Modeling an Enhanced Intrusion Detection System using Mobile Agent: A Methodological Framework

Isah Olawale Mustapha
Al_Hikmah University Ilorin, Nigeria
salnet2002@yahoo.com

R. G. Jimoh
University of Ilorin, Ilorin, Nigeria
jimoh_rasheed@yahoo.com

ABSTRACT
Increase demand by all and sundry for internet and share network, has enhanced the development of various network technology that has linked together different people of different motives, consequently it has paved way for malicious and unauthorized user to intrude into information resources of organization. As a result of the advantage embedded in the layered framework and those of signature base approach proposed by a number of earlier researchers, this research proposed an hybridized framework with the use of two comparators for detection of intrusion using secured, collaborative and optimum numbers of mobile agents. The framework if implemented is expected to be of better efficiency with respect to time of detection, storage space and reduction of network congestion.

CCS Concepts
• Security and privacy →Intrusion/anomaly detection and malware mitigation → Intrusion Detection systems

Keywords
Intrusion, Intrusion Detection System, Mobile Agent, Dijkstra Algorithm.

1. INTRODUCTION
Most companies, institutions and organizations today rely on information for decision making [4]. Hence, other things being equal, the efficiency of any organization today depends on how well it can secure its information resources especially through the use of computer system [30]. Apart from that, computer system also responds to issues based on available resources and information that are presented to it [5]. More so, resources and information sharing are the two primary objectives of setting up a computer network such information and resources serve as a major factor in attaining and sustaining competitive advantage in the emerging information driven organizations [16].

This among other factors, led the world into ubiquitous computing with e-banking ,e-commerce, e-messages, e-training and so on as its dividend, this however does not come without its challenges as it equally paved ways for intruder and unauthorized user to gain undue access to certain sensitive information [17].

CoRI'16, Sept 7–9, 2016, Ibadan, Nigeria.

A number of previous researchers in the field of information security equally testify to the fact that information is becoming more vulnerable [17]. Computer network consists of heterogeneous entities that include all kinds of processors, communication devices, and different human beings with different motives. Along with the heterogeneous nature of each of the entities on computer network, the entities have continuously diversify exponentially over the years [9].

The internet traffic together with it's data and other resources is on the increasing trend and it is projected to maintain such trend as far back as 2009 [9]. This is illustrated in Figure 1.

Consequently, network overload, delay in network transmission, insufficient storage facilities, inadequate information, insufficient resources, traffic congestions that result to dropping of packet along the channel of transmission, increase computational bottleneck on the central processing modules of applications and total coordination of network affairs become a problem [9]. These factors among others are posing insecurity problem to the computer network and are creating more avenues for intrusion [21]

[32] also stated that Some vital information that are disseminated within institutions, offices, across offices, between branches of an organization and different types of establishment today atimes get to the hands of an unauthorized persons who tampered with the contents of the information, therefore there is need to put some security measures in place, capable of detecting intrusion attempt promptly across every network settings otherwise lots of valuable data and other sensitive information may continue to experience threats such as impersonation, corruption, repudiation, break-in or denial of services which can cause serious danger on the individual or organization that are concerned.

Insecurity as a result of intrusion has been a teething problem that has been scaring user of computer network, despite the inevitable benefit derived from it.

On 20th Feb. 2012 there was a report by Jinshan that China"s internet security shows that network insecurity incidents are on a rising trend. This shows a global trend in the information security threat.

In a null shell, the problem of information and network insecurity especially by virtue of intrusion has become more rampant, prominent, complicated and dynamic along with the rapid development of network technology, and up till now the network security technology has not been able to eradicate intrusion [25]. Hence, there is need for enhancement of the current intrusion detection technologies capable of prompt detection. Such system design should not add too much load to the network and must be fast for better detection.

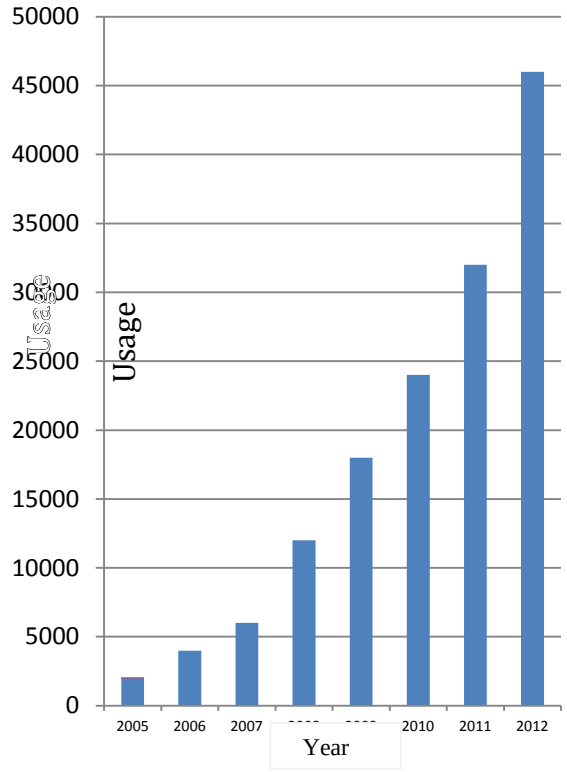


Figure 1. Internet Usage Trend (Holz, David, & Timoteo, 2011)

2. PROBLEM STATEMENT

As much as the use of computer network even internet is inevitable in the emerging information driven world, rapid development and increase demand for internet has pave way for malicious user to illegally intrude into computer network [27].

Day in day out, number of attackers is increasing, and the technologies and the targets of attacks are diversified [18]. These among other insecurity issues has led to various researches and development of IDS with the use of different technologies that include data mining, multi agent, Honey pot, multiclass, mobile agent etc.

Up till today, previous research work reveals that, the technology of mobile agent can still be enhanced to reduce the dynamism and mutative rapid development of hacker technology and that the benefit of using mobile agents in detecting intrusion cannot be denied, however securing the agent itself still poses a great challenge in the information security domain [28]. Therefore, mobile agent effectiveness in IDS depends on some factors relating to the agent itself [15].

According to [15], mobile agent portability, and security affect agent system's usability and efficiency in intrusion detection. Hence, attempt to improve on the security of mobile agent result to increase in network load on the part of the agent system. [14] also asserted that the main obstacle hindering the application of mobile agent to IDS is insecurity on the part of the agent. This reveals that if mobile agent is highly secured, the performance of IDS will be improved. The question here is that if such performance is improved through the enhancement of mobile agent security, would there be any significant effect on the network traffic and network load?.

[28] also enlisted some shortcoming of mobile agent in the area of insecurity that has affected the usability and performance of IDS.

In a recent study of mobile agent security threats, it was stated that lots of security issues of mobile agent needs to be addressed and such issues include inter mobile agent collaboration, and mutual authentication between host and mobile agents [1].

[25] also claimed that agents' security, management, coordination, and collaboration are important problems for effective identification of distributed attack in a system. The fact here is that when agents are highly secured and well collaborated, better detection of attack by the agent's system can be achieved. In such scenario, how can secured agents be achieved to mutually address intrusions with little or no effect on system usability and efficiency ?

What enhancement can be done on agents such that there will be little or no effect on processor's load , processing time and network traffic ?

3. METHODOLOGY

As a result of the need to make effective usage of mobile agents and to take advantage of their inevitable characteristics for intrusion detection, this research is aimed at proposing an enhanced intrusion detection model with the use of more secured and collaborative mobile agents. Since mobile agent is central to the proposed model for intrusion detection then the idea is to improve their safety, collaborative ability and reduce their response time such that the agent system usability and efficiency can be improved.

To this end, this research work proposed an improvement on the framework of [11] where mobile agents were used to detect user anomalities (i.e model of normal behaviour) in two level: user activities and program operations. The model uses two approaches which include misuse detection approach (model of abnormal behaviour base on experience) and anomaly approach, this hybridized approaches is proposed to enhance effectiveness of the detection. It will also give room for Network Administrator to make a decision on the suspected intrusion so as to avoid False Positive Alarm to some extent. It gives room for mobile agents to collaborate by triggering and communicating on any detected intrusion then store the characteristics of such intrusion attempt, this also enhance fast detection when such attempt is made again.

3.1 Modified Hybrid Framework

The architecture of this proposed model consists of two comparators being handled by mobile agent as shown below:

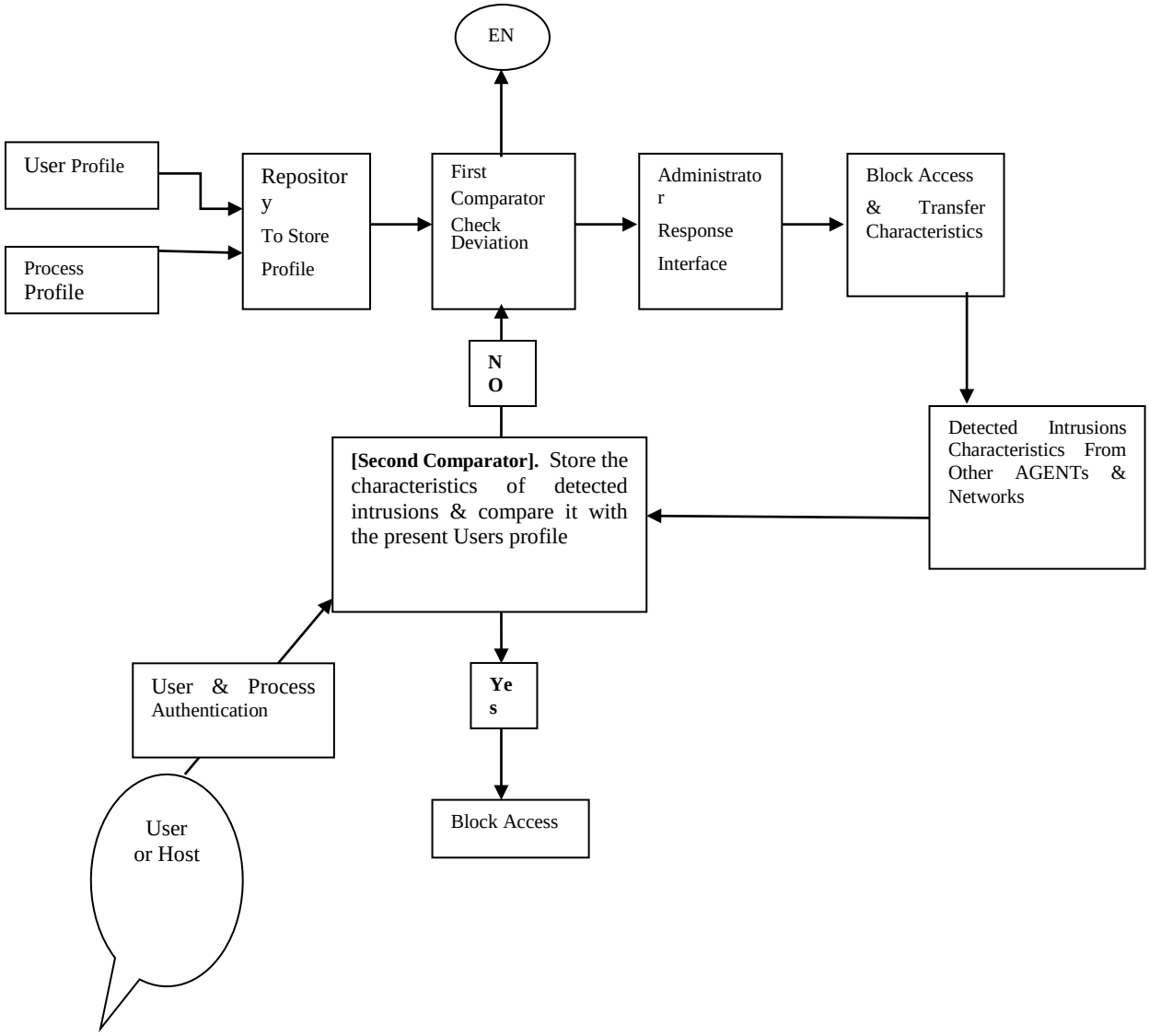


Figure 2. Propose Framework for the Hybridized Architecture

Mobile agent will perform the function of comparing profile in the first and second comparators. It will gather information and data relating to user and process profile of its domain from repository, this task is performed on timely basis or based on an event occurrence.

Each agent will have an access to relay the characteristics of detected intrusion within its domain to other agents outside its domain and within some other network for future detection (collaboration). Such characteristics may include recorded user activities, start time, speed of input, system resource used, energy consumption, and some other expected deviance behavior of user and process detail for comparism purpose. Here, matching algorithm can be used by agent.

3.2 Mobile Agent Security Enhancement

Since security is also a key factor in ensuring the efficiency, ease of use and wide spread deployment of intrusion detection application base on mobile agent technology. Without proper solution to security problem of mobile agent, there will be severe impediment on IDS. Therefore, the following principles of mobile agent need to be applied to guarantee safety of the agents [11]:

1. Participants cannot be assumed to trust each other by default.
2. Any agent-critical decisions should be made on trusted hosts.
3. Unchanging components of the state should be sealed cryptographically.

Therefore, this research design has proposed to look at security issues of mobile agents from four different perspectives of threat as follows

Agent to platform threat.

Platform to agent threat.

Agent to agent threat.

Platform to platform threat **[1]**

Some of those threats that can cause insecurity include Alteration, Eavesdropping, Repudiation, Denial of service, Unauthorized Access, Masquerading etc.

i. Masquerading is away of impersonating legitimate user, it gives room for extraction of sensitive information by the fake agent.
ii. Unauthorized access exist by way of illegal interference with a platform or when agents invoke the public method of another agent.
iii. Denial of service as to do with exhausting resources so that others can be deprived of it.
iv. Repudiation attack refers to threat that involve preventing agent from participating in communication or transaction.
v. Alteration is a threat that has to do with undetected change of code or data of an agent.
vi. Eavesdropping is a passive attack that involves the interception and monitoring of secret communication.

It may be concluded by close assessment and analysis of some of the above listed threats, that agents may be safe to certain level if

i. Their privacy and integrity is assured.
ii. Agent to platform or server authentication is ensured.
iii. Authorization and access control is highly observed [11].

In a null shell, to provide security for mobile agents in this model against all or some of the above mentioned threats, this research work proposed to employ some of the following techniques:

i. During collaboration between agent from other domain for exchange of intrusion characteristics, agent and platform will be design to authenticate themselves (i.e verification of each other identity). Implementation of this is proposed to use digital signature and password protection strategies.
ii. To enhance high level of agent data and behavioural privacy, encryption and cloning is proposed.
iii. Agent communication and security related transactions is proposed to be recorded so that auditing and tracing of non participating agent can be fish out.
iv. Platform will be structured in such away that it can control concurrent and simultaneous access to data and services. It must also be a good manager of dead lock.
v. A platform or agent will also be design to signal the administrator in case any agent belonging to a domain has been changed or not, by monitoring a code that has been tempered, or whose state has been changed or whose execution flow has been redirected.
vi. Some other proposed mobile agent security mechanism for this model includes hash function, range checker, execution tracing and cryptography that allows detection of attack against code manipulation.

3.3 Placement and Distribution Enhancement

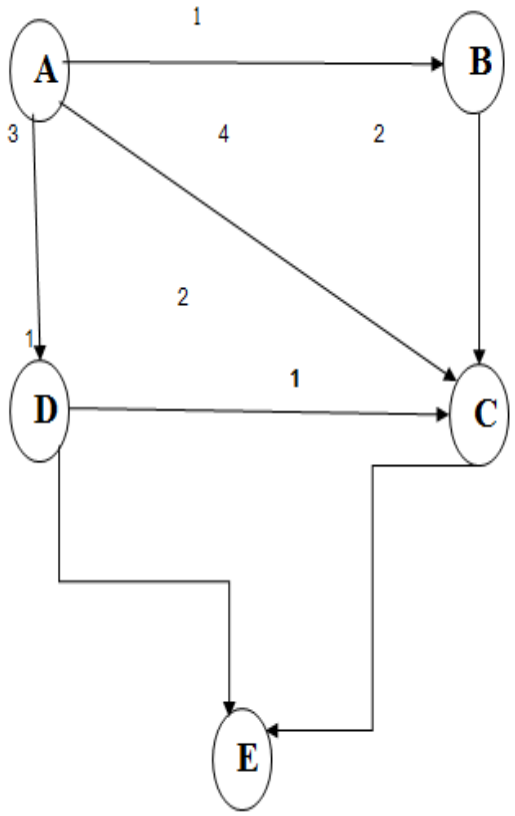
It is not an overemphasis, to say that too much of mobile agents in many intrusion detection application have an effect on data transmission, network traffic congestion and on computational and processing time of the central processor. Hence, to improve the performance of the proposed design as regard to fastness and network traffic, we propose the use of Dijkstra Algorithm as follows:

In line with Dijkstra algorithm, G is propose to be a graph which will represent the network of nodes in a domain and is going to have two sets associated with it.
The first set is N which represents all nodes in the domain.
The second set is C which represents all connections between nodes in the domain.
For each c ϵ C, we have d(c) $\geq$ 0, which represents the delay of edge c.
The symbol σ will be used to represent the delay of the shortest path from one node to another node within the domain.
Having defined these symbols we can formally define our mobile agent placement method as follows:

Given G = (N, C) where each c ϵ C, d(c) > 0 , select a node v ϵ V, such that the maximum σ from node v to all other nodes in the domain, will be the minimum. This will be the location for an agent to be placed. (i.e minmum of the maximum delay)
Alternatively we can say that the node with min{max {σ(v, vi v□) for i v□ϵ V}for j ϵ V } will be the location for an agent to be place within the domain.

Hence for practical purpose, we shall examine the delay from a node to all other nodes within a domain and pick the maximum delay for all the available nodes and store it in an array call MAXARRAY. Then from MAXARRAY we shall pick the node with the smallest and place our Mobile Agent there.

The diagram and table below shows an instance of this:



As an instance, the domain in the above diagram has five nodes and the weight of the delay from node to node is has shown above. Therefore, N = 5 and for the connection between **node a** to **node e**
We have the following alternative connections together with their respective delay,

p1=< a, b, c, e > and it"s weighted delay
= w(a, b) + w(b, c) + w(c, e)
= 1 + 2 + 1 = 4

also

p2=< a, d, c, e > and it"s weighted delay =
w(a, d) + w(d, c) + w(c, e) = 3 + 2 + 1 = 6.

Table 1: shows the list of shortest delay from node to node for the above sample network.

NODE	a	b	C	d	e
A	0	1	3	3	**4**
B	1	0	2	**4**	3
C	**3**	2	0	2	1
D	3	**4**	2	0	1
E	**4**	3	1	1	0

Table 2: MAXARRAY shows the maximum delay from each node to other nodes as follows.

NODE	MAXIMUM DELAY
A	**4**
B	**4**
C	**3**
D	**4**
E	**4**

Hence from MAXARRAY, NODE C is the appropriate node to place the mobile agent such that the IDS can be more efficient by virtue of less workload. This is to say that Node C alone may be assigned an agent rather than assigning agents to every nodes within the domain.

We can also have a SORTED MAXARRAY as shown in Table 3 below

Table 3: SORTED MAXARRAY

NODE	MAXIMUM DELAY
C	**3**
A	**4**
B	**4**
D	**4**
E	**4**

Atimes increasing the number of agents in the network will allow intrusions, anomalies and other security issues to be detected faster as well as spread the workload out across the network.

Suppose we have a very large network consisting of network of networks, in which case there is a need to use more than a single agent in the agent system (i.e the proposed intrusion detection system) for effective intrusion detection.
Therefore in such scenario, we propose the following strategies inline with the above MAXARRAY list for selection and assignment of mobile agent to various domain within a large network. As an instance, suppose the outcome of our SORTED MAXARRAY is as follows:

Table 4: SORTED MAXARRAY

NODE	MAXIMUM DELAY
C	**3**
A	**4**
B	**5**
D	**5**
E	**5**

Here it imply that if we wish to assign two agents, they are preferably better placed in Node **c** and Node **a.** If we pick all the weighted delays of Node **a** and Node **c** to all other nodes within the network from Table 1, we can come out with the following two dimensional array:

Table 5: Multiple Agents Assignment Table [MAAT]

NODE	a	b	C	d	e
A	0	1	3	3	**4**
C	**3**	2	0	2	1

Consequently, Table 5 clearly indicates that if we are to assign two agents, they should be place in Node **a** and Node **c**. Apart from that , mobile agent in Node **a** should be responsible for node **a** and node **b** while mobile agent in Node **c** should be responsible for Node **c,** Node **d,** and Node **e.** Hence this kind of assignment strategy is proposed for this research design so as to use minimum mobile agents that can respond to every other nodes efficiently in case of any intrusion to our network.

3.4.1 Algorithm for Placement and Distribution of Mobile Agent.

Single mobile agent placement algorithm for small network

i) Input all the available nodes delay
ii) Apply Dijkstra Algorithm to get all shortest distance from node to node
iii) For each node, select the highest delay out of all the available shortest delay from a node to all other nodes.
iv) Tabulate all the highest delay with their corresponding node.
v) Sort the table in ascending order
vi) Output the node with the smallest delay in the table

3.4.2 Multiple Mobile Agent Placement Algorithm for Large Network.

i. Input the max(min(delay)) for each node.
ii. Arrange and tabulate them in ascending order.
iii Select the number of node you need in line with tabulated order. Ziv Create your multiple agent assignment table
v Determine and pick which of the nodes has a minimum delay to the selected node
vi Output the selected node with those node for which they have minimum delay.

3.5 Experimental Data:

This research work proposed to use randomly generated data to evaluate the efficiency of the research model through a series of experimental simulation. The randomly generated data shall be used to evaluate the resources required to operate the IDS model on a computer in term of memory usage, network traffic, network load and processing load.

4. CONCLUSION

This paper has presented a proposed research framework which is aimed at faster detection of attack, reduction of network congestion and bottle neck in packet processing. After implementation, it stand to be robust by it's ability to receive characteristics of known attack from other network user and it's hybridized usage of user activity, and program operation monitoring for intrusion detection.

5. REFERENCES

[1] Amro, B. (2013). Mobile Agent Systems, Recent Security Threats and Counter Measures. Journal of ResearchGate. Pages 160-167.

[2] Ande, A. T. (2013) (ed), History and Philosophy of Science in General Studies, General Studies Division, University of Ilorin, ISBN: 978-36284-0-2

[3] Bernardes and Moreira (2000), Implementation of an Intrusion Detection System Based on Mobile Agent. international symposium on software engineering for parallel and distributed systems *IEEE Computer Society*,

[4] Chapke, P. P., and Raut, A. B. (2012). Intrusion Detection System using Fuzzy logic and Data Mining Technique. *International Journal of Advanced Research in Computer Science and Software Engineering* , Pages 152-154.

[5] Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide.* USA: Special Publication 800-61 Revision 2.

[6] Corporate White Paper. "Deploying and Tunning Network Intrusion Detection System." intrusion .com White Paper 2001 (2004): 3

[7] Ehimen, O. R., & Oyakhilome, I. (2009). Development of a Software Based Firewall System for Computer Network. *Leonardo Electronic Journal of Practices and Technologies* , 75-80.

[8] Ganapathy, S., Yogesh, P., & Kannan, A. (2012). Intelligent Agent-Based Intrusion Detection System Using. *Computational Intelligence and Neuroscience* .

[9] Holtz, M. D., David, B. M., & Timoteo, R. (2011). Building Scalable Distributed Intrusion Detection System Based on the MapReduced Framework . *REVISTA TELECOMUNICACOES* , 22-31.

[10] Jabez, J., & Muthukumarb, B. (2015). Intrusion Detection System (IDS): Anomaly Detection using Outlier. *International Conference on Intelligent Computing, Communication & Convergence* (pp. 338 – 346). India: Procedia Computer Science Press.

[11] Jaisankar, N., Saravanan, R., & Swamy, K. D. (July 2009). Intelligent Intrusion Detection System Framework Using Mobile. *International Journal of Network Security & Its Applications (IJNSA)* , Vol 1, No 2., 72-88.

[12] Jansen, W. A. (2003). *Intrusion Detection With Mobile Agents.* USA: NIST Special Publication 800-.

[13] Jansen, W., & Karygiannis, T. (october, 2000). Privilege Management of Mobile Agents. *Twenty-third National Information Systems Security Conference* (pp. pp.362-370). USA: NIST Special publication.

[14] Jansen, W., Mell, P., Karygiannis, T., & Marks, D. (1999). Applying Mobile Agents to Intrusion Detection and Response. *National Institute of Standards* , 1-46.

[15] Jianxiao, L., & Lijuan, L. (2009). Research of Distributed Intrusion Detection System Model Based. *International Forum on Information Technology and Applications* , 53-57.

[16] Jimoh, R. G. (2013). Knowledge Management Functionality by Information Technology in Adeleke, B. L., Abdus-Salam, N. &

[17] Kabiri, P., & Ghorbani, A. A. (2005). Research on Intrusion Detection and Response:. *International Journal of Network Security*, , 84-102.

[18] Lee, D.-h., Kim, D.-y., & Jung, J.-i. (2008). Multi-Stage Intrusion Detection System Using Hidden Markov Model Algorithm. *International Conference on Information Science and Security* , 72-77.

[19] Lee, W., & Stolfo, S. (2001). Real time data mining-based intrusion detection. *Proceedings of DARPA Information* , pp. 89 -100.

[20] Minar, N., Kramer, K. H., & Maes, P. (n.d.). *www.media.mit.edu/~nelson/research/routes/*. Retrieved 11 03, 2014, from www.media.mit.edu/~nelson/research/routes/: http://www.media.mit.edu/~nelson/research/routes/

[21] Mohammed, H. A. (2015). HYBRID INTELLIGENT APPROACH FOR NETWORK. MALAYSIA.

[22] *ntrusion-detection-system-group.co.uk*. (n.d.). Retrieved march 15, 2015, from intrusion-detection-system-group: http://www.intrusion-detection-system-group.co.uk

[23] Pages 158-164.

[24] Pathak, H. (2011). Hybrid Security Architecture (HSA) for Secure Execution. *International Journal of Information Technology* , 499-502.

[25] Ran, Z. (2012). A Model of Collaborative Intrusion Detection System based on Multi-agents. *International*

Conference on Computer Science and Service System , 789-792.

[26] Scarfone, K., & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems. *National Institute of Standard and Technology* .

[27] Tian, -r. L., & Pan, W.-m. (2005). Intrusion Detection System Based on New Association Rule Mining Model. 512-515.

[28] Trushna, T., Patil1, K., & Banchhor, C. (2013). Distributed Intrusion Detection System using. *International Journal of Advanced Research in Computer and Communication Engineering* , 1901-1903.

[29] Verwoerd, T., & Hunt, R. (2003). Intrusion Detection Techniques and Approaches.

[30] Whitman, Michael E., Townsend, Anthony M., and Hendrickson, Anthony R. "Cross-National Differences in Computer-Use Ethics: A Nine Country Study." The Journal of International Business Studies 30, no. 4 (1999): 673–687.

[31] Yanxin W.(2004). *An hybrid intrusion detection system* (Unpublished dissertation). Iowa State University, Ames. Retrieved from UMI Microform 3145689

[32] Zirra, P. B., & Wajiga, G. M. (2011). Cryptographic algorithms for Secure data Communication. *International Journal of computer science and Security* , 227-243.