial fulfillment of the requirements for the degree of Doctor of Philosophy, Computer Science & Engineering.
27. Venkatesh, V., James Y. L. and Thong X, X. (2012). Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and use of Technology. *MIS Quarterly.*
28. Venkatesh, V., Morris, M.G., Davis, G.B. & Davis, D.F. (2003). "User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly,* Vol. 27, No. 3, pp. 425-478.

Appendices

PP Plots

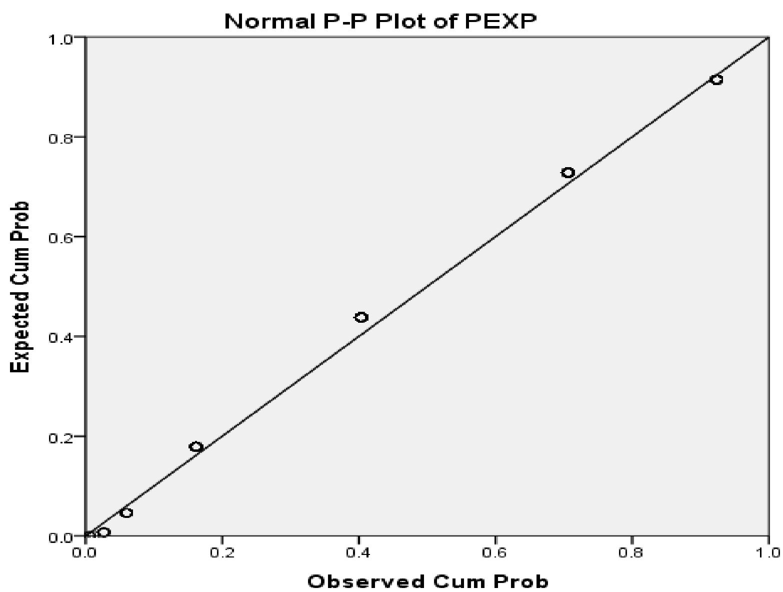


Figure 1: PP Plot for Performance Expectancy

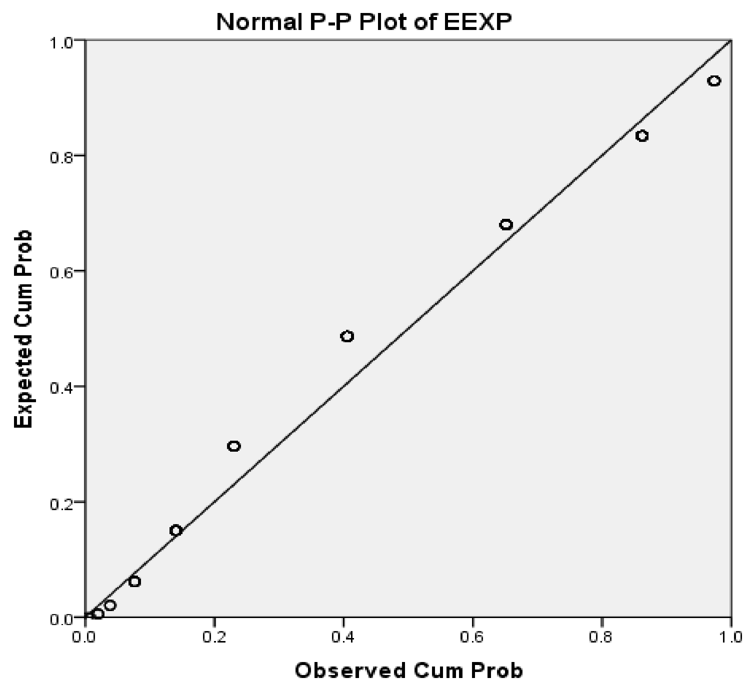


Figure 2: PP Plot for Effort Expectancy

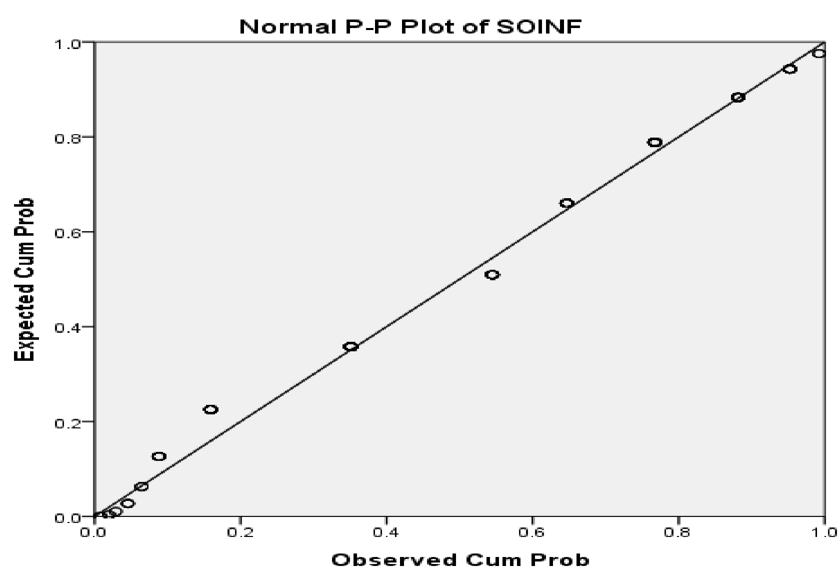


Figure 3: PP Plot for Social Influence

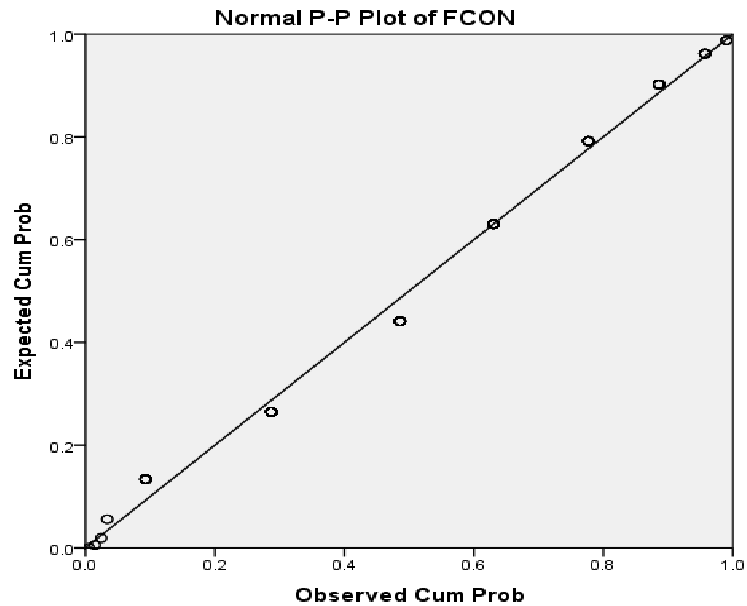


Figure 4: PP Plot for Facilitating Conditions

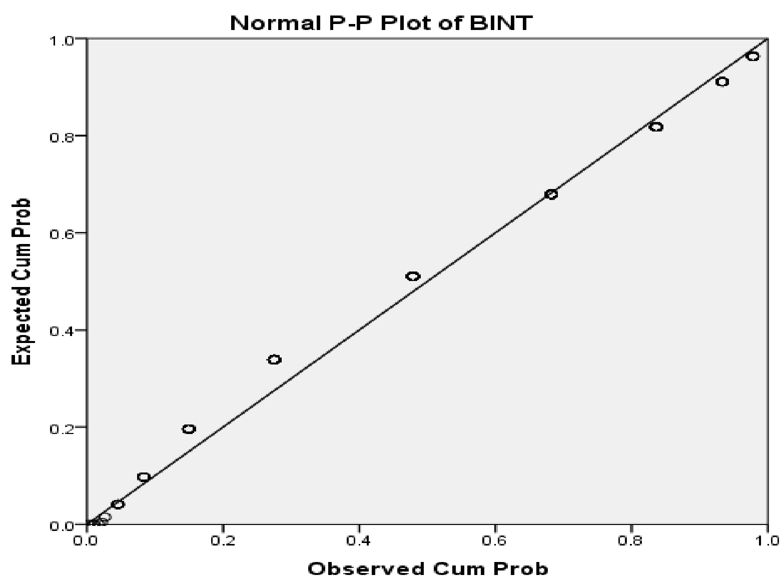


Figure 5: PP Plot for Behavioral Intention to use

QQ Plots

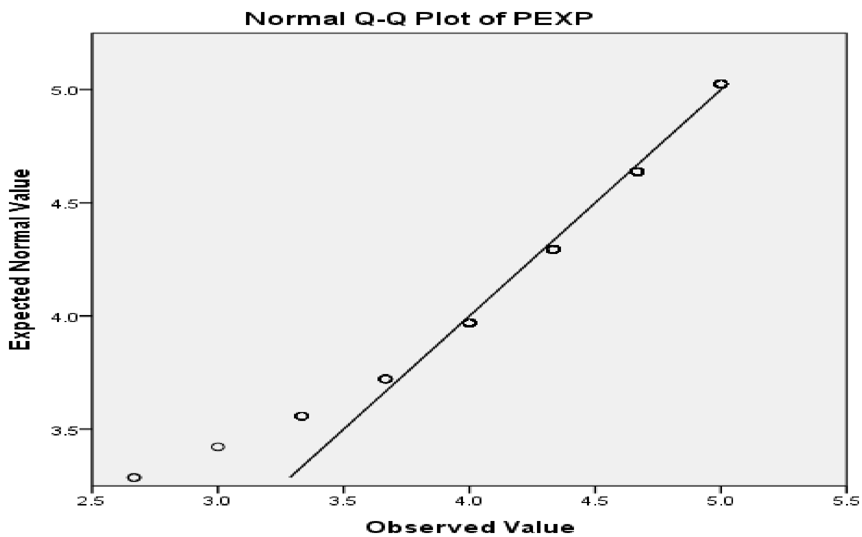


Figure 6: QQ Plots for Performance Expectancy

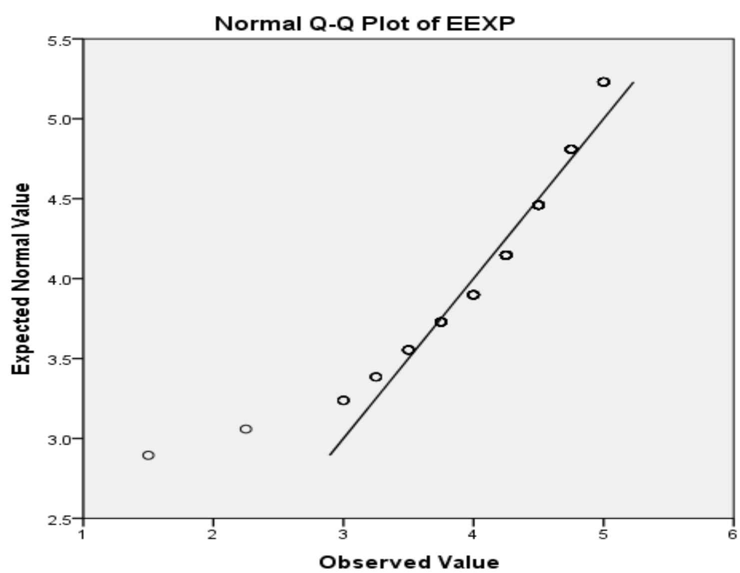


Figure 7: QQ Pots for Effort Expectancy

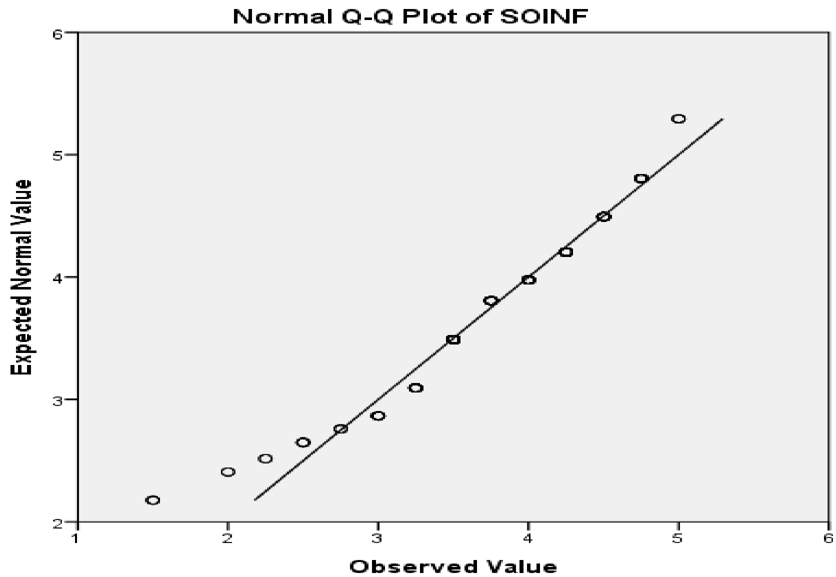


Figure 8: QQ Plot for Social Influence

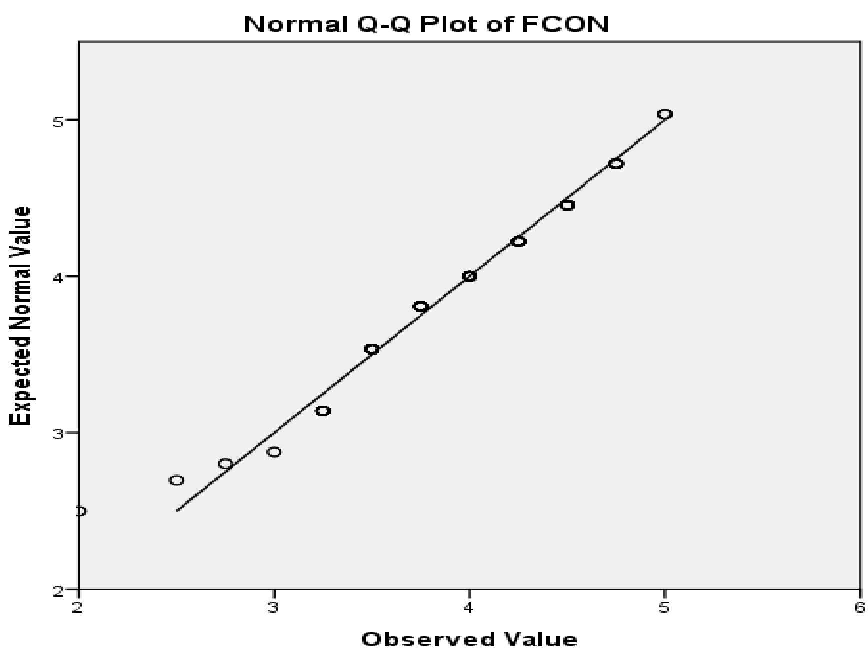


Figure 9: QQ Plot for Facilitating Conditions

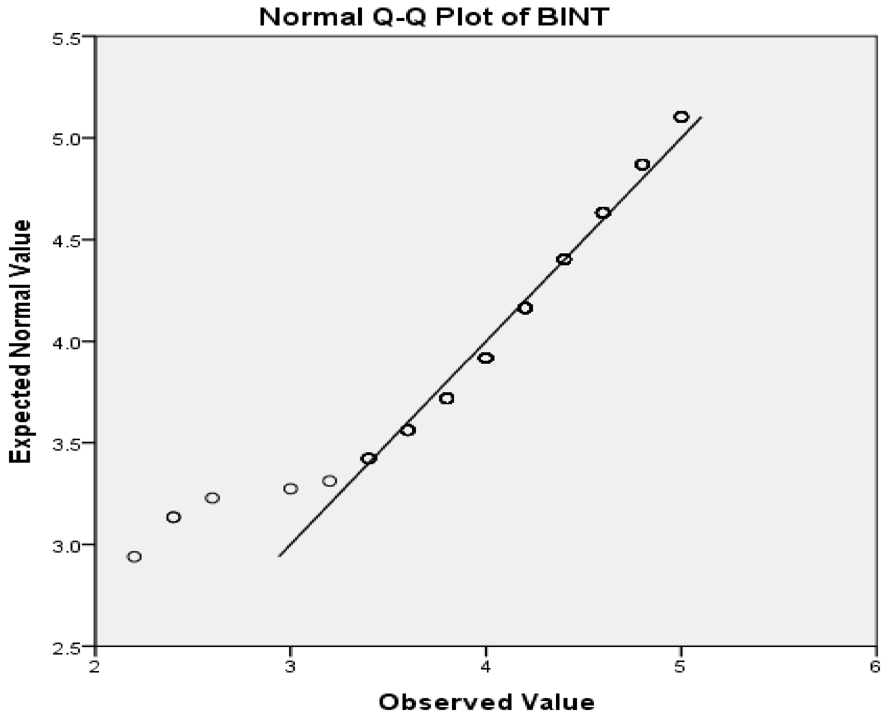


Figure 10: QQ Plot for Behavioral Intention

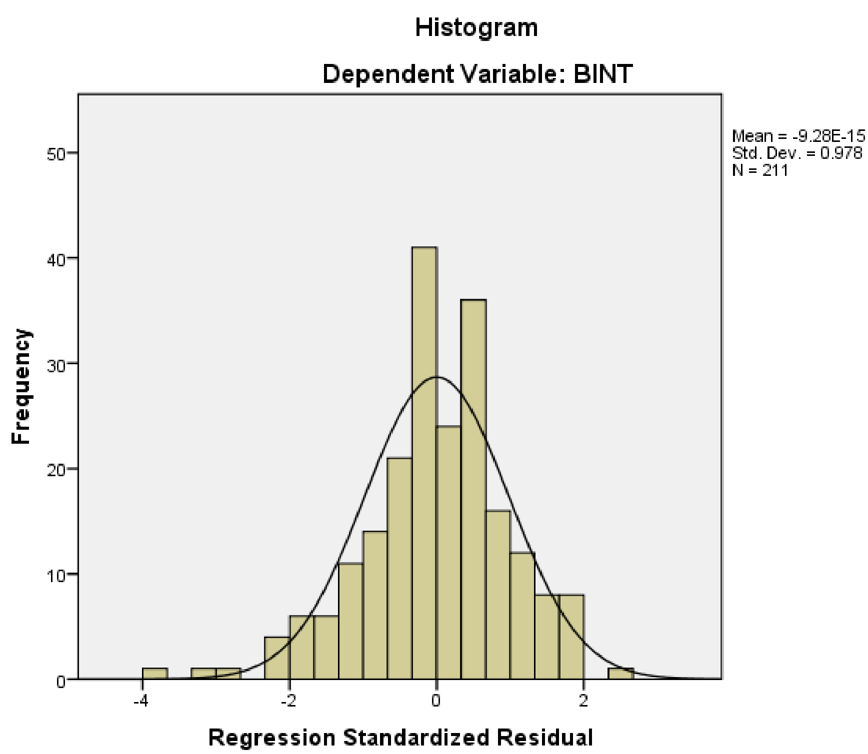


Figure 11: Histogram for Behavioral intentions to use

This page is intentionally left blank

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 17 Issue 5 Version 1.0 Year 2017
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Understanding Network Routing Problem and Study of Routing Algorithms and Heuristics through Implementation

By Saumya Shandilya
Symbiosis Institute of Technology

Abstract- In this project, we intend to identify, understand and compare various routing algorithms used in real world networks. The various objectives of this research are:

1. Define and understand the concepts of routing.
2. Determine if a Greedy or Dynamic Programming strategy algorithm is more efficient for routing, in general. Identify which strategy is used more in real world networks.
3. Identify the common routing algorithms used in networks. Identify which algorithms are used in which scenarios.
4. Identify the performance metrics for gauging algorithms.
5. Compare existing routing algorithms in various scenarios (on the simulation software). Also note specific phenomena or anomalies during simulation.
6. Think of modifications (if any) in existing routing algorithms, or devise a new routing algorithm.

Keywords: routing, throughput, latency, greedy strategy, dynamic programming.

GJCST-E Classification: B.7.2, C.2.2

UNDERSTANDINGNETWORKROUTINGPROBLEMANDSTUDYOFROUTINGALGORITHMSANDHEURISTICSTHROUGHIMPLEMENTATION

Strictly as per the compliance and regulations of:

Understanding Network Routing Problem and Study of Routing Algorithms and Heuristics through Implementation

Saumya Shandilya

Abstract- In this project, we intend to identify, understand and compare various routing algorithms used in real world networks.

The various objectives of this research are:

1. Define and understand the concepts of routing.
2. Determine if a Greedy or Dynamic Programming strategy algorithm is more efficient for routing, in general. Identify which strategy is used more in real world networks.
3. Identify the common routing algorithms used in networks. Identify which algorithms are used in which scenarios.
4. Identify the performance metrics for gauging algorithms.
5. Compare existing routing algorithms in various scenarios (on the simulation software). Also note specific phenomena or anomalies during simulation.
6. Think of modifications (if any) in existing routing algorithms, or devise a new routing algorithm.

Keywords: routing, throughput, latency, greedy strategy, dynamic programming.

I. Introduction

The transport layer provides communication service between two processes running on two different hosts. In order to provide this service, the transport layer relies on the services of the network layer, which provides a communication service between hosts. In particular, the network-layer moves transport-layer segments from one host to another. At the sending host, the transport layer segment is passed to the network layer. In order to this, the network layer requires the coordination of each and every host and router in the network. In simple terms, if we have to define Routing in a lay man's language we can simply say that Routing is the manner/order in which we decide the path a segment shall follow from the sending host to the receiving one. This path includes a connection of links and routers. In technical terms though routing is a complex yet challenging concept.

Technically, Routing broadly consists of the following 3 functions:

1. *Path Determination:* This function determines the path/route the packets will follow from the sender to receiver. It involves various routing algorithms which are discussed further.
2. *Switching:* When a packet arrives at a router it needs to be further dispatched to other routers i.e. it is further switched to other routers.
3. *Call Setup:* Just like a TCP carries out 3 -way handshake similarly some network layer architectures (e.g., ATM) requires that the routers along the chosen path from source to destination handshake with each other in order to setup state before data actually begins to flow. In the network layer, this process is referred to as call setup.

The main goals of routing are:

Correctness: The routing should be done properly and correctly so that the packets may reach their proper destination.

Simplicity: The routing should be done in a simple manner so that the overhead is as low as possible. With increasing complexity of the routing algorithms the overhead also increases.

Robustness: Once a major network becomes operative, it may be expected to run continuously for years without any failures. The algorithms designed for routing should be robust enough to handle hardware and software failures and should be able to cope with changes in the topology and traffic without requiring all jobs in all hosts to be aborted and the network rebooted every time some router goes down.

Stability: The routing algorithms should be stable under all possible conditions.

Fairness: Every node connected to the network should get a fair chance of transmitting their packets. This is generally done on a first come first serve basis.

Optimality: The routing algorithms should be optimal in terms of throughput and minimizing mean packet delays. Here there is a trade-off and one has to choose depending on his suitability.

Author: Computer Science Department, Symbiosis Institute of Technology, Bachelors of Engineering in Computer Science.
e-mail: saumyanda@gmail.com

Global Journal of Computer Science and Technology (E) Volume XVII Issue V Version I Year 2017

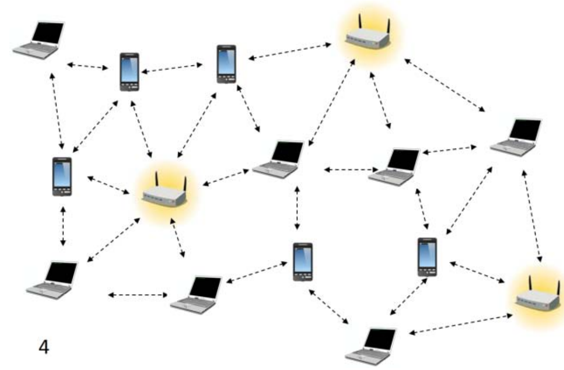


Fig. 1: Connected devices through routers

Routing is performed for many kinds of networks, including the telephone network (circuit switching), electronic data networks (such as the Internet), and transportation networks. This article is concerned primarily with routing in electronic data networks using packet switching technology. In packet switching networks, routing directs packet forwarding (the transit of logically addressed network packets from their source toward their ultimate destination) through intermediate nodes. Intermediate nodes are typically network hardware devices such as routers, bridges, gateways, firewalls, or switches. General purpose computers can also forward packets and perform routing, though they are not specialized hardware and may suffer from limited performance. The routing process usually directs forwarding on the basis of routing tables, which maintain a record of the routes to various network destinations. Thus, constructing routing tables, which are held in the router's memory, is very important for efficient routing. Most routing algorithms use only one network path at a time. Multipath routing techniques enable the use of multiple alternative paths. In case of overlapping/equal routes, algorithms consider the following elements to decide which routes to install into the routing table (sorted by priority):

Prefix-Length: where longer subnet masks are preferred (independent of whether it is within a routing protocol or over different routing protocol).

Metric: where a lower metric/cost is preferred (only valid within one and the same routing protocol).

Administrative Distance: where a route learned from a more reliable routing protocol is preferred (only valid between different routing protocols).

II. Research Elaboration

a) Algorithmic strategies used in routing

1. Brute force algorithm
2. Greedy strategy
3. Dynamic programming
4. Backtracking
5. Branch and Bound
6. Divide and Conquer
7. Decrease and Conquer
8. Transfer and Conquer

b) Types of Routing Algorithms

i. *Link state routing*

Link-state routing protocols are one of the two main classes of routing protocols used in packet switching networks for computer communications, the other being distance-vector routing protocols. Examples of link-state routing protocols include open shortest path first (OSPF) and intermediate system to intermediate system (IS-IS).The link-state protocol is performed by every switching node in the network (i.e., nodes that are prepared to forward packets; in the Internet, these are called routers). The basic concept of link-state routing is that every node constructs a map of the connectivity to the network, in the form of a graph, showing which nodes are connected to which other nodes. Each node then independently calculates the next best logical path from it to every possible destination in the network. The collection of best paths will then form the node's routing table. This contrasts with distance-vector routing protocols, which work by having each node share its routing table with its neighbours. In a link-state protocol the only information passed between nodes is connectivity related.

Strategy used: Greedy programming, generally a variant of Dijkstra's algorithm is used.

ii. *Distance vector routing*

In computer communication theory relating to packet-switched networks, a distance-vector routing protocol is one of the two major classes of intra domain routing protocols, the other major class being the link-state protocol.

Distance-vector routing protocols use the Bellman–Ford algorithm, Ford–Fulkerson algorithm, or DUAL FSM (in the case of Cisco Systems's protocols) to calculate paths. A distance-vector routing protocol requires that a router inform its neighbors of topology changes periodically. Compared to link-state protocols, which require a router to inform all the nodes in a network of topology changes, distance-vector routing protocols have less computational complexity and message overhead. The term distance vector refers to the fact that the protocol manipulates vectors (arrays) of distances to other nodes in the network. The vector distance algorithm was the original ARPANET routing algorithm and was also used in the internet under the name of RIP (Routing Information Protocol).Examples of distance-vector routing protocols include RIPv1 and IGRP.

Strategy used: Dynamic programming, generally bellman ford algorithm.

c) Common Routing Algorithms

The shortest paths are calculated using suitable algorithms on the graph representations of the networks. Let the network be represented by graph G (V, E) and let the number of nodes be 'N'. For all the algorithms discussed below, the costs associated with the links are assumed to be positive. A node has zero cost w.r.t itself. Further, all the links are assumed to be symmetric, i.e. if di,j = cost of link from node i to node j, then d i,j = d j,i . The graph is assumed to be complete. If there exists no edge between two nodes, then a link of infinite cost is assumed. The algorithms given below find costs of the paths from all nodes to a particular node; the problem is equivalent to finding the cost of paths from a source to all destinations.

d) Bellman-Ford Algorithm

This algorithm iterates on the number of edges in a path to obtain the shortest path. Since the number of hops possible is limited (cycles are implicitly not allowed), the algorithm terminates giving the shortest path.

Notation:

d i,j = Length of path between nodes i and j, indicating the cost of the link.
h = Number of hops.
D[i,h] = Shortest path length from node i to node 1, with upto 'h' hops.
D[1,h] = 0 for all h.

Algorithm:

Initial condition: D[i, 0] = infinity, for all i (i != 1)

Iteration: D[i,h+1]=min {di, j+ D [j, h]}over all values of j

Termination: The algorithm terminates when

D[i, h] = D [i, h+1] for all i .

Principle:

For zero hops, the minimum length path has length of infinity, for every node. For one hop the shortest-path length associated with a node is equal to the length of the edge between that node and node 1. Hereafter, we increment the number of hops allowed, (from h to h+1) and find out whether a shorter path exists through each of the other nodes. If it exists, say through node 'j', then its length must be the sum of the lengths between these two nodes (i.e. di, j) and the shortest path between j and 1 obtainable in upto h paths. If such a path doesn't exist, then the path length remains the same. The algorithm is guaranteed to terminate, since there are utmost N nodes, and so N-1 paths. It has time complexity of O (N3).

i. *Dijkstra's Algorithm*

Notation:

Di = Length of shortest path from node 'i' to node 1.
di,j = Length of path between nodes i and j .

Algorithm:

Each node j is labeled with Dj, which is an estimate of cost of path from node j to node 1. Initially, let the estimates be infinity, indicating that nothing is known about the paths. We now iterate on the length of paths, each time revising our estimate to lower values, as we obtain them. Actually, we divide the nodes into two groups; the first one, called set P contains the nodes whose shortest distances have been found, and the other Q containing all the remaining nodes. Initially P contains only the node 1. At each step, we select the node that has minimum cost path to node 1. This node is transferred to set P. At the first step, this corresponds to shifting the node closest to 1 in P. Its minimum cost to node 1 is now known. At the next step, select the next closest node from set Q and update the labels corresponding to each node using: Dj = min [Dj, Di + dj, i]. After N-1 iterations, shortest paths for all nodes are known, and the algorithm terminates after completing these many iterations.

Principle:

Let the closest node to 1 at some step be i. Then i is shifted to P. Now, for each node j, the closest path to 1 either passes through i or it doesn't. In the first case Dj remains the same. In the second case, the revised estimate of Dj is the sum Di + di,j . So we take the minimum of these two cases and update Dj accordingly. As each of the nodes get transferred to set P, the estimates get closer to the lowest possible value. When a node is transferred, its shortest path length is known. So finally all the nodes are in P and the Dj 's represent the minimum costs. The algorithm is guaranteed to terminate in N-1 iterations and its complexity is O(N2).

e) The Floyd Warshall Algorithm

This algorithm iterates on the set of nodes that can be used as intermediate nodes on paths. This set grows from a single node (say node 1) at start to finally all the nodes of the graph. At each iteration, we find the shortest path using given set of nodes as intermediate nodes, so that finally all the shortest paths are obtained. It is observed that all the three algorithms mentioned above give comparable performance, depending upon the exact topology of the network.

III. Results and Findings

a) Performance metrics for comparision

Router metrics are metrics used by a router to make routing decisions. It is typically one of many fields in a routing table. Metrics are used to determine whether one route should be chosen over another.

The routing table stores possible routes, while link-state or topological databases may store all other information as well. For example, Routing Information Protocol uses hopcount (number of hops) to determine the best possible route. The route will go in the direction of the gateway with the lowest metric. The direction with the lowest metric can be a default gateway.

Router metrics can contain any number of values that help the router determine the best route among multiple routes to a destination. A router metric typically based on information like path length, bandwidth, load, hop count, path cost, delay, Maximum Transmission Unit (MTU), reliability and communications cost.

A Metric can include:

1. measuring link utilization (using SNMP)
2. number of hops (hop count)
3. speed of the path
4. packet loss (router congestion/conditions)
5. latency (delay)
6. path reliability
7. path bandwidth
8. throughput [SNMP - query routers]
9. load
10. MTU

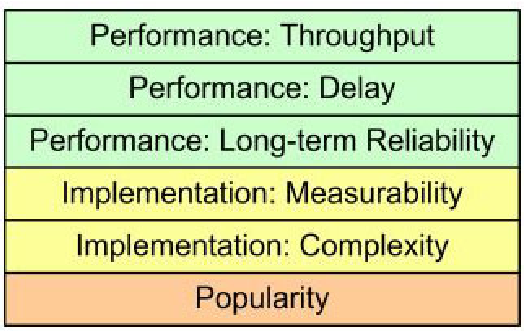


Fig. 2: Six network evaluation criteria

Throughput: In general terms, throughput is the rate of production or the rate at which something can be processed. When used in the context of computer networking, such as Ethernet or packet radio, throughput or network throughput is the rate of successful message delivery over a communication channel. The data these messages belong to may be delivered over a physical or logical link or it can pass through a certain network node/router. Throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second (p/s or pps).The system throughput or aggregate throughput is the sum of the data rates that are delivered to all terminals in a network. It can be analyzed mathematically by applying the queueing theory, where the load in packets per time unit is denoted as the arrival rate (λ), and the throughput, in packets per time unit, is denoted as the departure rate (μ).

Goodput: In computer networks, good put is the application level throughput, i.e. The number of useful information bits delivered by the network to a certain destination per unit of time. The amount of data considered excludes protocol overhead bits as well as retransmitted data packets. This is related to the amount of time from the first bit of the first packet sent (or delivered) until the last bit of the last packet is delivered. For example, if a file is transferred, the good put that the user experiences corresponds to the file size in bits divided by the file transfer time. The good put is always lower than the throughput (the gross bit rate that is transferred physically), which generally is lower than network access connection speed.

Network Latency: Network latency in a packet-switched network is measured either one-way (the time from the source sending a packet to the destination receiving it), or round-trip delay time (the one-way latency from source to destination plus the one-way latency from the destination back to the source). It further consists of the processing delay, queuing delay and transmission delay. The processing delay is basically the time a sender host takes to process a packet and identify the router. Once the router is identified, queuing delay is encountered when a packet has to wait in the queuing buffer before it is transferred further. Transmission delay consists of the time to transmit the packet over the link.

Link Capacity: The term link capacity defines the net bit rate (aka. Peak bit rate, information rate, or physical layer useful bit rate), or the maximum throughput of a logical or physical communication path in a digital communication system. For example, bandwidth tests measure the maximum throughput of a computer network.

Number of Bottlenecks: Bottleneck basically means traffic/congestion at various points in the network link. The number of bottlenecks signifies the number of place throughout the network link where a bottleneck has occurred.

Traffic Intensity: In a digital network, the traffic intensity measures the ratio of the arrival rate of packets to the average packet length. Is: (al)/R where a is the average arrival rate of packets (e.g. In packets per second), L is the average packet length (e.g. In bits), and R is the transmission rate (e.g. Bits per second).

Performance metrics selected for the implementation of this project:

1. Throughput
2. Delay

b) Software and Testing Environment

A network simulator is software that predicts the behaviour of a computer network. Since communication Networks have become too complex for traditional analytical methods to provide an accurate understanding of system behaviour network simulator are used. In simulators, the computer network is typically modelled with devices, links, applications etc. and the performance is analysed. Simulators typically come with support for the most popular technologies and networks in use today.

Most of the commercial simulators are GUI driven, while some network simulators are CLI driven. The network model/configuration describes the state of the network (nodes, routers, switches, links) and the events (data transmissions, packet error etc.). An important output of simulations are the trace files. Trace files log every packet, every event that occurred in the simulation and are used for analysis. Network simulators can also provide other tools to facilitate visual analysis of trends and potential trouble spots.

Simulation of networks is a very complex task. For example, if congestion is high, then estimation of the average occupancy is challenging because of high variance. To estimate the likelihood of a buffer overflow in a network, the time required for an accurate answer can be extremely large. Specialized techniques such as "control variates" and "importance sampling" have been developed to speed simulation.

The network simulator must enable a user to:

1. Model the network topology specifying the nodes on the network and the links between those nodes
2. Model the application flow (traffic) between the nodes
3. Providing network performance metrics as output
4. Visualization of the packet flow
5. Logging of packet / events for drill down analyses or debugging.

The “ns-3” simulation software is built using C++ and Python with scripting capability. The ns-3 library is wrapped by Python thanks to the pybindgen library which delegates the parsing of the ns-3 C++ headers to gccxml and pygccxml to automatically generate the corresponding C++ binding glue. These automatically-generated C++ files are finally compiled into the ns-3 Python module to allow users to interact with the C++ ns-3 models and core through Python scripts. The ns-3 simulator features an integrated attribute-based system to manage default and per-instance values for simulation parameters. All of the configurable default values for parameters are managed by this system, integrated with command-line argument processing. The large majority of its users focuses on wireless simulations which involve models for Wi-Fi.

Network Topology

The general process of creating a simulation can be divided into several steps:

1. *Topology Definition:* To ease the creation of basic facilities and define their interrelationships, ns-3 has a system of containers and helpers that facilitates this process.
2. *Model Development:* Models are added to simulation (for example, UDP, IPv4, point-to-point devices and links, applications); most of the time this is done using helpers.
3. *Node and link configuration:* Models set their default values (for example, the size of packets sent by an application or MTU of a point-to-point link); most of the time this is done using the attribute system.
4. *Execution:* Simulation facilities generate events, data requested by the user is logged.
5. *Performance Analysis:* After the simulation is finished and data is available as a time-stamped event trace. This data can then be statistically analysed with tools like R to draw conclusions.
6. *Graphical Visualization:* Raw or processed data collected in a simulation can be graphed using tools like Gnuplot, matplotlib or XGRAPH.

The selection of a network topology can affect:

1. Type of equipment the network needs.
2. Capabilities of the equipment.
3. Growth of the network.
4. Way the network is managed.

Standard Topologies:

1. Bus – Devices connected to a common, shared cable.
2. Star - Connecting computers to cable segments branch out from a single point, or hub.
3. Ring - Connecting computers to cable that form a loop.
4. Mesh – Connects all computers in a network to each other with separate cables.

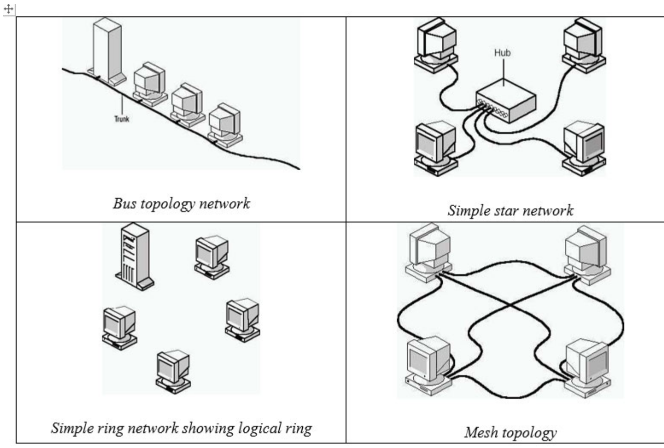


Fig. 3: Types of common network topologies

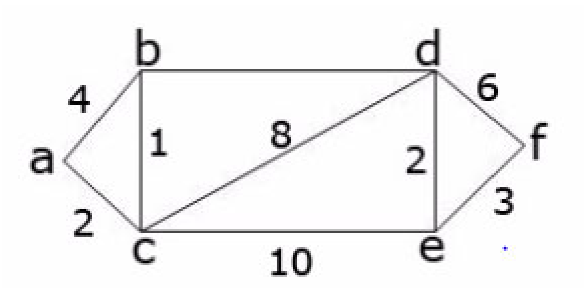


Fig. 4: Network topology used

w(u,v)	a	b	c	d	d	f
a	0	4	2	INF	INF	INF
b	4	0	1	5	INF	INF
c	2	1	0	8	10	INF
d	INF	5	8	0	2	6
e	INF	INF	10	2	0	3
f	INF	INF	INF	6	3	0

Fig. 5: Network Topology

c) Observations

Experimental results (simulation) in the IPv4 network protocol uses RIPv2 and OSPFv2 by using two different simulators is GNS3. The result that the speed OSPFv2 router for inter-router converge better than RIPv2 routers in the experiment with GNS3.

In experiments with GNS3 time from R converge on IP 192.168.5.2 which uses OSPFv2 router, round-trip min / avg / max = 996/1142/1200 ms, and the process of tracing the route from R5 to R1 which is headed to the IP 192.168. 1.1 through 192.168.6.2 takes 1060 msec while through the IP 192.168.5.2 takes 340 msec and through IP 192.168.2.2 takes 1768 msec.

For RIPv2 routers show round-trip min / avg / max = 924/1292/1440 and processes tracing the route from R1 to R5 is heading to IP 192.168.1.1 through 192.168.6.2 takes 1460 msec while through the IP 192.168.5.2 takes 884 msec and through IP 192.168.2.2 takes 1972msec. RIP multicast method takes a long time in terms of packet delivery.

d) Inferences

From the description and comparison of performance as well as the experimental results OSPFv2 Routing Protocol (OPEN Shortest Path First version 2) and RIPv2 (Routing Information Protocol version 2) in the IPv4 network, then it can be concluded that:

1. Every router within the same routing protocols build routing tables, based on information from neighboring routers for sharing information between routers.
2. Based on the speed of delivery of the package with the parameter used is the time between networks that converge OSPFv2 routing protocols rather than RIPv2 better use.
3. RIPv2 using distance / hops while for OSPF will use the same area thus saving bandwidth usage.
4. ENSP Simulator GNS3 looks faster than the time required for inter-network converge.To wider network then it would be better to use Dijkstra routers because of its ability to divide the network area into several sections.

References Références Referencias

1. Setiawati L. Differences Performance OSPFv2 and RIPv2 Routing Protocols In Network IPv4 Using Simulator GNS3 And ENSP
2. Wu, B. (2011). Simulation Based Performance Analyses on RIPv2, EIGRP, and OSPF Using OPNET.
3. Youssef, M., Younis, M. F., & Arisha, K. (2002, March). A constrained shortest-path energy-aware routing algorithm for wireless sensor networks. In *Wireless Communications and Networking Conference, 2002. WCNC2002. 2002 IEEE*(Vol. 2, pp. 794-799). IEEE.
4. Liu, L., Jin, J., Palaniswami, M., Liu, M., Li, X., & Huang, Z. (2012). *Graph-Based Routing, Broadcasting and Organizing Algorithms for Ad-Hoc Networks*. INTECH Open Access Publisher.
5. Kassabalidis, I., Das, A. K., El-Sharkawi, M. A., Marks II, R. J., Arabshahi, P., & Gray, A. (2001, August). Intelligent routing and bandwidth allocation in wireless networks. In *Proc. NASA Earth Science Technology Conf. College Park, MD, August 28* (Vol. 30)
6. Devi, G. S., Kumar, G. S., G D, P. V., & Reddy, P. (2011). Minimum Hop Energy Efficient Routing Protocol. *International Journal of Computer Applications*, *34*(4).
7. Chiang, S. S., Huang, C. H., & Chang, K. C. A Minimum Hop Routing Protocol for Wireless Sensor Networks.
8. Klampfer, S., Mohorko, J., Cucej, Z., & Chowdhury, A. (2012). Graph's theory approach for searching the shortest routing path in RIP protocol: a case study. *PRZEGLAD ELEKTROTECHNICZNY*, *88*(8), 224-231.

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 17 Issue 5 Version 1.0 Year 2017
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

A Survey on Network Security

By C. Sridevi
NPR Arts And Science College

Abstract- Computer security is one of the most expected factor in the current & future industry. Nowadays computers are available in all places from home to big organization where they are all connected to networks. Hence the risk of data security is high whereas many algorithms are emerging according to the needs of various categories of people. Still we can see the security threats. In this paper I am going to present the threat attacks and the mechanisms that were used to secure data.

Keywords: *security attacks, intrusion detection, hackers.*

GJCST-E Classification: *C.2.0, D.4.6*

ASURVEYONNETWORKSECURITY

Strictly as per the compliance and regulations of:

A Survey on Network Security

C. Sridevi

Abstract- Computer security is one of the most expected factor in the current & future industry. Nowadays computers are available in all places from home to big organization where they are all connected to networks. Hence the risk of data security is high whereas many algorithms are emerging according to the needs of various categories of people. Still we can see the security threats. In this paper I am going to present the threat attacks and the mechanisms that were used to secure data.

Keywords: security attacks, intrusion detection, hackers.

I. Introduction

There are many kinds of attacks in networking. Whereas we can classify into wired and wireless attacks. Here we are going to see about various attacks and attackers and defenders in this paper.

A *network* is basically all of the components (hardware and software) involved in connecting computers across small and large distances [2]. Networks are used to provide easy access to information, thus increasing productivity for users. There are following main types of networks:[1]

Personal area network (PAN): It is a network that is used for the communication among the personal system ad its connecting devices like printer, modem, telephone, etc. in close proximity limited to one person only.

Local area network (LAN): It is a network used for connecting two or more than two persons in a small geographical area like campus, office building, etc.

Wide area network (WAN): It is a network used for connecting people at large geographical area. Large numbers of LAN are connected with each other creating a WAN so as to connect almost whole world.

Metropolitan area network (MAN): It is a hybrid network ranging between LAN and WAN where the connecting devices lies within the city. It is mainly used by the co-operate companies who want to share data from its one branch to another in the same city.

Global area network (GAN): This network is used for supporting mobile across arbitrary number satellite coverage areas and wireless LANs etc. The key challenge in mobile communications is handing off user communications from one local coverage area to the next.

Virtual private network (VPN): It is a network which is maintained by companies who wants to do the private communication over the public network. The path between the two companies in VPN is encrypted and forming a tunnel for the safe communication.

Author: Assistant Professor, Department of SW, BCA, NPR Arts & Science College, Natham. e-mail: c.sridevi1983@gmail.com

II. Classification of Attackers

Hackers: He is a person who gains unauthorized access to data classified into inside and outside attacks.

Cracker: Detects vulnerability and take advantage over it To develop a secure system we consider the following:

Hacker Types:

Black hats
White hats
Grey hats
Blue hats

a) *Various Types of Attacks*

Vulnerability – Weak point used as entry point
Threat -
Attacks
Controls

4 Types of Attacks

1) Interception : Watches packets
2) Interruption : Steals or disturbs the data
3) Modification : Changes the data
4) Fabrication : Sends another message apart from original but having the same sender name.

b) *Attacks on Password*

Loose Lipped Systems: When System asks for password and username to typed in the system accepts username before the password is typed in where unrevealing the user name.

Exhaustive Attack: Tries all types of passwords

Probable likely for the user: Thinks of user familiarities and guesses what the password the user could might have choosen.

Plain text system password list: Accesses the password database directly.

c) *Defending mechanisms*

Password selection criteria: Carefully selecting password where one cannot guess so.

One time passwords: On every access changes password by giving a function and the user solves.

Encrypted password File: Even when the database is accessed the passwords cannot be accessed when it is stored in an encrypted form.

d) Other Attacks

i. *Phishing*

Unsuspecting user submits sensitive information in to a fraud system believing it is a trustworthy one.

ii. *Pharming*

Also called as DNS Spoofing. It changes DNS address of the original website. Redirects to fake website.

iii. *Packet Sniffing*

Hacker observes conversation between 2 conversation.

iv. *Packet Spoofing*

Hacker obverses conversation and also sends false packet with false address.

v. *Spreading Viruses*

Viruses spreads itself through networks and through all medias.

Virus Types:

Parasitic Virus: Attach itself and spread

Memory resident virus: Stored in main memory and then spread to all executable files.

Stealth Virus: Remains undetected from antivirus.

Boot sector viruses: Starts whenever the system gets booted.

Polymorphic Virus: Changes code every time it copies to other.

Metamorphic Virus: Keeps rewriting itself every time.

e) Other Attacks

Packet Sniffing: In networks attacker observes packets between two conversation.

Packet Spoofing: Attacker receives the message of the sender and in turn sends another message with false address.

Phishing: Creates duplicate website with simple modification to the original website , if user access this page their secret data like online bank passwords and security questions and answers will be accessed through the website. This will be used to steal and transfer their money.

Pharming (DNS Spoofing): This will create a website duplicating the DNS address itself where whenever the website is tried to access this website will be loaded.

III. Various Algorithms

a) Data Encryption Standard (DES)

DES was the result of a research project set up by International Business Machines (IBM) Corporation in the late 1960‟ s which resulted in a cipher known as LUCIFER. DES is based on a cipher known as the Feistel block cipher. It consists of a number of rounds where each round contains bit-shuffling, nonlinear substitutions (S-boxes) and exclusive OR operations. Once a plain-text message is received to be encrypted, it is arranged into 64 bit blocks required for input. If the number of bits in the message is not evenly divisible by 64, then the last block will be padded. DES performs an initial permutation on the entire 64 bit block of data. It is then split into 2, 32 bit sub-blocks, Li and R I which are then passed into 16 rounds. The output of this final permutation is the 64 bits ciphertext.

b) AES (Advanced Encryption Standard)

AES is also known as the Rijndael's algorithm, is a symmetric block cipher. It was recognized that DES was not secure because of advancement in computer processing power. It encrypts data blocks of 128 bits using symmetric keys. It has a variable key length of 128, 192 or 256 bits : by default 256 is used. AES encrypts 128 bit data block into 10, 12 and 14 rounds according to the key size. AES can be implemented on various platforms such as small device encryption of AES is fast and flexible. AES has been tested for many security applications. The purpose of NIST was to define a replacement for DES that can be used in non-military information security applications by US government agencies.

c) Blowfish

It is one of the most public domain encryption algorithms. Blowfish was designed in 1993 by Bruce Schneider as a fast alternative to existing encryption algorithms. Blowfish is a symmetric key block cipher that uses a 64 bit block size and variable key length from 32 bits to 448 bits. Blowfish has 16 rounds or less. Blowfish is a very secure cipher and to use encryption free of patents and copyrights. No attack is successful against Blowfish, although it suffers from weak key problem.

d) IDEA(International Data Encryption Algorithm)

IDEA is a block cipher algorithm and it operates on 64-bit plaintext blocks. The key size is 128 bits long. The design of algorithms is one of mixing operations from different algebraic groups. Three algebraic groups are mixed, and they are easily implemented in both hardware and software: XOR, Addition modulo 216, Multiplication modulo 216 + 1. All these operations operate on 16-bit subblocks. This algorithm is efficient on 16-bit processors. IDEA is symmetric key algorithm based on the concept of Substitution- Permutation Structure, is a block cipher that uses a 64 bit plain text with 8 rounds and a Key Length of 128-bit permuted into 52 subkeys each of 128- bits. It does not contain Sboxes and same algorithm is used in reversed for decryption.

e) RC4

RC4 is a stream cipher symmetric key algorithm. as the data stream is simply XOR with generated key sequence. It uses a variable length key 256 bits to initialize a 256- bit state table. A state table is used for generation of pseudo-random bits which is XOR with the plaintext to generate the cipher text.

f) RC6

RC6 is a derivative of RC5. RC6 is designed by Matt Robshaw, Ron Rivest Ray Sidney and is a symmetric key algorithm that is used to congregate the requirements of AES contest. RC6 was also presented to the CRYPTREC and NESSIE projects. It is patented by RSA Security . RC6 offers good performance in terms of security and compatibility. RC6 is a Feistel Structured private key algorithm that makes use a 128 bit plain text with 20 rounds and a variable Key Length of 128, 192, and 256 bit. As RC6 works on the principle of RC that can sustain an extensive range of key sizes, word-lengths and number of rounds, RC6 does not contain S-boxes and same algorithm is used in reversed for decryption.[4]

g) Serpent

Serpent is an Advanced Encryption Standard (AES) competition, stood 2nd to Rijndael, is a symmetric key block cipher, designed by Eli Biham, Ross Anderson, and Lars Knudsen. Serpent is a symmetric key algorithm that is based on substitution permutation network Structure. It consists of a 128 bit plain text with 32 rounds and a variable Key Length of 128, 192 and 256 bit. It also contains 8 S- boxes and same algorithm is used in reversed for decryption. Security presented by Serpent was based on more conventional approaches than the other AES finalists. The Serpent is open in the public sphere and not yet patented.[4]

h) Twofish

Twofish is also a symmetric key algorithm based on the Feistel Structure and was designed by Bruce Schneier along with Doug Whiting, John Kelsey, David Wagner, Niels Ferguson and Chris Hall,. The AES is a block cipher that uses a 128 bit plain text with 16 rounds and a variable Key Length of 128, 192, 256 bit. It makes use of 4 S-boxes (depending on Key) and same algorithm is used in reversed for decryption. The inventors extends the Blowfish team to enhance the earlier block cipher Blowfish to its modified version named Twofish to met the standards of AES for algorithm designing. It was one of the finalists of the AES, but was not selected for standardization. The Twofish is an open to public sphere and not yet patented. [4]

i) TEA

TEA is also a Feistel Structured symmetric key algorithm. TEA is a block cipher that uses a 64 bit plain text with 64 rounds and a Key Length of 128-bit with variable rounds having 32 cycles. It does not contain S-boxes and same algorithm is used in reversed for decryption. TEA is designed to maximize speed and minimize memory footprint. Cryptographers have discovered three related-key attacks on TEA. Each TEA key can be found to have three equal keys, thus it can be used as a hash function. David Wheeler and Roger Needham have proposed extensions of TEA that counter the above attacks.[4]

j) CAST

CAST is symmetric key algorithm based on the backbone concept of Feistel Structure. It is designed by Stafford Taveres and Carlisle Adams, is considered to be a solid algorithm. The CAST is a block cipher that uses a 64 bit plain text with 12 or 16 rounds and a variable Key Length of 40 to128-bit. It also contains 4 S-boxes and same algorithm is used in reversed for decryption. Bruce Schneier, John Kelsey, and David Wagner have discovered a related-key attack on the 64 bit of CAST that requires 217 chosen plaintexts, one related query, and 248offline computations. CAST is patented, which was generously released it for free use.[4]

IV. Security Protocols

a) Secure Socket Layer

It is used in secure exchange of information between web browser and web server. It gives 2 security services.

1. Authentication
2. Confidentiality

It has five layers

Application Layer
Secure Socket Layer
Transport Layer
Internet Layer
Data Link Layer
Physical Layer

SSL layer perform encryption on the data received and supports an algorithm called Fortezza.

b) Transport Layer uses HMAC

SSL have 3 sub protocol

Handshake protocol– Connection Establishment.

Record protocol –Actual message protocol.

Alert Protocol - If client/ server detects error other party discloses the connection and the secret key is deleted.

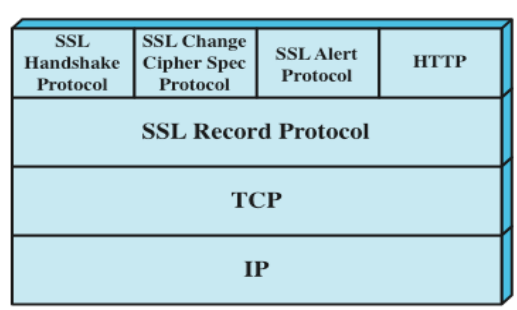


Fig.1

Global Journal of Computer Science and Technology (E) Volume XVII Issue V Version I Year 2017

SSL is attacked by Buffer Overflow.

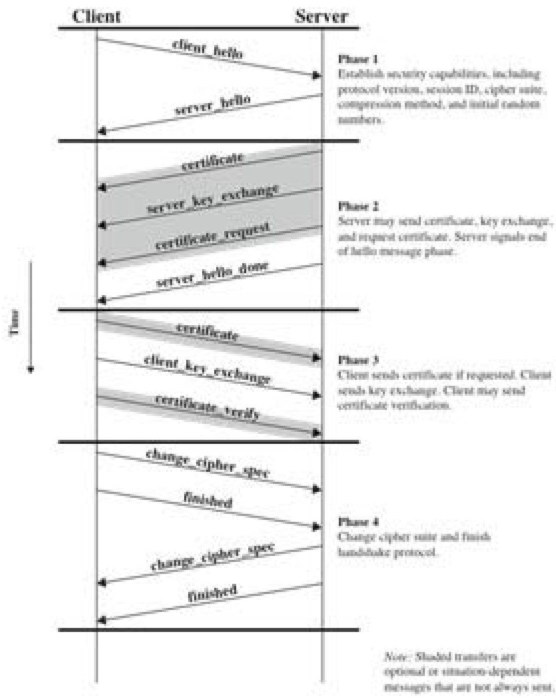


Fig. 2: Handshake protocol action

c) *SHTTP- Secure HTTP*

Combination of HTTP and SSL to implement secure communication between a Web browser and a Web server SSL don't differentiate different messages. SHTTP is similar to SSL but work on individual messages.

d) *Internet Protocol Security (IPSec)*

Although it was designed to run in the new version of the Internet Protocol, IP Version 6 (IPv6), it has also successfully run in the older IPv4 as well.

IPSec sets out to offer protection by providing the following services at the network layer:

Access Control: To prevent an unauthorized access to the resource.

Connectionless Integrity: To give an assurance that the traffic received has not been modified in any way.

Confidentiality: To ensure that Internet traffic is not examined by non-authorized parties. This requires all IP datagrams to have their data field, TCP, UDP, ICMP or any other datagram data field segment, encrypted.

Authentication: Particularly source authentication so that when a destination host receives an IP datagram, with a particular IP source address, it is possible to be sure that the IP datagram was indeed generated by the host with the source IP address. This prevents spoofed IP addresses.

Replay protection: To guarantee that each packet exchanged between two parties is different.

IPSec protocol achieves these objectives by dividing the protocol suite into two main protocols:

1. Authentication Header (AH) protocol
2. Encapsulation Security Payload (ESP) protocol.

The AH protocol provides source authentication and data integrity but no confidentiality.

The ESP protocol provides authentication, data integrity, and confidentiality. [5]

IPSec operates in two modes: transport and tunnel:

i. *Transport Mode*

The Transport mode provides host-to-host protection to higher layer protocols in the communication between two hosts in both IPv4 and IPv6.

ii. *Tunnel Mode*

Tunnel mode offers protection to the entire IP datagram both in AH and ESP between two IPSec gateways. This is possible because of the added new IP header in both IPv4 and IPv6. Between the two gateways, the datagram is secure and the original IP address is also secure.

e) *SET - Secure Electronic Transactions*

SET[6] is a protocol specifically designed to secure payment-card transactions over the Internet. It was originally developed by Visa International and MasterCard International in February 1996 with participation from leading technology companies around the world.

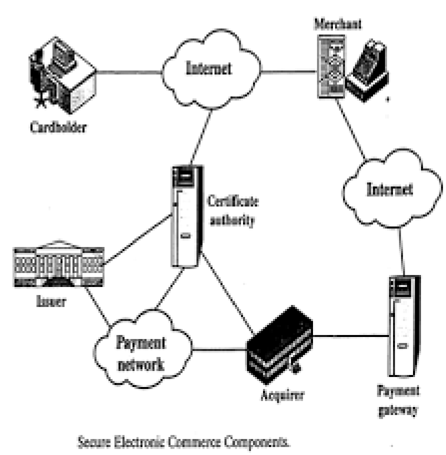


Fig. 3

1. Bob indicates to Alice that he is interested in making a credit card purchase.
2. Alice sends the customer an invoice and a unique transaction identifier.
3. Alice sends Bob the merchant's certificate which includes the merchant's public key. Alice also sends the certificate for her bank, which includes the

bank's public key. Both of these certificates are encrypted with the private key of a certifying authority.

4. Bob uses the certifying authority's public key to decrypt the two certificates. Bob now has Alice's public key and the bank's public key.
5. Bob generates two packages of information: the order information (OI) package and the purchase instructions (PI) package. The OI, destined for Alice, contains the transaction identifier and brand of card being used; it does not include Bob's card number. The PI, destined for Alice's bank, contains the transaction identifier, the card number and the purchase amount agreed to Bob. The OI and PI are dual encrypted: the OI is encrypted with Alice's public key; the PI is encrypted with Alice's bank's public key. (We are bending the truth here in order to see the big picture. In reality, the OI and PI are encrypted with a customer-merchant session key and a customer-bank session key.) Bob sends the OI and the PI to Alice.

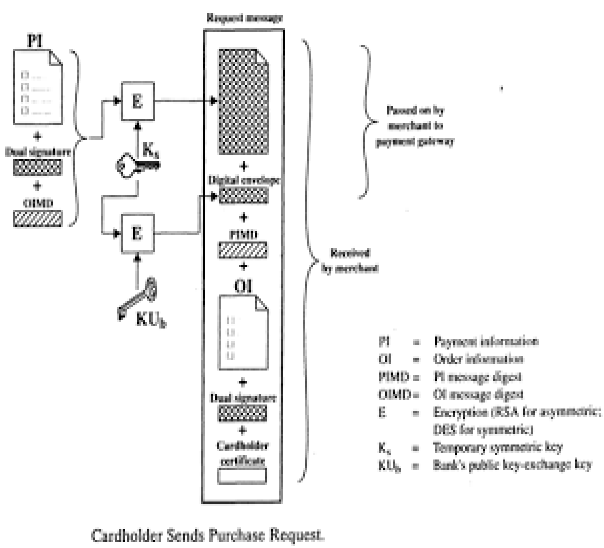


Fig. 4

6. Alice generates an authorization request for the card payment request, which includes the transaction identifier.
7. Alice sends to her bank a message encrypted with the bank's public key. (Actually, a session key is used.) This message includes the authorization request, the PI package received from Bob, and Alice's certificate.
8. Alice's bank receives the message and unravels it. The bank checks for tampering. It also make ssure that the transaction identifier in the authorization request matches the one in Bob's PI package.
9. Alice's bank then sends a request for payment authorization to Bob's payment-card bank through traditional bank-card channels -- just as Alice's bank would request authorization for any normal payment-card transaction.

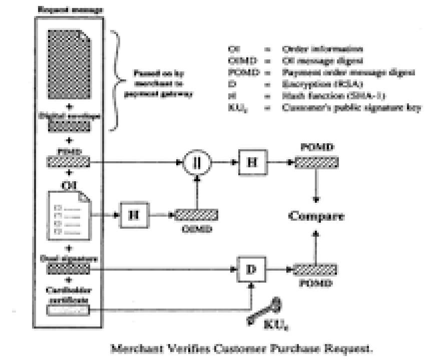


Fig. 5

One of the key features of SET is the non-exposure of the credit number to the merchant. This feature is provided in Step 5, in which the customer encrypts the credit card number with the bank's key.

Encrypting the number with the bank's key prevents the merchant from seeing the credit card. Note that the SET protocol closely parallels the steps taken in a standard payment-card transaction. To handle all the SET tasks, the customer will have a so-called digital wallet that runs the client-side of the SET protocol and stores customer payment-card information (card number, expiration date, etc.)

V. Conclusion

This papers dealt with various attacks on networks and the defencing mechanisms present. Many algorithms have been developed as an measure to secure the system. All the algorithms are useful based on the requirement as and when needed. Various security mechanisms and security protocols are available.

References Références Referencias

1. Dr. Parminder Singh Assistant Professor (Department of Information Technology) Chandigarh Group of Colleges, Landran, Mohali, Punjab, India. "A Survey on Different aspects of Network Security in Wired and Wireless Networks" in International Journal of Latest Trends in Engineering and Technology (IJLTET)
2. http://computernetworkingnotes.com/network-technologies/basic-networking.html
3. "Cryptography and Network Security" – Behrouz A. Forouzon.
4. "A Survey On Various Encryption And Decryption Algorithms M.Chanda Mona et al.," International Journal of Security (IJS) Singaporean Journal of Scientific Research(SJSR) Vol.6.No.6 2014 Pp. 289-300.

5. Kizza Guide to Network Security.
6. Creative World 9 – Website.
7. "Cryptography and Network Security" – Atul Kahate
8. Gurjeevan Singh, Ashwani Kumar Singla,K.S. Sandha, "Through Put Analysis Of Various Encryption Algorithms", IJCST Vol. 2, Issue 3, September 2011.
9. Deepak Kumar Dakate, Pawan Dubey," Performance Comparison of Symmetric Data Encryption Techniques ", International Journal of Advanced Research in Computer Engineering & Technology, Volume 3, No. 8, August 2012, pp . 163-166.
10. Shashi Mehrotra Seth, Rajan Mishra," Comparative Analysis Of Encryption Algorithms For Data Communication", IJCST Vol. 2, Issue 2, pp.192- 192 *June 2011.*
11. Agarwal, R., Dafouti, D., Tyagi, S. "Peformance analysis of data encryption algorithms ", Electronics Computer Technology (ICECT), 2011 3rd International Conference, vol.5, April 2011, pp. 399 – 403.

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 17 Issue 5 Version 1.0 Year 2017
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

A Review of Technical Issues on IDS and Alerts

By Dr. Nehinbe Joshua Ojo & Onyeabor Uchechukwu Solomon

Federal University

Abstract- The fact that swindlers can trick computer and mobile systems to commit different criminal offenses have to lead to the current advancement in the domain of Intrusion Detection Systems (IDSs). While the toolkits are growing mechanisms for monitoring, analyzing, gathering and reporting activities that can endanger computer and mobile systems, however, they are frequently subjected to series of fiery debates over the years. Thus, a wide range of taxonomy has been proposed to clarify their strengths and weaknesses. Nonetheless, researchers often reticent from critical issues associated with the "used alerts" and "unused alerts" that the toolkits can generate to warn analysts. Thus, this paper presents the progression of the above mechanisms over the years; and exhaustively explains some salient issues that were faulted in the previous reviews. Finally, we suggest various ways to improve the efficacy of the toolkits and how to lessen cases of intrusions across the globe.

Keywords: *intrusion detection system; a detector; alerts; redundant alerts; workload.*

GJCST-E Classification: *H.3.7*

AREVIEWOFTECHNICALISSUESONIDSANDALERTS

Strictly as per the compliance and regulations of:

A Review of Technical Issues on IDS and Alerts

Dr. Nehinbe Joshua Ojo[α] & Onyeabor Uchechukwu Solomon[σ]

Abstract- The fact that swindlers can trick computer and mobile systems to commit different criminal offenses have to lead to the current advancement in the domain of Intrusion Detection Systems (IDSs). While the toolkits are growing mechanisms for monitoring, analyzing, gathering and reporting activities that can endanger computer and mobile systems, however, they are frequently subjected to series of fiery debates over the years. Thus, a wide range of taxonomy has been proposed to clarify their strengths and weaknesses. Nonetheless, researchers often reticent from critical issues associated with the "used alerts" and "unused alerts" that the toolkits can generate to warn analysts. Thus, this paper presents the progression of the above mechanisms over the years; and exhaustively explains some salient issues that were faulted in the previous reviews. Finally, we suggest various ways to improve the efficacy of the toolkits and how to lessen cases of intrusions across the globe.

Keywords: intrusion detection system; a detector; alerts; redundant alerts; workload.

I. Introduction

The likelihood that companies and private individuals across the globe can lose large sum of financial and material resources to swindlers under false ploys committed with the support of mobile and computer services is of great concerns both in academia and in the industrial sector in general. These problems were envisaged in about four decades ago; and accordingly, the Intrusion Detection System (IDS) was proposed (Nehinbe, 2011). Although, the present-day Intrusion Detection Systems (IDSs) have evolved through different models, however, there are increasing concerns that new issues are constantly emerging from time to time (Ghorbani et al. 2010; Mohamed, 2013).

While various discussions and open arguments have been carried out in media and contemporary literature, some technical issues are erroneously unstressed over the years. For instance, the concept of IDS started from the work of Anderson in 1980 when the scholar classified users of mainframe computer systems into abnormal; and normal users (Anderson, 1980). Some of the existing IDSs that can be used for research purposes include Snort, Bro; and OSSEC (Stavroulakis and Stamp, 2010; Rehman, 2003; Bro, 2017).

Author α σ: Federal University, Oye-Ekiti, NG.
e-mails: nehinbe@yahoo.com, uchechukwu.onyeabor@fuoye.edu.ng.

```
[**] [116:150:1] (snort decoder) Bad Traffic Loopback IP [**]

[Priority: 3]

04/16-21:06:19.079160 127.170.84.62:45544 -> 131.84.1.31:24004

TCP TTL:255 TOS:0x8 ID:36226 IpLen:20 DgmLen:40 DF

***A**** Seq: 0x7BEA192D  Ack: 0x0  Win: 0x4000  TcpLen: 20
```

Figure 1: Alert from Snort on public trace file

The central issue here is that as shown in Figure 1, IDS extracts and logs attributes from every suspected packet it notices for further analysis. Unfortunately, these have also generated series of issues over the years.

An intrusion is a breach of security of a computer or mobile system (Stallings, 2011). Also, it can represent an act of unlawful access to a digital system. In this case, the location of the intruders can be inside or outside of the networks. For this reason, intruders are categorized as intruders that are insiders and intruders that are outsiders. As both names imply, the former depicts malicious users that are inside the computer or mobile networks and the latter are malicious users that are outside the computer or mobile networks.

The concept of intrusions may signify interruption of traffics in transit, stoppage or deliberate delay of services from reaching service users; invading sensitive information, destruction of components of the computer and mobile systems by causing severe damage to the software, hardware and some useful files (Kizza, 2009). Some intrusions can modify, corrupt, delete and erase directory. Accordingly, the developments of their various types often generate series of technical issues that were raised, analyzed, discussed and meticulously disputed in the past years.

The development has also lead to the evolution of standards, policies and best practices being proposed to lessen cases of intrusions over the years. In this note, qualifications, professional development and professional certifications are also emphasized as benchmarks for the recruitment of computer and mobile security professionals in some settings. Unfortunately, cases of intrusions are emerging every day. Computer users, mobile users; and community of security teams are mostly apprehensive due to the unpredictable menace of dangerous and sophisticated dimensions for compromising the security of resources reportedly occurring in some quarters globally.

Organizations and people that are victims of sophisticated intrusions can be devastated as a result of their experiences. Sophisticated intruders can swindle people and firms funds that they have accumulated, stored and planned for the implementation or funding of projects within overnight.

Sophisticated intruders can damage corporate image and personality that have built over the years within a twinkle of eyes (Gary, 2007; Mohamed, 2013). Sophisticated intruders can intrude into the computer or mobile systems with the purpose to cheaply embarrass a wide range of community of people. They can leak sensitive information about the governments, agencies, corporate firms and highly dignified people such as celebrity and scholars to competitors, opponents; and enemies without the rethink of the consequences of their malicious behaviors on the victims.

In another dimension, there are series of overheads regarding spending, cost, apportioning of resources, control and the mechanisms necessary to promptly thwart sophisticated intrusions in a real-life environment.

Irrespective of the motives and the category of the intruders, successful and unsuccessful attacks on computer and mobile systems always leave potential dangers behind. The existence of cartel of intruders is often reaffirmed in literature. Thus, intruders may share the previous experience they have garnered with colleagues. The danger of such information sharing can be enormous if they divulge the information to dangerous and more skillful intruders that are bent to launch devastating, stealthy or destructive attacks against the previous victims.

A technical issue here is that, in the present day setting, strong IDSs will alert whenever unskilful computer and mobile users mistakenly infringe the security of other digital systems that the detectors monitor. Conversely, despite the evolutionary trend in the development of IDSs, it is improbable for the mechanism of intrusion detections to discriminate and subsequently classify attacks by the intention of each intruder.

Besides, numerous scholars have categorized IDSs into different categories. Debar et al. (2000) notably categorized IDSs by source of data, method; and concept that an IDS uses for detecting attacks. The taxonomy produced by Axelsson (2000) classified them by the detection, operations and objectives of the IDSs. In the reviewed carried out by Debar et al. (2000), misuse and anomaly detection methods are fundamental approaches for developing the IDSs. Nonetheless, as argued by Lazarevic et al. (2005) and corroborated by Scarfone and Mell (2007), IDSs lack universally acceptable classification models.

This paper exhaustively reclassifies existing IDSs on the bases of the source of data the IDS uses, the method of detection, function, structural design, the location of the detector and reporting strategies used by the IDS. Unlike the previous taxonomy, this paper explains critical and inherent issues that can maximize values and trust repose on the usage of IDSs as devices for adequately safeguarding computer and mobile systems from intrusions. Also, the paper has delved into the complexity of the intrusion detections and the existence of different methodologies for detecting malicious activities and eventually evolves better strategies for manufacturers on how they can upgrade the existing toolkits.

The remaining sections of this paper are organized as follows: Section 2 discusses the evolution of IDSs since the 1980s. Sections 3 and 4 express some of the emerging issues identified with IDS alerts and the conclusion of the paper, respectively. The latter also provides the overview of the analyses and opens up new research directions to improve the efficacies of IDSs.

II. The Advancement in Intrusion Detection Systems (IDSs)

Debar et al. (2000), Ghorbani et al. (2010) and some scholars have proposed revised taxonomy for IDSs. However, such classifications have not explicated some technical issues recently identified while working with IDSs. Accordingly, we reclassify IDSs by the source of data that the IDS uses; the method the existing IDS use for detection of intrusions; the basic functions the IDS can perform; the structural design underpinning each IDS, the location of the detector within computer and mobile networks and various reporting strategies that the IDS used over the years. Hence, Figure 2 illustrates the schematic drawing of the proposed taxonomy to simplify the relationship between one category of IDS and another category.

a) Classification by source of data

An IDS can be categorized on whether the detector obtains data from the database logs, operating system's logs, application's logs, transaction logs (in the case of financial organisations), trace files such as network traces, dump of an operating system, database and network operations and alerts from other intrusion detectors (Axelsson, 2000; Nehinbe, 2011).

Global Journal of Computer Science and Technology (E) Volume XVII Issue V Version I Year 2017

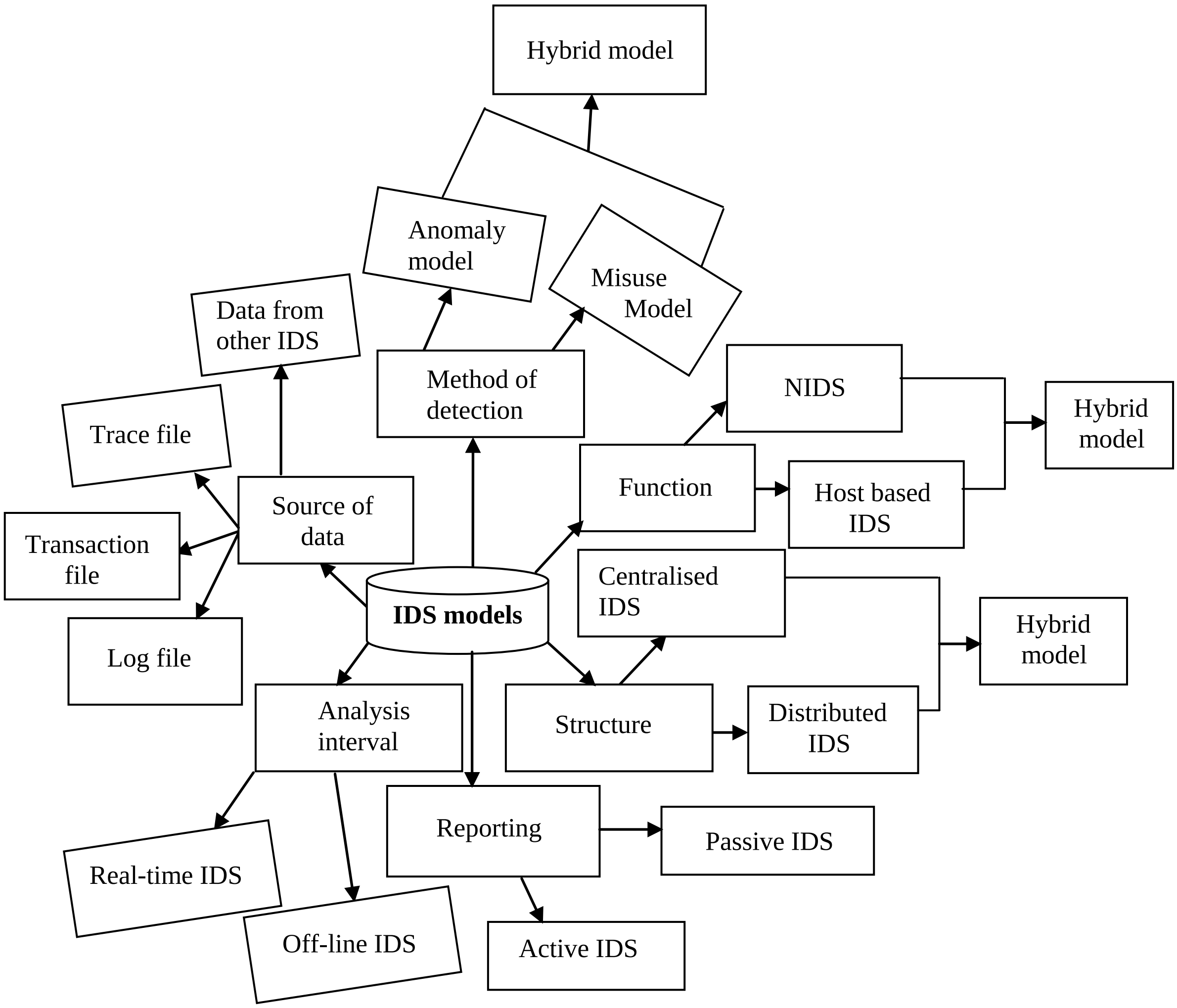


Figure 2: Categories of IDS

b) Classification by function

Different models of intrusion detectors have different capabilities. Accordingly, intrusion detectors can be categorized into host-based, network-based and hybrid intrusion detection systems (Karthikeyan and Indra, 2010). A host-based intrusion detector analyses activities of users occurring on the host computers. However, this model is ineffective to detect attacks that flood computer networks such as buffer over-flow and Distributed Denial of Service (DDoS) attacks that specialized IDS can quickly detect at the network level (Scarfone and Mell, 2007).

Contrarily, a Network-based Intrusion Detector (NID) otherwise known as Network Intrusion Detection System (NIDS) can only analyze activities of users at the network level. The detector validates each packet that migrates across its sensor with inbuilt rules or policies. Subsequently, the NIDS raises alerts to warn the presence of intrusions on the networks whenever a packet matches any of its detection rules (Amer and Hamilton, 2011). Usually, network-based intrusion detectors can also monitor activities on wired and wireless networks. Mobile network intrusion detector is a device that monitors wireless network nodes (Scarfone and Mell, 2007). However, NIDS has critical drawbacks. For instance, the strengths of NIDS depend on the capability of the rules or policies that the detector uses to detection network intrusions. Besides, the inability of some categories of the NIDS to accurately decode traffics that intruders deliberately encrypt is often a subject of contention in a realistic environment. Also, the efficacy of the NIDS to report fraudulent activities at the database, operating system and application levels is bad (Rehman, 2003).

The hybrid model integrates network-based and host-based intrusion detectors (HIDS) together. This category of detectors can concurrently monitor activities of the user both at the host level and at the network level. Nevertheless, adequate amount of capital and memory space are usually required to effectively implement HIDS in a realistic setting.

c) Classification by method of detection

Some intrusion detectors can detect activity that deviates from normal behavior, while others can only detect known or anticipated attacks. The former category is called anomaly detectors while the latter is known as signature detectors. In Bishop (2003), an anomaly detector has a set of activities or profiles to represent "normal behaviors" in its detection engine. Operators of the IDS can derive normal behaviors from the historical behaviors of the host, operating system, application and the users of the networks. The detector then compares inbound and outbound traffics with its profiles and subsequently raises alerts for traffics deviate from the normal behaviors. The significance of this design is its capability to detect new attacks. However, the major concern about anomaly detectors is the integrity of the reports they generate. Secondly, activities that constitute normal and abnormal behaviors can change over time (Chandola and Kumar, 2009).

Misuse detectors are also called signature-based detectors because they keep databases of patterns, known vulnerabilities or signatures of known and anticipated attacks (Bishop, 2003; Wang et al. 2006).

The IDS that uses misuse detection methods usually compares incoming and outgoing traffics with each of its detection rules in a top-down manner. The detector will subsequently trigger alerts whenever a packet matches any of its rules to indicate the presence of suspicious message intending to access the computer. Conversely, the mechanism will ignore a packet that does not match any of its rules by treating each of them as a normal packet (Bishop, 2003). However, a signature-based detector can only detect attacks that match its detection rules.

Most signature-based detectors are criticised for the inability to decode encrypted traffics (Scarfone and Mell, 2007). Network intrusion detectors have limited capacity to process packets. For this reason, some of them can drop significant number of packets whenever attackers overload them with network traffics.

In effect, misuse and anomalous IDSs have several flaws. Operators must constantly update profiles of anomaly detectors and the signatures of misuse detectors (Karthikeyan and Indra, 2010).

d) Classification by intervals between detection and analysis

In Lazarevic et al. (2005), IDSs are classified into real-time and off-line systems. A real-time intrusion detector analyzes computer activities while in progress and concurrently raises alerts once an attack is detected. Contrarily, off-line intrusion detector reports activities after the events have happened.

Furthermore, giving the inadequacies of detection capacities of the current versions of IDSs, it is plausible that analyzers of intrusion logs can take wrong decisions against legitimate events in a real-time manner.

Similarly, an off-line intrusion detection mode exposes computer resources to risks, especially if there is a relatively long time interval between the time the detector detects the attacks and the time to review the IDS logs.

e) Classification by method of deployment

There are centralized, distributed and hybrid intrusion detection models (Lazarevic et al. 2005). A centralized IDS usually aggregates alerts of other IDSs at a fixed location. The detector can easily detect stealthy attacks that below threshold operators have defined in each segment of the network whenever they analyze intrusion logs at a central location.

Nevertheless, the efficacy of this design depends on stable communications between the contributing sources and the repository where the operators will analyze the data. Furthermore, the capability of centralized IDS to overcome discrepancies that may exist within the logs of different models of IDS is another weakness that is peculiar to this model.

Distributed intrusion detectors analyze logs of computer activities in individual locations. In Debar et al. (2000), the benefit of this model is that multiple intrusion logs can be used to validate each other in reducing false positives. Nevertheless, security experts often encounter different challenges whenever they have to review several intrusion logs.

Also, a hybrid model combines centralized and distributed models to achieve high intrusion detection rate. Nonetheless, integrated IDSs often combine the weaknesses inherent in all the cooperating IDSs.

f) Classification by method of reporting

The action that an IDS takes upon the detection of an intrusion has a significant impact on the group the detector belongs. Hence, Lazarevic et al. (2005) group IDSs into passive and active response models. The passive response detectors can not deter attacks in progress, unlike the active response detectors that can generate alerts and initiate preventive actions to block attacks from achieving the objectives of the attackers. The major problem with passive and active response models is that both approaches still exhibit shortcomings that are similar to that of the real-time and offline models (Lazarevic et al. 2005).

The fundamental truth is that all the above models of IDS collectively generate alerts such as shown in Figure 3 and such information can degenerate to series of problems.

III. Emerging Issues with Formats of IDS Alerts

IDSs organize, log and display alerts in different manner. This paper uses Bro and Snort IDS as examples of NIDSs (Alder et al. 2007; Bro, 2017). For instance, Snort logs alert in ASCII and full alert's formats. Nonetheless, ASCII formats cannot be immediately discernible or readable by human operators. Operators will still need specialized tools to decode, read and analyze them before they can make meanings decisions from them. This indicates a danger if the analyzers that can decode the logs are not readily available and operators must promptly take decisons to discern suitable countermeasures that will thwart attacks signified by such logs.

Snort can generate comprehensive information that will include the packet's headers and Snort's assigned attributes. The mechanism can further assign the rule that triggers the alerts, the description, time and date the event is logged. The detector can be configured to produce different output modes such as fast, full or console. This functionality enables the operators to configure Snort to generate less output whenever such requirements arise.

Each NIDS has its peculiar signatures and formats for writing the detection rules. For example, Bro captures comprehensive information about suspicious traffics into tab-separated log files. Such verbose narrations usually include each the host, connection, extraction of vital information from many application-layer protocols and server responses. The major strengths of NIDSs are many. Experience suggests that NIDSs such as Snort and Bro can analyze PCAP files in offline mode and IPv4 and IPv6 formats (Bro, 2017). The detectors can be used for forensic analysis of intrusive evidence in real-life networks.

IV. Emerging Issues with Kinds of IDS Alerts

Existing IDSs trigger "disused alerts" and "used alerts". The former are categories of warnings that analysts will never use for any significant purpose. Also, they are warnings that are mostly abandoned by professionals for some reasons. However, it is usually hard to establish the degree of severity of such messages without making a thorough investigation about them. Hence, analysts must be prudent in handling them in a realistic environment.

```
08/03-22:14:26.756815 192.168.2.2:21 -> 192.168.2.1:1067
TCP TTL:64 TOS:0x10 ID:6518 IpLen:20 DgmLen:83 DF
***AP*** Seq: 0x17BA8D92  Ack: 0xFBCEEF87  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 116909 288736
[**] [125:1:1] (ftp_telnet) TELNET CMD on FTP Command Channel [**]
[Priority: 3]
08/03-22:14:26.757820 192.168.2.1:1067 -> 192.168.2.2:21
TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:66
***AP*** Seq: 0xFBCEEF87  Ack: 0x17BA8DB1  Win: 0x7D78  TcpLen: 20
[**] [125:1:1] (ftp_telnet) TELNET CMD on FTP Command Channel [**]
[Priority: 3]
08/03-22:14:26.762762 192.168.2.2:21 -> 192.168.2.1:1067
TCP TTL:64 TOS:0x10 ID:6519 IpLen:20 DgmLen:75 DF
***AP*** Seq: 0x17BA8DB1  Ack: 0xFBCEEFA1  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 116910 288736
[**] [125:1:1] (ftp_telnet) TELNET CMD on FTP Command Channel [**]
```

Figure 3: Snort's alerts on a publicly available dataset

Conversely, the latter are warnings that analysts use for decision purposes such as the investigation of the incident of intrusions, designing countermeasures and mitigation's strategies. Redundant warnings, alerts workload and diverse processing methods for processing IDS alerts are central aspects of emerging issues associated with "used alerts" that are within IDS logs in a recent time.

a) *Redundant alerts*

Redundant alerts are fundamental problems of intrusion detection technology. These issues are the main challenges to the usage of IDSs for network forensics over the years because they can complicate the problems of classification, data reduction, false positive; intrusion correlation and reporting (Nehinbe, 2011; Tjhai et al. 2008).

It is possible to explain the above concept in three different perspectives: The first problem is how to reasonably reduce the entire alerts in an intrusion log without underestimating security breach the IDS has reported (Nehinbe, 2011). The second challenge is how to promptly discern false warnings from realistic attacks so that operators will not implement countermeasures are against legitimate events (Stallings, 2011). The third issue is how to eliminate less critical alerts from an intrusion log to enhance clarity of the reports.

Redundant alerts originate from the point at which the NIDS decides on the network packets that it would respectively classify as suspicious and normal packets or activities (Scarfone and Mell, 2007). On the whole, every NIDS has detection rules or signatures, patterns or characteristics of events that suggest intrusions. The detector uses the rules to validate each of the packets that the detector notices.

Fundamentally, the detector will raise an alert each time a packet matches its detection rule to signify an intrusion or suspicious activity. The mechanism records the warnings inside the log in the order of occurrence for further review. NIDS treats outbound or inbound traffic as a new occurrence within the same timestamp. Hence, the IDS toolkit often triggers overwhelming alerts that may suggest notices of closely related packets (Nehinbe, 2010). Therefore, analysts automatically inherit the classification problems that the detector cannot adequately tackle.

Global Journal of Computer Science and Technology (E) Volume XVII Issue V Version I Year 2017

b) Alerts workload

Human operators must re-examine the content of IDS logs. Usually, more time and efforts are spent to ascertain the correctness of the redundant warnings, and to substantiate suitable preventive measures. Furthermore, the occurrence of indiscernible relationships among the entries within the log can complicate the process of analyzing them.

Furthermore, the problems of alerts workload can degenerate to swamping whereby the detector triggers excessive warnings that exceed the capability of the analyst. One of the established approaches to lessen the problems of alerts workload is to configure the detector to suppress some significant quantity of alerts at a specified time and by ignoring specific network traffic (Alder et al. 2007; Rehman, 2003; Scarfone and Mell, 2007). Similarly, operators can configure the detectors to trigger specific quantity of alerts. The operators can also deactivate nuisance rules. Also, they can reconfigure the IDS by prioritizing the detection rules so that rules that have low priorities will trigger little or no alerts. Nevertheless, any of the methods above will only be possible to be carried out with a detector that has such functionalities.

Secondly, alerts suppression techniques are vulnerable to the high rate of false negatives, especially whenever an intruder attacks a target machine with probing attacks that are below the threshold for suppressing the alerts. For instance, a packet of ping attack that is below the threshold is enough to evade detections.

Alerts suppression techniques have a propensity to bury small relationships that are sneaky intruders deliberately embedded in multiple alerts. For these reasons, alerts suppression methods frequently underestimate security breaches on the computer and mobile networks.

Moreover, it is cumbersome to reconfigure all the detection rules that NIDS uses as a method for reducing alerts workload (Alder et al. 2007). These tradeoffs have necessitated the implementation of NIDS in a default mode while operators can decide to adopt correlation and aggregation techniques to manage the problems of alerts workload that are inherent in its operations.

c) Different methods for processing IDS alerts

There are numerous ways and approaches to process alerts logged by IDSs. For instance, Figure 4 shows how we analyze alerts from Snort in the course of implementing clustering of intrusive trace files by C++ programs.

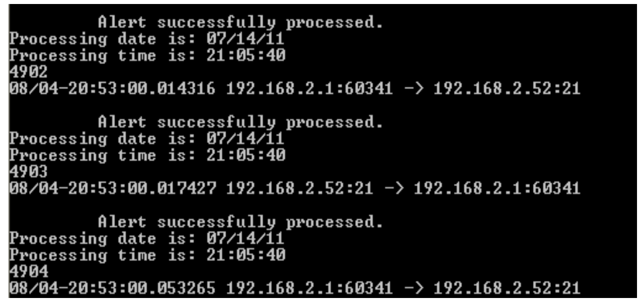


Figure 4: Processing alerts from Snort

In Nehinbe (2011), some authors have used Neural Networks (NN), Genetic programming, Visualizations; and Petri net to analyze the same category of publicly available datasets for testing IDS models in a different context (Wang et al. 2006).

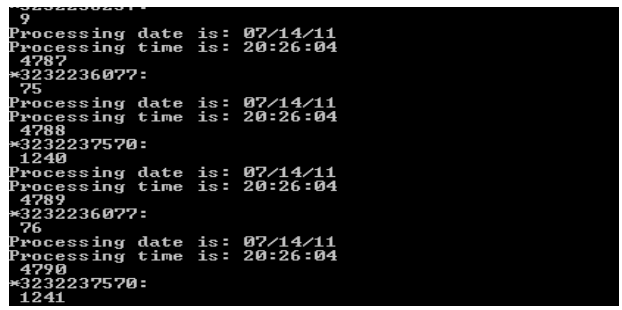


Figure 5: Alerts from Snort

Similarly, analysts can adapt the same group of alerts from the IDS such as Snort IDS for different purposes. For examples, Figure 5 illustrates how timestamp can be used to group alerts from Snort on the trace files into different clusters while Figure 6 gives the statistical transformation we carried out with the same trace file.

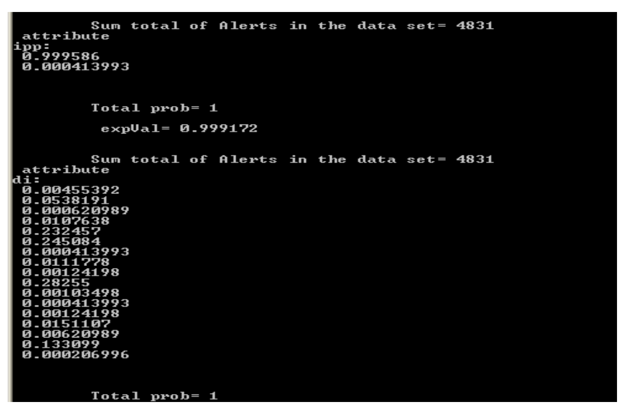


Figure 6: Statistical analysis of logs of Snort

Some authors have used other programming languages to process the same public trace files and to achieve different objectives. The central problem here is that it is difficult to substantiate which of the available methods and programming languages for analyzing logs of IDSs are the best ways to present such events in the context of digital security and forensics.

V. Conclusion

The possibility that victims of intrusions can suffer serious loss of business and trade secrets is a major concern across the globe. This paper critically reviews the evolution of the IDSs since the 1980s and some technical issues that arise with the existing models over the years. Thus, we also discuss a wide range of taxonomy together with their strengths and weaknesses.

Furthermore, we examine potential loss that victims of intrusions can experience. We affirm that intrusions can modify and delete a listing of the files stored in the memory of a computer system. Intrusions can embarrass private users and corporate firms. Intruders can divulge classified information about the governments, agencies, corporate firms and highly dignified people to their competitors, opponents and enemies.

Also, we show that there are overheads regarding control, spending, cost, apportioning of resources and the mechanisms necessary to quickly thwart intrusions in a real-life environment. However, series of technical issues were erroneously over-sighted over the years. This paper thoroughly presents a new review of the IDS technology to lessen them.

Overview of the weaknesses of IDSs collectively suggests that they can trigger many redundant alerts. Such alerts can degenerate to the problems of swamping if the trade-offs between true positives and false positives are not methodologically balanced. Hence, a thorough review of intrusion log requires a high level of expertise to establish the meaning and validity of each alert.

Furthermore, capabilities of attributes of alerts in the intrusion logs to discriminate attacks are some of the emerging issues we have mentioned above. The vast majority of the models we have reviewed above must be evaluated across a wide range of synthetic and realistic datasets. They must also be evaluated with big datasets to establish their performances with large and small evaluative datasets.

Additionally, intrusion aggregation techniques lack the capability for detecting patterns of attacks because they are unable to isolate alerts that respond to failed packets from suspicious activities that can reach their destinations.

Some intrusion aggregation models fundamentally reduce alerts redundancies and workload by focusing only on alerts with high priorities. Hence, suspicious activities that have low priorities may easily elude detections.

The underpinning theories and principles of some research designs may not be very useful for solving real-world problems. Graphical approaches usually produce series of hyper-alerts and numerous correlation graphs with numerous nodes. Graphical approaches tend to produce edges that are difficult to interpret.

Above all, the review above has not described how IDSs can eliminate ineffectiveness and inability to discriminate alerts by the information content they convey. We have not discussed existing mechanisms that are designed to ensure the predictability of each attribute IDSs extracted to describe suspicious packets. These are areas of further research direction that can be pursued to reduce the issues above and to improve the efficacies of IDSs in general.

References Références Referencias

1. Alder, R., Baker, A.R., Carter, E.F., Esler, J., Foster, J.C., Jonkman, M., Keefer, C., Marty, R. and Seagren, E.S. Snort: IDS and IPS Toolkit, Syngress publishing, Burlington, Canada, 2007.
2. Axelsson, S. Intrusion Detection Systems: A Survey and Taxonomy, Department of Computer Engineering, Chalmers University of Technology, Goteborg, Sweden, 2000.
3. Amer. S.H. and Hamilton, J.A. Intrusion Detection Systems (IDS) Taxonomy – A short review, 2011.
4. Anderson, J.P. Computer Security Threat Monitoring and Surveillance, Technical Report Washing, PA, James P. Anderson Co., 1980.
5. Bishop, M. Computer Security: Art and Science, Pearson Education, Inc, New York, 2003.
6. Gary, M. (2007), Silver Bullet Talks with Becky Bace, IEEE Security & Privacy Magazine, Vol. 5 , pp. 6–9.
7. Bro (2017), Bro Logging; https://www.bro.org/documentation/index.html; Accessed 14/12/2017
8. Chandola, V. and Kumar. V. Anomaly detection: A survey, University of Minnesota, 2009.
9. Debar, H., Dacier, M. and and Wespi, A. A Revised Taxonomy for Intrusion-Detection Systems, Annals of Telecommunications, vol. 55, pp. 361-78, 2000.
10. Ghorbani, A.A., Lu, W. and Tavallaee, M. Network Intrusion Detection and Prevention: Concepts and Techniques, Springer, New York, LLCC, 2010.
11. Kizza, J.M. A Guide to Computer Network Security, Springer-Verlag London, 2009.
12. Karthikeyan .K.R. and Indra, A. Intrusion Detection Tools and Techniques- A Survey, International Journal of Computer Theory and Engineering, Vol. 2, pp. 901-906, 2010.
13. Lazarevic, A., Kumar, V. and Srivastava, J. Intrusion detection: A survey, Managing Cyber Threats, pp. 19–78, June 2005.
14. Mohamed, A.A. (2013), Design Intrusion Detection System Based On Image Block Matching, International Journal of Computer and Communication Engineering, Vol. 2.

15. Nehinbe, J.O. Methods for reducing workload during investigations of intrusion logs, PhD thesis, University of Essex, UK, 2011.
16. Nehinbe J.O. Concurrent Reduction of False Positives and Redundant Alerts, International Conference on Information Society (i-Society 2010), proceedings of IEEE, London, UK.
17. Rehman, R. Intrusion Detection Systems with Snort: Advanced IDS Techniques Using Snort, Apache, MySQL, PHP and ACID, Prentice Hall PTR Upper Saddle River, New Jersey, 2003.
18. Stavroulakis, P. and M. Stamp. Handbook of Information and Communication Security, Springer-Heidelberg, Dordrecht London New York, 2010.
19. Scarfone, K. and Mell, P. Guide to Intrusion Detection and Prevention Systems (IDPS), Recommendations of the National Institute of Standards and Technology, Special Publication 800-94, Technology Administration, Department of Commerce, USA, 2007.
20. Stallings, W. Network Security Essentials: Applications and Standards, 4th edition, Prentice Hall, 2011.
21. Tjhai, G.C., Papadaki, M., Furnell, S.M. and Clarke, N.L. The Problem of False Alarms: Evaluation with Snort and DARPA 1999 Dataset, Trust, Privacy and Security in Digital Business, LNCS Vol. 5185, pp. 139–150, Springer-Verlag Berlin Heidelberg, 2008.
22. Wang, J., Wang, Z. and Kui-Dai. Intrusion Alert Analysis Based on PCA and the LVQ Neural Network, Neural Information Processing Lecture Notes in Computer Science, Vol. 4234, pp. 217-224, 2006.

Global Journals Inc. (US) Guidelines Handbook 2017

www.GlobalJournals.org

FELLOW OF ASSOCIATION OF RESEARCH SOCIETY IN COMPUTING (FARSC)

Global Journals Incorporate (USA) is accredited by Open Association of Research Society (OARS), U.S.A and in turn, awards “FARSC” title to individuals. The 'FARSC' title is accorded to a selected professional after the approval of the Editor-in-Chief/Editorial Board Members/Dean.

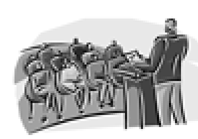
- The “FARSC” is a dignified title which is accorded to a person’s name viz. Dr. John E. Hall, Ph.D., FARSC or William Walldroff, M.S., FARSC.

FARSC accrediting is an honor. It authenticates your research activities. After recognition as FARSC, you can add 'FARSC' title with your name as you use this recognition as additional suffix to your status. This will definitely enhance and add more value and repute to your name. You may use it on your professional Counseling Materials such as CV, Resume, and Visiting Card etc.

The following benefits can be availed by you only for next three years from the date of certification:

FARSC designated members are entitled to avail a 40% discount while publishing their research papers (of a single author) with Global Journals Incorporation (USA), if the same is accepted by Editorial Board/Peer Reviewers. If you are a main author or co-author in case of multiple authors, you will be entitled to avail discount of 10%.

Once FARSC title is accorded, the Fellow is authorized to organize a symposium/seminar/conference on behalf of Global Journal Incorporation (USA).The Fellow can also participate in conference/seminar/symposium organized by another institution as representative of Global Journal. In both the cases, it is mandatory for him to discuss with us and obtain our consent.

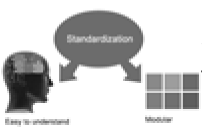


You may join as member of the Editorial Board of Global Journals Incorporation (USA) after successful completion of three years as Fellow and as Peer Reviewer. In addition, it is also desirable that you should organize seminar/symposium/conference at least once.

We shall provide you intimation regarding launching of e-version of journal of your stream time to time. This may be utilized in your library for the enrichment of knowledge of your students as well as it can also be helpful for the concerned faculty members.

The FARSC can go through standards of OARS. You can also play vital role if you have any suggestions so that proper amendment can take place to improve the same for the benefit of entire research community.

As FARSC, you will be given a renowned, secure and free professional email address with 100 GB of space e.g. johnhall@globaljournals.org. This will include Webmail, Spam Assassin, Email Forwarders, Auto-Responders, Email Delivery Route tracing, etc.



The FARSC will be eligible for a free application of standardization of their researches. Standardization of research will be subject to acceptability within stipulated norms as the next step after publishing in a journal. We shall depute a team of specialized research professionals who will render their services for elevating your researches to next higher level, which is worldwide open standardization.

The FARSC member can apply for grading and certification of standards of their educational and Institutional Degrees to Open Association of Research, Society U.S.A. Once you are designated as FARSC, you may send us a scanned copy of all of your credentials. OARS will verify, grade and certify them. This will be based on your academic records, quality of research papers published by you, and some more criteria. After certification of all your credentials by OARS, they will be published on your Fellow Profile link on website https://associationofresearch.org which will be helpful to upgrade the dignity.

The FARSC members can avail the benefits of free research podcasting in Global Research Radio with their research documents. After publishing the work, (including published elsewhere worldwide with proper authorization) you can upload your research paper with your recorded voice or you can utilize chargeable services of our professional RJs to record your paper in their voice on request.

The FARSC member also entitled to get the benefits of free research podcasting of their research documents through video clips. We can also streamline your conference videos and display your slides/ online slides and online research video clips at reasonable charges, on request.

The FARSC is eligible to earn from sales proceeds of his/her researches/reference/review Books or literature, while publishing with Global Journals. The FARSC can decide whether he/she would like to publish his/her research in a closed manner. In this case, whenever readers purchase that individual research paper for reading, maximum 60% of its profit earned as royalty by Global Journals, will be credited to his/her bank account. The entire entitled amount will be credited to his/her bank account exceeding limit of minimum fixed balance. There is no minimum time limit for collection. The FARSC member can decide its price and we can help in making the right decision.

The FARSC member is eligible to join as a paid peer reviewer at Global Journals Incorporation (USA) and can get remuneration of 15% of author fees, taken from the author of a respective paper. After reviewing 5 or more papers you can request to transfer the amount to your bank account.

MEMBER OF ASSOCIATION OF RESEARCH SOCIETY IN COMPUTING (MARSC)

The ' MARSC ' title is accorded to a selected professional after the approval of the Editor-in-Chief / Editorial Board Members/Dean.
The “MARSC” is a dignified ornament which is accorded to a person’s name viz. Dr. John E. Hall, Ph.D., MARSC or William Walldroff, M.S., MARSC.

MARSC accrediting is an honor. It authenticates your research activities. After becoming MARSC, you can add 'MARSC' title with your name as you use this recognition as additional suffix to your status. This will definitely enhance and add more value and repute to your name. You may use it on your professional Counseling Materials such as CV, Resume, Visiting Card and Name Plate etc.

The following benefitscan be availed by you only for next three years from the date of certification.

MARSC designated members are entitled to avail a 25% discount while publishing their research papers (of a single author) in Global Journals Inc., if the same is accepted by our Editorial Board and Peer Reviewers. If you are a main author or co-author of a group of authors, you will get discount of 10%.

As MARSC, you will be given a renowned, secure and free professional email address with 30 GB of space e.g. johnhall@globaljournals.org. This will include Webmail, Spam Assassin, Email Forwarders, Auto-Responders, Email Delivery Route tracing, etc.

We shall provide you intimation regarding launching of e-version of journal of your stream time to time. This may be utilized in your library for the enrichment of knowledge of your students as well as it can also be helpful for the concerned faculty members.

The MARSC member can apply for approval, grading and certification of standards of their educational and Institutional Degrees to Open Association of Research, Society U.S.A.

Once you are designated as MARSC, you may send us a scanned copy of all of your credentials. OARS will verify, grade and certify them. This will be based on your academic records, quality of research papers published by you, and some more criteria.

It is mandatory to read all terms and conditions carefully.

Auxiliary Memberships

Institutional Fellow of Open Association of Research Society (USA)-OARS (USA)

Global Journals Incorporation (USA) is accredited by Open Association of Research Society, U.S.A (OARS) and in turn, affiliates research institutions as "Institutional Fellow of Open Association of Research Society" (IFOARS).

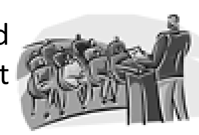
The "FARSC" is a dignified title which is accorded to a person's name viz. Dr. John E. Hall, Ph.D., FARSC or William Walldroff, M.S., FARSC.

The IFOARS institution is entitled to form a Board comprised of one Chairperson and three to five board members preferably from different streams. The Board will be recognized as "Institutional Board of Open Association of Research Society"-(IBOARS).

The Institute will be entitled to following benefits:

The IBOARS can initially review research papers of their institute and recommend them to publish with respective journal of Global Journals. It can also review the papers of other institutions after obtaining our consent. The second review will be done by peer reviewer of Global Journals Incorporation (USA) The Board is at liberty to appoint a peer reviewer with the approval of chairperson after consulting us.

The author fees of such paper may be waived off up to 40%.



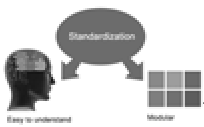
The Global Journals Incorporation (USA) at its discretion can also refer double blind peer reviewed paper at their end to the board for the verification and to get recommendation for final stage of acceptance of publication.

The IBOARS can organize symposium/seminar/conference in their country on behalf of Global Journals Incorporation (USA)-OARS (USA). The terms and conditions can be discussed separately.

The Board can also play vital role by exploring and giving valuable suggestions regarding the Standards of "Open Association of Research Society, U.S.A (OARS)" so that proper amendment can take place for the benefit of entire research community. We shall provide details of particular standard only on receipt of request from the Board.

The board members can also join us as Individual Fellow with 40% discount on total fees applicable to Individual Fellow. They will be entitled to avail all the benefits as declared. Please visit Individual Fellow-sub menu of GlobalJournals.org to have more relevant details.

We shall provide you intimation regarding launching of e-version of journal of your stream time to time. This may be utilized in your library for the enrichment of knowledge of your students as well as it can also be helpful for the concerned faculty members.



After nomination of your institution as “Institutional Fellow” and constantly functioning successfully for one year, we can consider giving recognition to your institute to function as Regional/Zonal office on our behalf.
The board can also take up the additional allied activities for betterment after our consultation.

The following entitlements are applicable to individual Fellows:

Open Association of Research Society, U.S.A (OARS) By-laws states that an individual Fellow may use the designations as applicable, or the corresponding initials. The Credentials of individual Fellow and Associate designations signify that the individual has gained knowledge of the fundamental concepts. One is magnanimous and proficient in an expertise course covering the professional code of conduct, and follows recognized standards of practice.

Open Association of Research Society (US)/ Global Journals Incorporation (USA), as described in Corporate Statements, are educational, research publishing and professional membership organizations. Achieving our individual Fellow or Associate status is based mainly on meeting stated educational research requirements.

Disbursement of 40% Royalty earned through Global Journals : Researcher = 50%, Peer Reviewer = 37.50%, Institution = 12.50% E.g. Out of 40%, the 20% benefit should be passed on to researcher, 15 % benefit towards remuneration should be given to a reviewer and remaining 5% is to be retained by the institution.

We shall provide print version of 12 issues of any three journals [as per your requirement] out of our 38 journals worth $ 2376 USD.

Other:

The individual Fellow and Associate designations accredited by Open Association of Research Society (US) credentials signify guarantees following achievements:

- The professional accredited with Fellow honor, is entitled to various benefits viz. name, fame, honor, regular flow of income, secured bright future, social status etc.

- In addition to above, if one is single author, then entitled to 40% discount on publishing research paper and can get 10%discount if one is co-author or main author among group of authors.
- The Fellow can organize symposium/seminar/conference on behalf of Global Journals Incorporation (USA) and he/she can also attend the same organized by other institutes on behalf of Global Journals.
- The Fellow can become member of Editorial Board Member after completing 3yrs.
- The Fellow can earn 60% of sales proceeds from the sale of reference/review books/literature/publishing of research paper.
- Fellow can also join as paid peer reviewer and earn 15% remuneration of author charges and can also get an opportunity to join as member of the Editorial Board of Global Journals Incorporation (USA)
- • This individual has learned the basic methods of applying those concepts and techniques to common challenging situations. This individual has further demonstrated an in–depth understanding of the application of suitable techniques to a particular area of research practice.

Note :

"

- In future, if the board feels the necessity to change any board member, the same can be done with the consent of the chairperson along with anyone board member without our approval.
- In case, the chairperson needs to be replaced then consent of 2/3rd board members are required and they are also required to jointly pass the resolution copy of which should be sent to us. In such case, it will be compulsory to obtain our approval before replacement.
- In case of "Difference of Opinion [if any]" among the Board members, our decision will be final and binding to everyone.

"

Process of submission of Research Paper

The Area or field of specialization may or may not be of any category as mentioned in 'Scope of Journal' menu of the GlobalJournals.org website. There are 37 Research Journal categorized with Six parental Journals GJCST, GJMR, GJRE, GJMBR, GJSFR, GJHSS. For Authors should prefer the mentioned categories. There are three widely used systems UDC, DDC and LCC. The details are available as 'Knowledge Abstract' at Home page. The major advantage of this coding is that, the research work will be exposed to and shared with all over the world as we are being abstracted and indexed worldwide.

The paper should be in proper format. The format can be downloaded from first page of 'Author Guideline' Menu. The Author is expected to follow the general rules as mentioned in this menu. The paper should be written in MS-Word Format (*.DOC,*.DOCX).

The Author can submit the paper either online or offline. The authors should prefer online submission.Online Submission: There are three ways to submit your paper:

(A) (I) First, register yourself using top right corner of Home page then Login. If you are already registered, then login using your username and password.

(II) Choose corresponding Journal.

(III) Click 'Submit Manuscript'. Fill required information and Upload the paper.

(B) If you are using Internet Explorer, then Direct Submission through Homepage is also available.

(C) If these two are not convenient, and then email the paper directly to dean@globaljournals.org.

Offline Submission: Author can send the typed form of paper by Post. However, online submission should be preferred.

Preferred Author Guidelines

MANUSCRIPT STYLE INSTRUCTION **(Must be strictly followed)**

Page Size: 8.27" X 11'"

- Left Margin: 0.65
- Right Margin: 0.65
- Top Margin: 0.75
- Bottom Margin: 0.75
- Font type of all text should be Swis 721 Lt BT.
- Paper Title should be of Font Size 24 with one Column section.
- Author Name in Font Size of 11 with one column as of Title.
- Abstract Font size of 9 Bold, “Abstract” word in Italic Bold.
- Main Text: Font size 10 with justified two columns section
- Two Column with Equal Column with of 3.38 and Gaping of .2
- First Character must be three lines Drop capped.
- Paragraph before Spacing of 1 pt and After of 0 pt.
- Line Spacing of 1 pt
- Large Images must be in One Column
- Numbering of First Main Headings (Heading 1) must be in Roman Letters, Capital Letter, and Font Size of 10.
- Numbering of Second Main Headings (Heading 2) must be in Alphabets, Italic, and Font Size of 10.

You can use your own standard format also.
Author Guidelines:

1. General,

2. Ethical Guidelines,

3. Submission of Manuscripts,

4. Manuscript’s Category,

5. Structure and Format of Manuscript,

6. After Acceptance.

1. GENERAL

Before submitting your research paper, one is advised to go through the details as mentioned in following heads. It will be beneficial, while peer reviewer justify your paper for publication.

Scope

The Global Journals Inc. (US) welcome the submission of original paper, review paper, survey article relevant to the all the streams of Philosophy and knowledge. The Global Journals Inc. (US) is parental platform for Global Journal of Computer Science and Technology, Researches in Engineering, Medical Research, Science Frontier Research, Human Social Science, Management, and Business organization. The choice of specific field can be done otherwise as following in Abstracting and Indexing Page on this Website. As the all Global

Journals Inc. (US) are being abstracted and indexed (in process) by most of the reputed organizations. Topics of only narrow interest will not be accepted unless they have wider potential or consequences.

2. ETHICAL GUIDELINES

Authors should follow the ethical guidelines as mentioned below for publication of research paper and research activities.

Papers are accepted on strict understanding that the material in whole or in part has not been, nor is being, considered for publication elsewhere. If the paper once accepted by Global Journals Inc. (US) and Editorial Board, will become the copyright of the Global Journals Inc. (US).

Authorship: The authors and coauthors should have active contribution to conception design, analysis and interpretation of findings. They should critically review the contents and drafting of the paper. All should approve the final version of the paper before submission

The Global Journals Inc. (US) follows the definition of authorship set up by the Global Academy of Research and Development. According to the Global Academy of R&D authorship, criteria must be based on:

1) Substantial contributions to conception and acquisition of data, analysis and interpretation of the findings.

2) Drafting the paper and revising it critically regarding important academic content.

3) Final approval of the version of the paper to be published.

All authors should have been credited according to their appropriate contribution in research activity and preparing paper. Contributors who do not match the criteria as authors may be mentioned under Acknowledgement.

Acknowledgements: Contributors to the research other than authors credited should be mentioned under acknowledgement. The specifications of the source of funding for the research if appropriate can be included. Suppliers of resources may be mentioned along with address.

Appeal of Decision: The Editorial Board's decision on publication of the paper is final and cannot be appealed elsewhere.

Permissions: It is the author's responsibility to have prior permission if all or parts of earlier published illustrations are used in this paper.

Please mention proper reference and appropriate acknowledgements wherever expected.

If all or parts of previously published illustrations are used, permission must be taken from the copyright holder concerned. It is the author's responsibility to take these in writing.

Approval for reproduction/modification of any information (including figures and tables) published elsewhere must be obtained by the authors/copyright holders before submission of the manuscript. Contributors (Authors) are responsible for any copyright fee involved.

3. SUBMISSION OF MANUSCRIPTS

Manuscripts should be uploaded via this online submission page. The online submission is most efficient method for submission of papers, as it enables rapid distribution of manuscripts and consequently speeds up the review procedure. It also enables authors to know the status of their own manuscripts by emailing us. Complete instructions for submitting a paper is available below.

Manuscript submission is a systematic procedure and little preparation is required beyond having all parts of your manuscript in a given format and a computer with an Internet connection and a Web browser. Full help and instructions are provided on-screen. As an author, you will be prompted for login and manuscript details as Field of Paper and then to upload your manuscript file(s) according to the instructions.

To avoid postal delays, all transaction is preferred by e-mail. A finished manuscript submission is confirmed by e-mail immediately and your paper enters the editorial process with no postal delays. When a conclusion is made about the publication of your paper by our Editorial Board, revisions can be submitted online with the same procedure, with an occasion to view and respond to all comments.

Complete support for both authors and co-author is provided.

4. MANUSCRIPT'S CATEGORY

Based on potential and nature, the manuscript can be categorized under the following heads:

Original research paper: Such papers are reports of high-level significant original research work.

Review papers: These are concise, significant but helpful and decisive topics for young researchers.

Research articles: These are handled with small investigation and applications.

Research letters: The letters are small and concise comments on previously published matters.

5. STRUCTURE AND FORMAT OF MANUSCRIPT

The recommended size of original research paper is less than seven thousand words, review papers fewer than seven thousands words also.Preparation of research paper or how to write research paper, are major hurdle, while writing manuscript. The research articles and research letters should be fewer than three thousand words, the structure original research paper; sometime review paper should be as follows:

Papers: These are reports of significant research (typically less than 7000 words equivalent, including tables, figures, references), and comprise:

(a)Title should be relevant and commensurate with the theme of the paper.

(b) A brief Summary, "Abstract" (less than 150 words) containing the major results and conclusions.

(c) Up to ten keywords, that precisely identifies the paper's subject, purpose, and focus.

(d) An Introduction, giving necessary background excluding subheadings; objectives must be clearly declared.

(e) Resources and techniques with sufficient complete experimental details (wherever possible by reference) to permit repetition; sources of information must be given and numerical methods must be specified by reference, unless non-standard.

(f) Results should be presented concisely, by well-designed tables and/or figures; the same data may not be used in both; suitable statistical data should be given. All data must be obtained with attention to numerical detail in the planning stage. As reproduced design has been recognized to be important to experiments for a considerable time, the Editor has decided that any paper that appears not to have adequate numerical treatments of the data will be returned un-refereed;

(g) Discussion should cover the implications and consequences, not just recapitulating the results; conclusions should be summarizing.

(h) Brief Acknowledgements.

(i) References in the proper form.

Authors should very cautiously consider the preparation of papers to ensure that they communicate efficiently. Papers are much more likely to be accepted, if they are cautiously designed and laid out, contain few or no errors, are summarizing, and be conventional to the approach and instructions. They will in addition, be published with much less delays than those that require much technical and editorial correction.

The Editorial Board reserves the right to make literary corrections and to make suggestions to improve briefness.

It is vital, that authors take care in submitting a manuscript that is written in simple language and adheres to published guidelines.

Format

Language: The language of publication is UK English. Authors, for whom English is a second language, must have their manuscript efficiently edited by an English-speaking person before submission to make sure that, the English is of high excellence. It is preferable, that manuscripts should be professionally edited.

Standard Usage, Abbreviations, and Units: Spelling and hyphenation should be conventional to The Concise Oxford English Dictionary. Statistics and measurements should at all times be given in figures, e.g. 16 min, except for when the number begins a sentence. When the number does not refer to a unit of measurement it should be spelt in full unless, it is 160 or greater.

Abbreviations supposed to be used carefully. The abbreviated name or expression is supposed to be cited in full at first usage, followed by the conventional abbreviation in parentheses.

Metric SI units are supposed to generally be used excluding where they conflict with current practice or are confusing. For illustration, 1.4 l rather than 1.4 × 10-3 m3, or 4 mm somewhat than 4 × 10-3 m. Chemical formula and solutions must identify the form used, e.g. anhydrous or hydrated, and the concentration must be in clearly defined units. Common species names should be followed by underlines at the first mention. For following use the generic name should be constricted to a single letter, if it is clear.

Structure

All manuscripts submitted to Global Journals Inc. (US), ought to include:

Title: The title page must carry an instructive title that reflects the content, a running title (less than 45 characters together with spaces), names of the authors and co-authors, and the place(s) wherever the work was carried out. The full postal address in addition with the e-mail address of related author must be given. Up to eleven keywords or very brief phrases have to be given to help data retrieval, mining and indexing.

Abstract, used in Original Papers and Reviews:

Optimizing Abstract for Search Engines

Many researchers searching for information online will use search engines such as Google, Yahoo or similar. By optimizing your paper for search engines, you will amplify the chance of someone finding it. This in turn will make it more likely to be viewed and/or cited in a further work. Global Journals Inc. (US) have compiled these guidelines to facilitate you to maximize the web-friendliness of the most public part of your paper.

Key Words

A major linchpin in research work for the writing research paper is the keyword search, which one will employ to find both library and Internet resources.

One must be persistent and creative in using keywords. An effective keyword search requires a strategy and planning a list of possible keywords and phrases to try.

Search engines for most searches, use Boolean searching, which is somewhat different from Internet searches. The Boolean search uses "operators," words (and, or, not, and near) that enable you to expand or narrow your affords. Tips for research paper while preparing research paper are very helpful guideline of research paper.

Choice of key words is first tool of tips to write research paper. Research paper writing is an art.A few tips for deciding as strategically as possible about keyword search:

- One should start brainstorming lists of possible keywords before even begin searching. Think about the most important concepts related to research work. Ask, "What words would a source have to include to be truly valuable in research paper?" Then consider synonyms for the important words.
- It may take the discovery of only one relevant paper to let steer in the right keyword direction because in most databases, the keywords under which a research paper is abstracted are listed with the paper.
- One should avoid outdated words.

Keywords are the key that opens a door to research work sources. Keyword searching is an art in which researcher's skills are bound to improve with experience and time.

Numerical Methods: Numerical methods used should be clear and, where appropriate, supported by references.

Acknowledgements: Please make these as concise as possible.

References

References follow the Harvard scheme of referencing. References in the text should cite the authors' names followed by the time of their publication, unless there are three or more authors when simply the first author's name is quoted followed by et al. unpublished work has to only be cited where necessary, and only in the text. Copies of references in press in other journals have to be supplied with submitted typescripts. It is necessary that all citations and references be carefully checked before submission, as mistakes or omissions will cause delays.

References to information on the World Wide Web can be given, but only if the information is available without charge to readers on an official site. Wikipedia and Similar websites are not allowed where anyone can change the information. Authors will be asked to make available electronic copies of the cited information for inclusion on the Global Journals Inc. (US) homepage at the judgment of the Editorial Board.

The Editorial Board and Global Journals Inc. (US) recommend that, citation of online-published papers and other material should be done via a DOI (digital object identifier). If an author cites anything, which does not have a DOI, they run the risk of the cited material not being noticeable.

The Editorial Board and Global Journals Inc. (US) recommend the use of a tool such as Reference Manager for reference management and formatting.

Tables, Figures and Figure Legends

Tables: Tables should be few in number, cautiously designed, uncrowned, and include only essential data. Each must have an Arabic number, e.g. Table 4, a self-explanatory caption and be on a separate sheet. Vertical lines should not be used.

Figures: Figures are supposed to be submitted as separate files. Always take in a citation in the text for each figure using Arabic numbers, e.g. Fig. 4. Artwork must be submitted online in electronic form by e-mailing them.

Preparation of Electronic Figures for Publication

Even though low quality images are sufficient for review purposes, print publication requires high quality images to prevent the final product being blurred or fuzzy. Submit (or e-mail) EPS (line art) or TIFF (halftone/photographs) files only. MS PowerPoint and Word Graphics are unsuitable for printed pictures. Do not use pixel-oriented software. Scans (TIFF only) should have a resolution of at least 350 dpi (halftone) or 700 to 1100 dpi (line drawings) in relation to the imitation size. Please give the data for figures in black and white or submit a Color Work Agreement Form. EPS files must be saved with fonts embedded (and with a TIFF preview, if possible).

For scanned images, the scanning resolution (at final image size) ought to be as follows to ensure good reproduction: line art: >650 dpi; halftones (including gel photographs) : >350 dpi; figures containing both halftone and line images: >650 dpi.

Color Charges: It is the rule of the Global Journals Inc. (US) for authors to pay the full cost for the reproduction of their color artwork. Hence, please note that, if there is color artwork in your manuscript when it is accepted for publication, we would require you to complete and return a color work agreement form before your paper can be published.

Figure Legends: Self-explanatory legends of all figures should be incorporated separately under the heading 'Legends to Figures'. In the full-text online edition of the journal, figure legends may possibly be truncated in abbreviated links to the full screen version. Therefore, the first 100 characters of any legend should notify the reader, about the key aspects of the figure.

6. AFTER ACCEPTANCE

Upon approval of a paper for publication, the manuscript will be forwarded to the dean, who is responsible for the publication of the Global Journals Inc. (US).

6.1 Proof Corrections

The corresponding author will receive an e-mail alert containing a link to a website or will be attached. A working e-mail address must therefore be provided for the related author.

Acrobat Reader will be required in order to read this file. This software can be downloaded

(Free of charge) from the following website:

www.adobe.com/products/acrobat/readstep2.html. This will facilitate the file to be opened, read on screen, and printed out in order for any corrections to be added. Further instructions will be sent with the proof.

Proofs must be returned to the dean at dean@globaljournals.org within three days of receipt.

As changes to proofs are costly, we inquire that you only correct typesetting errors. All illustrations are retained by the publisher. Please note that the authors are responsible for all statements made in their work, including changes made by the copy editor.

6.2 Early View of Global Journals Inc. (US) (Publication Prior to Print)

The Global Journals Inc. (US) are enclosed by our publishing's Early View service. Early View articles are complete full-text articles sent in advance of their publication. Early View articles are absolute and final. They have been completely reviewed, revised and edited for publication, and the authors' final corrections have been incorporated. Because they are in final form, no changes can be made after sending them. The nature of Early View articles means that they do not yet have volume, issue or page numbers, so Early View articles cannot be cited in the conventional way.

6.3 Author Services

Online production tracking is available for your article through Author Services. Author Services enables authors to track their article - once it has been accepted - through the production process to publication online and in print. Authors can check the status of their articles online and choose to receive automated e-mails at key stages of production. The authors will receive an e-mail with a unique link that enables them to register and have their article automatically added to the system. Please ensure that a complete e-mail address is provided when submitting the manuscript.

6.4 Author Material Archive Policy

Please note that if not specifically requested, publisher will dispose off hardcopy & electronic information submitted, after the two months of publication. If you require the return of any information submitted, please inform the Editorial Board or dean as soon as possible.

6.5 Offprint and Extra Copies

A PDF offprint of the online-published article will be provided free of charge to the related author, and may be distributed according to the Publisher's terms and conditions. Additional paper offprint may be ordered by emailing us at: editor@globaljournals.org .

You must strictly follow above Author Guidelines before submitting your paper or else we will not at all be responsible for any corrections in future in any of the way.

Before start writing a good quality Computer Science Research Paper, let us first understand what is Computer Science Research Paper? So, Computer Science Research Paper is the paper which is written by professionals or scientists who are associated to Computer Science and Information Technology, or doing research study in these areas. If you are novel to this field then you can consult about this field from your supervisor or guide.

TECHNIQUES FOR WRITING A GOOD QUALITY RESEARCH PAPER:

1. Choosing the topic: In most cases, the topic is searched by the interest of author but it can be also suggested by the guides. You can have several topics and then you can judge that in which topic or subject you are finding yourself most comfortable. This can be done by asking several questions to yourself, like Will I be able to carry our search in this area? Will I find all necessary recourses to accomplish the search? Will I be able to find all information in this field area? If the answer of these types of questions will be "Yes" then you can choose that topic. In most of the cases, you may have to conduct the surveys and have to visit several places because this field is related to Computer Science and Information Technology. Also, you may have to do a lot of work to find all rise and falls regarding the various data of that subject. Sometimes, detailed information plays a vital role, instead of short information.

2. Evaluators are human: First thing to remember that evaluators are also human being. They are not only meant for rejecting a paper. They are here to evaluate your paper. So, present your Best.

3. Think Like Evaluators: If you are in a confusion or getting demotivated that your paper will be accepted by evaluators or not, then think and try to evaluate your paper like an Evaluator. Try to understand that what an evaluator wants in your research paper and automatically you will have your answer.

4. Make blueprints of paper: The outline is the plan or framework that will help you to arrange your thoughts. It will make your paper logical. But remember that all points of your outline must be related to the topic you have chosen.

5. Ask your Guides: If you are having any difficulty in your research, then do not hesitate to share your difficulty to your guide (if you have any). They will surely help you out and resolve your doubts. If you can't clarify what exactly you require for your work then ask the supervisor to help you with the alternative. He might also provide you the list of essential readings.

6. Use of computer is recommended: As you are doing research in the field of Computer Science, then this point is quite obvious.

7. Use right software: Always use good quality software packages. If you are not capable to judge good software then you can lose quality of your paper unknowingly. There are various software programs available to help you, which you can get through Internet.

8. Use the Internet for help: An excellent start for your paper can be by using the Google. It is an excellent search engine, where you can have your doubts resolved. You may also read some answers for the frequent question how to write my research paper or find model research paper. From the internet library you can download books. If you have all required books make important reading selecting and analyzing the specified information. Then put together research paper sketch out.

9. Use and get big pictures: Always use encyclopedias, Wikipedia to get pictures so that you can go into the depth.

10. Bookmarks are useful: When you read any book or magazine, you generally use bookmarks, right! It is a good habit, which helps to not to lose your continuity. You should always use bookmarks while searching on Internet also, which will make your search easier.

11. Revise what you wrote: When you write anything, always read it, summarize it and then finalize it.

12. Make all efforts: Make all efforts to mention what you are going to write in your paper. That means always have a good start. Try to mention everything in introduction, that what is the need of a particular research paper. Polish your work by good skill of writing and always give an evaluator, what he wants.

13. Have backups: When you are going to do any important thing like making research paper, you should always have backup copies of it either in your computer or in paper. This will help you to not to lose any of your important.

14. Produce good diagrams of your own: Always try to include good charts or diagrams in your paper to improve quality. Using several and unnecessary diagrams will degrade the quality of your paper by creating "hotchpotch." So always, try to make and include those diagrams, which are made by your own to improve readability and understandability of your paper.

15. Use of direct quotes: When you do research relevant to literature, history or current affairs then use of quotes become essential but if study is relevant to science then use of quotes is not preferable.

16. Use proper verb tense: Use proper verb tenses in your paper. Use past tense, to present those events that happened. Use present tense to indicate events that are going on. Use future tense to indicate future happening events. Use of improper and wrong tenses will confuse the evaluator. Avoid the sentences that are incomplete.

17. Never use online paper: If you are getting any paper on Internet, then never use it as your research paper because it might be possible that evaluator has already seen it or maybe it is outdated version.

18. Pick a good study spot: To do your research studies always try to pick a spot, which is quiet. Every spot is not for studies. Spot that suits you choose it and proceed further.

19. Know what you know: Always try to know, what you know by making objectives. Else, you will be confused and cannot achieve your target.

20. Use good quality grammar: Always use a good quality grammar and use words that will throw positive impact on evaluator. Use of good quality grammar does not mean to use tough words, that for each word the evaluator has to go through dictionary. Do not start sentence with a conjunction. Do not fragment sentences. Eliminate one-word sentences. Ignore passive voice. Do not ever use a big word when a diminutive one would suffice. Verbs have to be in agreement with their subjects. Prepositions are not expressions to finish sentences with. It is incorrect to ever divide an infinitive. Avoid clichés like the disease. Also, always shun irritating alliteration. Use language that is simple and straight forward. put together a neat summary.

21. Arrangement of information: Each section of the main body should start with an opening sentence and there should be a changeover at the end of the section. Give only valid and powerful arguments to your topic. You may also maintain your arguments with records.

22. Never start in last minute: Always start at right time and give enough time to research work. Leaving everything to the last minute will degrade your paper and spoil your work.

23. Multitasking in research is not good: Doing several things at the same time proves bad habit in case of research activity. Research is an area, where everything has a particular time slot. Divide your research work in parts and do particular part in particular time slot.

24. Never copy others' work: Never copy others' work and give it your name because if evaluator has seen it anywhere you will be in trouble.

25. Take proper rest and food: No matter how many hours you spend for your research activity, if you are not taking care of your health then all your efforts will be in vain. For a quality research, study is must, and this can be done by taking proper rest and food.

26. Go for seminars: Attend seminars if the topic is relevant to your research area. Utilize all your resources.

27. Refresh your mind after intervals: Try to give rest to your mind by listening to soft music or by sleeping in intervals. This will also improve your memory.

28. Make colleagues: Always try to make colleagues. No matter how sharper or intelligent you are, if you make colleagues you can have several ideas, which will be helpful for your research.

29. Think technically: Always think technically. If anything happens, then search its reasons, its benefits, and demerits.

30. Think and then print: When you will go to print your paper, notice that tables are not be split, headings are not detached from their descriptions, and page sequence is maintained.

31. Adding unnecessary information: Do not add unnecessary information, like, I have used MS Excel to draw graph. Do not add irrelevant and inappropriate material. These all will create superfluous. Foreign terminology and phrases are not apropos. One should NEVER take a broad view. Analogy in script is like feathers on a snake. Not at all use a large word when a very small one would be sufficient. Use words properly, regardless of how others use them. Remove quotations. Puns are for kids, not grunt readers. Amplification is a billion times of inferior quality than sarcasm.

32. Never oversimplify everything: To add material in your research paper, never go for oversimplification. This will definitely irritate the evaluator. Be more or less specific. Also too, by no means, ever use rhythmic redundancies. Contractions aren't essential and shouldn't be there used. Comparisons are as terrible as clichés. Give up ampersands and abbreviations, and so on. Remove commas, that are, not necessary. Parenthetical words however should be together with this in commas. Understatement is all the time the complete best way to put onward earth-shaking thoughts. Give a detailed literary review.

33. Report concluded results: Use concluded results. From raw data, filter the results and then conclude your studies based on measurements and observations taken. Significant figures and appropriate number of decimal places should be used. Parenthetical remarks are prohibitive. Proofread carefully at final stage. In the end give outline to your arguments. Spot out perspectives of further study of this subject. Justify your conclusion by at the bottom of them with sufficient justifications and examples.

34. After conclusion: Once you have concluded your research, the next most important step is to present your findings. Presentation is extremely important as it is the definite medium though which your research is going to be in print to the rest of the crowd. Care should be taken to categorize your thoughts well and present them in a logical and neat manner. A good quality research paper format is essential because it serves to highlight your research paper and bring to light all necessary aspects in your research.

Informal Guidelines of Research Paper Writing

Key points to remember:

- Submit all work in its final form.
- Write your paper in the form, which is presented in the guidelines using the template.
- Please note the criterion for grading the final paper by peer-reviewers.

Final Points:

A purpose of organizing a research paper is to let people to interpret your effort selectively. The journal requires the following sections, submitted in the order listed, each section to start on a new page.

The introduction will be compiled from reference matter and will reflect the design processes or outline of basis that direct you to make study. As you will carry out the process of study, the method and process section will be constructed as like that. The result segment will show related statistics in nearly sequential order and will direct the reviewers next to the similar intellectual paths throughout the data that you took to carry out your study. The discussion section will provide understanding of the data and projections as to the implication of the results. The use of good quality references all through the paper will give the effort trustworthiness by representing an alertness of prior workings.

Writing a research paper is not an easy job no matter how trouble-free the actual research or concept. Practice, excellent preparation, and controlled record keeping are the only means to make straightforward the progression.

General style:

Specific editorial column necessities for compliance of a manuscript will always take over from directions in these general guidelines.

To make a paper clear

· Adhere to recommended page limits

Mistakes to evade

- Insertion a title at the foot of a page with the subsequent text on the next page
- Separating a table/chart or figure - impound each figure/table to a single page
- Submitting a manuscript with pages out of sequence

In every sections of your document

· Use standard writing style including articles ("a", "the," etc.)

· Keep on paying attention on the research topic of the paper

· Use paragraphs to split each significant point (excluding for the abstract)

· Align the primary line of each section

· Present your points in sound order

· Use present tense to report well accepted

· Use past tense to describe specific results

· Shun familiar wording, don't address the reviewer directly, and don't use slang, slang language, or superlatives

· Shun use of extra pictures - include only those figures essential to presenting results

Title Page:

Choose a revealing title. It should be short. It should not have non-standard acronyms or abbreviations. It should not exceed two printed lines. It should include the name(s) and address (es) of all authors.

Abstract:

The summary should be two hundred words or less. It should briefly and clearly explain the key findings reported in the manuscript--must have precise statistics. It should not have abnormal acronyms or abbreviations. It should be logical in itself. Shun citing references at this point.

An abstract is a brief distinct paragraph summary of finished work or work in development. In a minute or less a reviewer can be taught the foundation behind the study, common approach to the problem, relevant results, and significant conclusions or new questions.

Write your summary when your paper is completed because how can you write the summary of anything which is not yet written? Wealth of terminology is very essential in abstract. Yet, use comprehensive sentences and do not let go readability for briefness. You can maintain it succinct by phrasing sentences so that they provide more than lone rationale. The author can at this moment go straight to shortening the outcome. Sum up the study, with the subsequent elements in any summary. Try to maintain the initial two items to no more than one ruling each.

- Reason of the study - theory, overall issue, purpose
- Fundamental goal
- To the point depiction of the research
- Consequences, including definite statistics - if the consequences are quantitative in nature, account quantitative data; results of any numerical analysis should be reported
- Significant conclusions or questions that track from the research(es)

Approach:

- Single section, and succinct
- As a outline of job done, it is always written in past tense
- A conceptual should situate on its own, and not submit to any other part of the paper such as a form or table
- Center on shortening results - bound background information to a verdict or two, if completely necessary
- What you account in an conceptual must be regular with what you reported in the manuscript
- Exact spelling, clearness of sentences and phrases, and appropriate reporting of quantities (proper units, important statistics) are just as significant in an abstract as they are anywhere else

Introduction:

The **Introduction** should "introduce" the manuscript. The reviewer should be presented with sufficient background information to be capable to comprehend and calculate the purpose of your study without having to submit to other works. The basis for the study should be offered. Give most important references but shun difficult to make a comprehensive appraisal of the topic. In the introduction, describe the problem visibly. If the problem is not acknowledged in a logical, reasonable way, the reviewer will have no attention in your result. Speak in common terms about techniques used to explain the problem, if needed, but do not present any particulars about the protocols here. Following approach can create a valuable beginning:

- Explain the value (significance) of the study
- Shield the model - why did you employ this particular system or method? What is its compensation? You strength remark on its appropriateness from a abstract point of vision as well as point out sensible reasons for using it.
- Present a justification. Status your particular theory (es) or aim(s), and describe the logic that led you to choose them.
- Very for a short time explain the tentative propose and how it skilled the declared objectives.

Approach:

- Use past tense except for when referring to recognized facts. After all, the manuscript will be submitted after the entire job is done.
- Sort out your thoughts; manufacture one key point with every section. If you make the four points listed above, you will need a least of four paragraphs.

- Present surroundings information only as desirable in order hold up a situation. The reviewer does not desire to read the whole thing you know about a topic.
- Shape the theory/purpose specifically - do not take a broad view.
- As always, give awareness to spelling, simplicity and correctness of sentences and phrases.

Procedures (Methods and Materials):

This part is supposed to be the easiest to carve if you have good skills. A sound written Procedures segment allows a capable scientist to replacement your results. Present precise information about your supplies. The suppliers and clarity of reagents can be helpful bits of information. Present methods in sequential order but linked methodologies can be grouped as a segment. Be concise when relating the protocols. Attempt for the least amount of information that would permit another capable scientist to spare your outcome but be cautious that vital information is integrated. The use of subheadings is suggested and ought to be synchronized with the results section. When a technique is used that has been well described in another object, mention the specific item describing a way but draw the basic principle while stating the situation. The purpose is to text all particular resources and broad procedures, so that another person may use some or all of the methods in one more study or referee the scientific value of your work. It is not to be a step by step report of the whole thing you did, nor is a methods section a set of orders.

Materials:

- Explain materials individually only if the study is so complex that it saves liberty this way.
- Embrace particular materials, and any tools or provisions that are not frequently found in laboratories.
- Do not take in frequently found.
- If use of a definite type of tools.
- Materials may be reported in a part section or else they may be recognized along with your measures.

Methods:

- Report the method (not particulars of each process that engaged the same methodology)
- Describe the method entirely
- To be succinct, present methods under headings dedicated to specific dealings or groups of measures
- Simplify - details how procedures were completed not how they were exclusively performed on a particular day.
- If well known procedures were used, account the procedure by name, possibly with reference, and that's all.

Approach:

- It is embarrassed or not possible to use vigorous voice when documenting methods with no using first person, which would focus the reviewer's interest on the researcher rather than the job. As a result when script up the methods most authors use third person passive voice.
- Use standard style in this and in every other part of the paper - avoid familiar lists, and use full sentences.

What to keep away from

- Resources and methods are not a set of information.
- Skip all descriptive information and surroundings - save it for the argument.
- Leave out information that is immaterial to a third party.

Results:

The principle of a results segment is to present and demonstrate your conclusion. Create this part a entirely objective details of the outcome, and save all understanding for the discussion.

The page length of this segment is set by the sum and types of data to be reported. Carry on to be to the point, by means of statistics and tables, if suitable, to present consequences most efficiently.You must obviously differentiate material that would usually be incorporated in a study editorial from any unprocessed data or additional appendix matter that would not be available. In fact, such matter should not be submitted at all except requested by the instructor.

Content

- Sum up your conclusion in text and demonstrate them, if suitable, with figures and tables.
- In manuscript, explain each of your consequences, point the reader to remarks that are most appropriate.
- Present a background, such as by describing the question that was addressed by creation an exacting study.
- Explain results of control experiments and comprise remarks that are not accessible in a prescribed figure or table, if appropriate.
- Examine your data, then prepare the analyzed (transformed) data in the form of a figure (graph), table, or in manuscript form.

What to stay away from

- Do not discuss or infer your outcome, report surroundings information, or try to explain anything.
- Not at all, take in raw data or intermediate calculations in a research manuscript.
- Do not present the similar data more than once.
- Manuscript should complement any figures or tables, not duplicate the identical information.
- Never confuse figures with tables - there is a difference.

Approach

- As forever, use past tense when you submit to your results, and put the whole thing in a reasonable order.
- Put figures and tables, appropriately numbered, in order at the end of the report
- If you desire, you may place your figures and tables properly within the text of your results part.

Figures and tables

- If you put figures and tables at the end of the details, make certain that they are visibly distinguished from any attach appendix materials, such as raw facts
- Despite of position, each figure must be numbered one after the other and complete with subtitle
- In spite of position, each table must be titled, numbered one after the other and complete with heading
- All figure and table must be adequately complete that it could situate on its own, divide from text

Discussion:

The Discussion is expected the trickiest segment to write and describe. A lot of papers submitted for journal are discarded based on problems with the Discussion. There is no head of state for how long a argument should be. Position your understanding of the outcome visibly to lead the reviewer through your conclusions, and then finish the paper with a summing up of the implication of the study. The purpose here is to offer an understanding of your results and hold up for all of your conclusions, using facts from your research and generally accepted information, if suitable. The implication of result should be visibly described. Infer your data in the conversation in suitable depth. This means that when you clarify an observable fact you must explain mechanisms that may account for the observation. If your results vary from your prospect, make clear why that may have happened. If your results agree, then explain the theory that the proof supported. It is never suitable to just state that the data approved with prospect, and let it drop at that.

- Make a decision if each premise is supported, discarded, or if you cannot make a conclusion with assurance. Do not just dismiss a study or part of a study as "uncertain."
- Research papers are not acknowledged if the work is imperfect. Draw what conclusions you can based upon the results that you have, and take care of the study as a finished work
- You may propose future guidelines, such as how the experiment might be personalized to accomplish a new idea.
- Give details all of your remarks as much as possible, focus on mechanisms.
- Make a decision if the tentative design sufficiently addressed the theory, and whether or not it was correctly restricted.
- Try to present substitute explanations if sensible alternatives be present.
- One research will not counter an overall question, so maintain the large picture in mind, where do you go next? The best studies unlock new avenues of study. What questions remain?
- Recommendations for detailed papers will offer supplementary suggestions.

Approach:

- When you refer to information, differentiate data generated by your own studies from available information
- Submit to work done by specific persons (including you) in past tense.
- Submit to generally acknowledged facts and main beliefs in present tense.

Please carefully note down following rules and regulation before submitting your Research Paper to Global Journals Inc. (US):

Segment Draft and Final Research Paper: You have to strictly follow the template of research paper. If it is not done your paper may get rejected.

- The **major constraint** is that you must independently make all content, tables, graphs, and facts that are offered in the paper. You must write each part of the paper wholly on your own. The Peer-reviewers need to identify your own perceptive of the concepts in your own terms. NEVER extract straight from any foundation, and never rephrase someone else's analysis.

- Do not give permission to anyone else to "PROOFREAD" your manuscript.

- Methods to avoid Plagiarism is applied by us on every paper, if found guilty, you will be blacklisted by all of our collaborated research groups, your institution will be informed for this and strict legal actions will be taken immediately.)
- To guard yourself and others from possible illegal use please do not permit anyone right to use to your paper and files.

Criterion for Grading a Research Paper (Compilation) by Global Journals Inc. (US)

Please note that following table is only a Grading of "Paper Compilation" and not on "Performed/Stated Research" whose grading solely depends on Individual Assigned Peer Reviewer and Editorial Board Member. These can be available only on request and after decision of Paper. This report will be the property of Global Journals Inc. (US).

Topics	Grades		
	A-B	**C-D**	**E-F**
Abstract	Clear and concise with appropriate content, Correct format. 200 words or below	Unclear summary and no specific data, Incorrect form Above 200 words	No specific data with ambiguous information Above 250 words
Introduction	Containing all background details with clear goal and appropriate details, flow specification, no grammar and spelling mistake, well organized sentence and paragraph, reference cited	Unclear and confusing data, appropriate format, grammar and spelling errors with unorganized matter	Out of place depth and content, hazy format
Methods and Procedures	Clear and to the point with well arranged paragraph, precision and accuracy of facts and figures, well organized subheads	Difficult to comprehend with embarrassed text, too much explanation but completed	Incorrect and unorganized structure with hazy meaning
Result	Well organized, Clear and specific, Correct units with precision, correct data, well structuring of paragraph, no grammar and spelling mistake	Complete and embarrassed text, difficult to comprehend	Irregular format with wrong facts and figures
Discussion	Well organized, meaningful specification, sound conclusion, logical and concise explanation, highly structured paragraph reference cited	Wordy, unclear conclusion, spurious	Conclusion is not cited, unorganized, difficult to comprehend
References	Complete and correct format, well organized	Beside the point, Incomplete	Wrong format and structuring

Index

A

B

C

D

E

I

L

P

S

save our planet

Global Journal of Computer Science and Technology

Visit us on the Web at www.GlobalJournals.org | www.ComputerResearch.org
or email us at helpdesk@globaljournals.org

ISSN 9754350