DEVELOPING A NETWORK COMPUTING MODEL FOR THREATS INFORMATION SHARING

Agborie Bishop Aguonorobo e-mail: bbagborie01@yahoo.com
NwaforAnthony C. e-mail: anthonynwafor981@gmail.com
Mgbeafulike J. Ike e-mail: ike.mgbeafulike@gmail.com

Department of Computer Science, Chukwu-Emeka Odumegwu Ojukwu University, Uli, Anambra State, Nigeria. Email: bbagborie@gmail.com

ABSTRACT
This research study is an improvement on network communication and computing for adequate sharing of information with an innovation on its threats detection accuracy by its ability to share threats information among LANs connected to the network. The inability to detect threats in network traffics and not sharing the information of threats or malicious attacks with other local area networks (LANs) connected has brought about insecurity of data and information, for which its integrity, availability and confidentiality would not be guaranteed. The threat information sharing module was modeled using Remote Method Invocation (RMI) and Mobile Agent (MA) techniques. The implementation would be carried out using C# object oriented programming language. The simulation result for training and test with the threat packets shows that mobile agent (MA) is more suitable for information sharing. The threats information sharing module was evaluated based on the metrics of "Response time to threats detection, Bandwidth usage and Fault tolerance". The intelligent model developed has the capability of improved threat detection and information sharing with higher accuracy and capability to gather information for timely investigation and information dissemination based on the true positive, true negative, false positive and false negative rates, and also the threats reporting agents (TRA), threats information sharing agents (TISA), and the Advisory recommendation agents (ARA). This model would definitely improve network security and monitoring of distributed LANs because of its capability to share threats information, disseminate advisory to all LANs connected to the network security server.

Keywords: Networks, Traffics, Communications, Mobile Agents, RMI, Evaluation metrics

1. INTRODUCTION

A computer network is an aggregate of two or more autonomous computers that are separated by physical distance but are connected together. It is any set of interlinking lines resembling a net, a network of roads, an interconnected system, a network of alliances (Tanenbaum, 2006) for the purpose of sharing data and information.

The challenges of information sharing, refusal or inability of network users to share or report cyber incidents and breaches on their networks to the public for awareness is a serious problem, which cyber criminals leverage upon to gain more grounds and succeed in their

operations, thereby causing economic havoc and sometimes putting the security of the nation at risk, by causing a great damage and a huge loss.

The component or devices that enable computers to send data with ease is known as the network packets. Network packet contain a pre-defined amount of data with additional headers that indicate how the data will be handled. Simple information will require few packets while large files will require a large number of packets. The packets flowing through a computer network are referred to as the network traffic. The functionality for handling packets in a computer network is provided by a set of protocols known as TCP/IP. A protocol is a set of rules and convention between the communicating participants (Forouzen and Fegan, 2003).

1.1 Statement of the problem

The challenges of not sharing information among networks, made it difficult to report cyber incidents, network breaches, crimes, attacks, etc. for the public to be aware of such dangers and finding a way to mitigate such problem. Hence, criminals take advantage of this and gain more grounds in their operations, thereby putting the integrity and confidentiality of data information to doubt.

1.2 Objective of the study

The aim and objective of this paper is to develop a system that has the capability of inter-linking and sharing information among networks so as to prevent any form of network breaches.

1.3 Significance of the study

Effective cyber security threat monitoring is crucial to economic survivability and security of a nation (Ayofe and Irwin, 2010; Wamala, 2011) hence it is necessary to solve the problem of cyber threats or attacks on network packets by analyzing any suspected threats information and sharing such information among networks connected so as to find a way of curbing or reducing the havoc it might cause.

1.4 Scope of the study

This study is to develop a system that would combat the current cyber space threats in network packets by its ability to constantly monitor the network traffic for the occurrence of novel threats in network packets, report the threats for investigation, share the new threats information on real time basis and disseminate solutions on the new threats to all the networks connected in the cyberspace. The aims of sharing threats information across many networks (LANS, WAN) is to create awareness and to take appropriate security measures when attacks occurs in one or more network.

The information sharing model was modelled using two approaches (Remote Method Invocation – RMI and Mobile Agent (MA). The performance evaluation of the threats information sharing model approaches was carried out using Metrics like “Response time to threats detection, Bandwidth usages and Fault tolerance”. The prototype implementation of the smart model was carried out using an appropriate object oriented programming language.

1. Literature review

A distributed system involves the coordination of two or more computers, geographically apart and connected by a physical network. The distributed system is constructed from a set of relatively; independent components such as Threats database files, LANS, centralized cyber security server that form a unified, but geographically and functionally in diverse entities.

Network computing and communication: An overview and comparism of three programming paradigms for distributed computing are; client-server, code-on-demand, and mobile agents as highlighted (Lange and Oshima, 1998).

(i). Client-server paradigm: - In the client-server paradigm, the server advertises a set of services that provides access to some resources (e.g. Databases). The code that implements these services is hosted locally by the server. In this regards, the server holds the know-how. Finally, it is the server itself that execute the services, and thus has the processor capability. If the client is interested in accessing some resources hosted by the server, it will simply use one or more of the services provided by the server. Client-Server computing could be through the "Remote Procedural Call (RPC)" or "Remote Method Innovation (RMI)" models.

(ii). Code-on-demand Paradigm: - In the code-on-demand paradigm, one would first get the know-how when one needs it. Let's assume that "Host A" could not execute its task at the initial stage due to the fact that it lacks the code (Know-How), and fortunately, another "Host B" in the network provides the needed code. Once the code is received by A, the computation is carried out in A. Host A holds the processor capability as well as the local resources, unlike the client-server paradigms, 'A' does not need knowledge about the remote host, since all the necessary code will be downloaded. We say that one Host 'A' has the resources and the processor while another Host 'B' has the know-how.

iii). Mobile Agent paradigm (MA): - The mobile agent paradigm has the characteristics of allowing any host in the network to possess any mixture of know-how, resources and processors. Its processing capabilities can be combined with local resources. Know-how (in the form of mobile agents) is not tied to a single host but is available throughout the network. If one compares these three paradigms, the chronological trend towards greater flexibility will be noticed. The client and the server have merged and become a host. The applet and servlet, while serving as client and server extenders respectively, have been combined and improved with the emergence of mobile agents.

2.1 Principles of mobile agent (MA): An agent is an independent software program that runs on behalf of a network user (Lange and Oshima, 1998). It can be characterized as having more or less intelligent and it has the ability to learn. Mobile agents add to regular agents the capabilities of travelling to multiple locations in the network by saving their state and restoring it in the new host. As they travel they work on behalf of the user, such as collecting

information or delivering requests. This mobility greatly enhances the network and creates a powerful; computing environment.

Mandatory Properties of an agent:

(a). Reactive: Senses changes in the environment and acts accordingly to these changes
(b). Autonomous: Has control over its own actions
(c). Goal driven: It is proactive.
(d). Temporal continuous: It is continuously executing.

Orthogonal Properties of an agent:

(a). Communicative; - Able to communicate with other agents.
(b) Mobile; - Can travel from one host to another
(c). Learning; - Adapt to accordance with previous experience
(d) Believable; - Appears believable to the end –user

Advantages of Mobile Agents: According to (oshima ,1998; Wooldridge, 2002) mobile agent has some advantages to the usual programming models, which are as follows;

(a) They Reduce the Network Load; - Distributed systems often rely on communications protocols that involve multiple interactions to accomplish a given task. This is especially true when security measures are enabled as a result of network traffic. Mobile agents allow you to package a conversation and dispatch it to a destination host where the interactions can take place locally.

(b) **It Overcomes Network Latency:** Critical real-time system such as robots in manufacturing processes need to respond to changes in their environments in real time. Controlling such systems through a factory network of a substantial size involves significant latencies. For critical real-time systems such as latencies are not acceptable. Mobile agents offer a solution since they can be dispatched from a central controller to act locally and directly execute the controller's direction.

(c) **They Encapsulates Protocols:** When data are exchanged in a distributed system, each host owns the code that implements the protocols needs to properly code outgoing data and interpret incoming data respectively.

(d). The Execute Asynchronously and Autonomously: - Often, mobile devices have to rely on expensive or fragile network connections, that is task that require a continuously open connection between a mobile device and a fixed network will most likely not to be economically or technically feasible. Task can be embedded into mobile agents, which can then be dispatched into the network dispatched. The mobile agents become independent of the creating process and can operate asynchronously and autonomously.

e). **They Adapt Dynamically: -** Mobile agents have the ability to sense their execution environment and react autonomously to changes. Multiple mobile agents, posseses the unique ability to distribute themselves among the host, in the network in such a way as to maintain the optimal configuration for solving a particular problem.

f). **They Are Naturally Heterogeneous: -** Network computing is fundamentally heterogeneous, often from both hardware and software perspective, as mobile agents are generally computer and transport layer independent and dependent only on their execution environment, they provide optimal conditions for seamless systems integration.

g). **They Are Robust and Fault Tolerant: -** The ability of mobile agents to react dynamically to unfavorable situations and events make it easier to build robust and fault tolerant distributed systems. If a host is being shut down, all agents executing on that machine will be warned and given time to dispatch and continue their operation on another host in the network.

3. PROPOSED SYSTEM AND IMPLEMENTATION

The cyber security manager runs on the security server and has the capability of listening to platform interactions and communications in the network platform. This developed intelligent model for detecting malicious threats in network packets, will provide the necessary platform for all threats detectors ie. Distributed LANs and security manager Server are in communications. The first step in using the software is for all the distributed LANs in the different locations to connect with the cyber security server, and after this the main operations of the system starts from the threat detection module (IDS) installed on the distributed LANs. The IDS components of the threat detector will constantly analyze the network traffics in its domain with a view to detecting any malicious and strange packets.

Once a malicious packet is detected, the IDS will quickly run its module by carrying out different levels of detection and classification on the suspected packets. If the packets classification is unknown, the checkmator or the decision module will route the packet to the cyber security manager installed on the server for further investigation, logging, threat information sharing and dissemination of advisories on the novel threat packets to other distributed LANs in the cyberspace network.

The server will perform threats investigation by comparing the pattern of the suspected packets with the stored threats patterns in the central threats database. The results of the investigation and analysis by the cyber security server will trigger the action of sending it to all the LANs connected to the server for awareness. The second action that will occur simultaneously with the first is the recommendation of solutions and advisories to all the distributed LANs administrators in the cyberspace for quick and emergency action to safeguard their networks

The program that will run the modules as specified and enhance the performance of the model are; a. The threat detection accuracy for base classifiers and ensemble classifiers.

b. Response time to threat detection as against the number of LANs connected that is generating novel threats alerts in a particular time for RMI and MA based architecture.
b. Bandwidth usage or consumed by the model in both RMI and MA based architecture.
d. Fault tolerance of the model in RMI and MA based architecture

This model deals with how communication takes place among the different components of the Network system. This model describes how the distributed LANs exchange threats information with the security server. This model was modelled with RMI and Mobile Agent based approaches and it was observed that mobile agents (MA) is more suitable because of its capabilities and efficiency. In this model, when any LAN detects a novel threat, the mobile agent residing in the LAN will be triggered and the MA will immediately obtain the novel threat information from the IDS residing in the LAN. The MA will migrate to the security server to report and log the newly detected novel threat information. Immediately the LAN mobile agent reports, the MA agent in the server will also be triggered to disseminate the reported threat information to other LAN in the Network.

4. IMPLEMENTATION AND RESULTS

It is expected that all the distributed LANs would have the threat detector installed in them with mobile agent (MA) capability for network communication and threat reporting agent (TRA). The cyber security manager software and mobile agent should also be installed on the server to enable client-server communications and service delivery. The two agents that will assist the server are the "Threat information sharing agent" (TISA) and the "Advisory recommendation agent" (ARA).

TRA = Threat reporting agent, sends threats information to security manager or server.
TISA = Threat information sharing agent sends message to all distributed LANs
ARA = Advisory recommendation agent sends message to all distributed LANs

Performance metrics for threats information sharing model: The network communication performance metrics chosen to evaluate the performance of the threats information sharing of the intelligent model are: "Response time, Bandwidth consumption and Fault tolerance".

a. Response time for RMI and MA is measured by;

D_t = Threat detection time of the attacked network.
S_{pt} = Server processing time.

DES_{RMI} = The time used by server to inform other networks of newly detected threats
Ns = [NI, N2, N3……Ns) no of networks in the cyberspace.
R_{RMI}= the time interval between when networks detect new threats, report the threats to the central server and the central server disseminate the threats information to other networks (LANs) using the proposed platform.
N_k= Number of network that detect new attack.

Therefore, for RMI;

$$R_{RMI} = N_k * (D_t + rrt) + S_{pt} + DES_{RMI} \quad (1)$$

Where DES_{RMI} = RMI dissemination time,

Rrt = Round trip latency,

$$DES_{RMI} = \sum_{i=1}^{N_k} \sum_{i=1}^{N_k} (rrt)_i \quad (2)$$

Put equation (2) into (1)

$$R_{RMI} = N_k * (D_t + rrt) + S_{pt} + \sum_{i=1}^{N_k} \sum_{i=1}^{N_k} (rrt)_i \quad (3)$$

Mobile Agents;

Let $R_{agent} = N_k * (D_t + rrt) + S_{pt} + DES_{agent}$ (4)

$S_{pt}$is same as in RMI model

R_{agent}= MA response time

Where DES_{agent} = MA dissemination time

$$DES_{agent} = \sum_{i=1}^{N_k} (rrt)_i \quad (5)$$

Putting equation (5) into (4)

$$R_{Agent} = N_k * (D_t + rrt) + S_{pt} + \sum_{i=1}^{N_k} (rrt)_i \quad (6)$$

b. Bandwidth usage for RMI and MA is measured by;

RMI Model: Let the message size from the client be denoted by y and the size of the acknowledgment from the server be z in bytes, for a single LAN, the total bandwidth usage in the bytes is given by

$$\beta_{RMI} = B_{client} + B_{server} \quad (7)$$

Where,

β_{RMI} = bandwidth consumption of RMI approach

β_{Client} = bandwidth used by the client (distributed LAN) to report threat to central server

β_{Server} = bandwidth used by the cybersecurity to inform other client networks (distributed LANs).

Let message size from client network be Y and acknowledgment from server be Z

$\beta_{Client} = (Y + Z)$

if N_k client networks detect threat (8)

$\beta_{Client} = (Y + Z) \times N_k$ (9)

assume that Y= Z

Assume that the message size Y (bytes) is the same with acknowledgment Z (bytes) from the server i.e Y=Z and it should be noted that a number of links must be established between the two communicating nodes before computation is completed then,

$\beta_{Client} = 2^* Yx\ N_k$ (10)

From server side that is B_{server}

Since the client networks will report to server whenever threats are detected, the server will in turn inform other networks and also consume bandwidth

$$\beta_{Server} = \sum_{i=1}^{N_k} \sum_{i=1}^{N_k} (Y+Z)_i \quad (11)$$

Since the client networks will report to server whenever threats are detected, the server will in turn inform other networks and also consume bandwidth.

$$\beta_{RMI} = 2^* Yx\ N_k + \sum_{i=1}^{N_k} \sum_{i=1}^{N_k} (2^* Y)_i \quad (12)$$

MA Model: In mobile agent (MA) scenario, the agent arises from the threat detecting LAN and migrates to the network security server.

$\beta_{Server=}B_{cag} + B_{sag}$ (13)

Bcag = Bandwidth used by client agent

Bsag = Bandwidth used by server agent

Bcag = (Xag + Y) +Xag (14)

Where

Xag = Agent code size

Y = packet size

If N_k = network detect threats

Bcag = (Xag + Y) + Xag) * N_k (15)

equation (3.35) can be rewritten as

Bcag = (2* Xag =Y) * N_k (16)

$$B_{Sag} = \sum_{i=1}^{N_k} (2^*Xag+Y)_i \quad (17)$$

Therefore, the total bandwidth for agent model

Putting (16) and (17) into (13)

$$\beta_{Agent} = (2^* Xag + Y)\ N_k + \sum_{i=1}^{N_k} (2^*Xag+Y)_i \quad (18)$$

c. Fault tolerance: Fault is a measure of robustness or adaptability of a system to breakdown

RMI Model: In the face of fault or network failure in RMI model, the model will not be able to scale. That is to say that the system will experience delay equal to the node

recovery time nRt. This will be added to the normal response time of the system when there is no failure. When failure of the node occurs, fault tolerance can be modeled as follows;

$$R_{RMI} = N_k * (D_t + rrt) + S_{pt} + \sum_{i=1}^{N_k} \sum_{i=1} (rrt)_t + nRt \qquad (19)$$

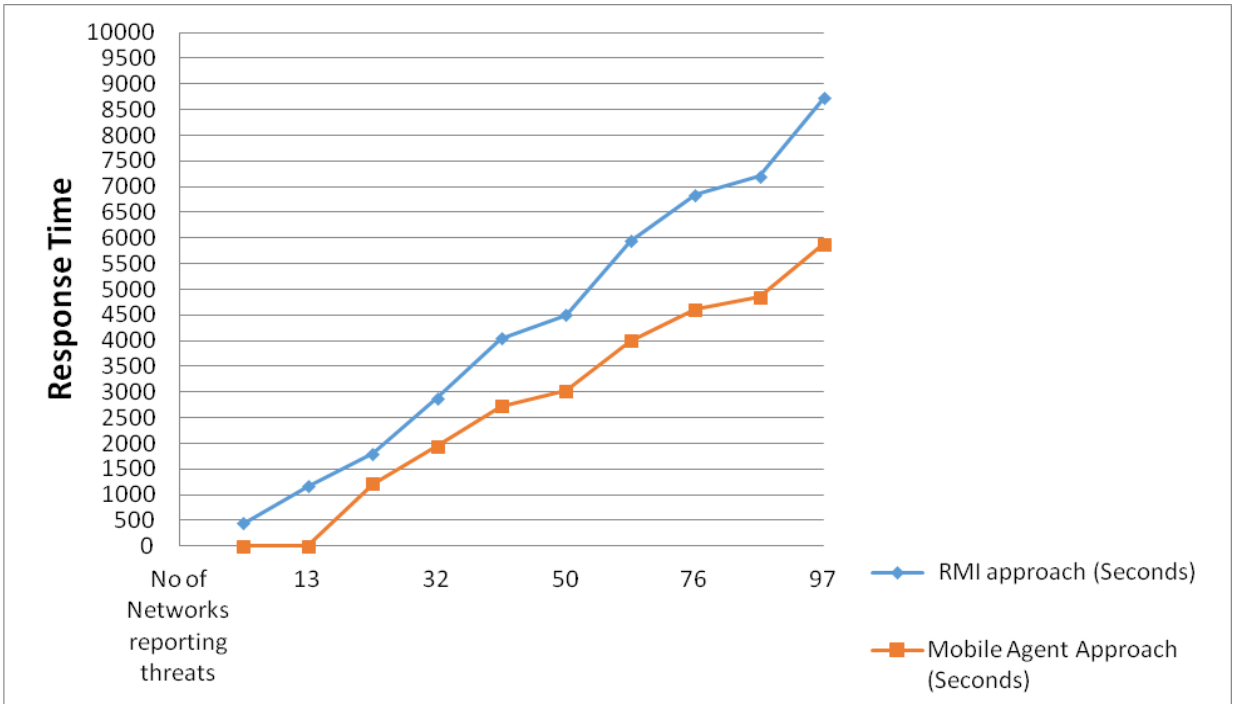
MA Model: In the face of failure or faulty links, the mobile agent can proactively determine alternative route in order to connect to the next node so that the destination could be reached and the total response time remain unchanged.

$$R_{Agent} = N_k * (D_t + rrt) + S_{pt} + \sum_{i=1}^{N_k} (rrt)_i \qquad (20)$$

Results:

The model response Time using RMI and Mobile Agent techniques

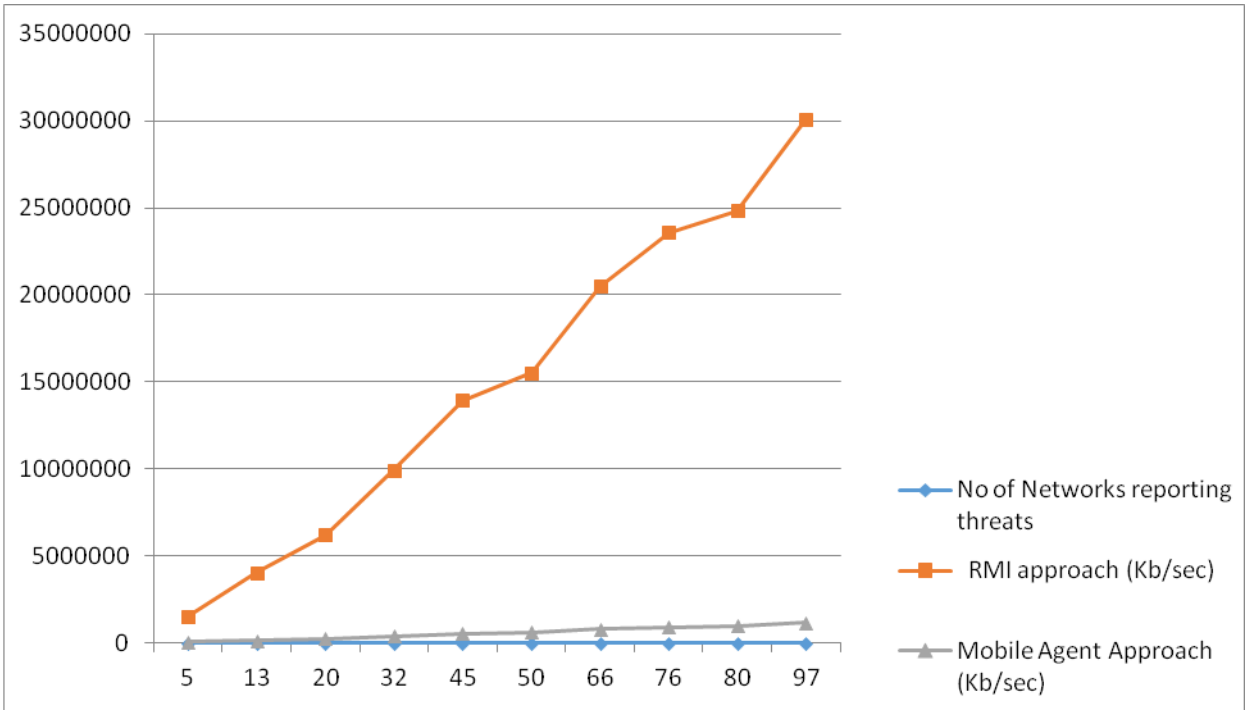
No of Networks reporting threats	RMI Approach (Seconds)	Mobile Agent Approach (Seconds)
5	450.01	303,01
13	1170.02	787,82
20	1800.03	1212.03
32	2880.05	1939.25
45	4050.06	2727.06
50	4500.07	3030.07
66	5940.09	3999.69
76	6840.11	4605.71
80	7200.11	4848.11
97	8730.14	5878.34



Response time for RMI and Mobile Agent

The model bandwidth consumption using RMI and Mobile Agent approaches

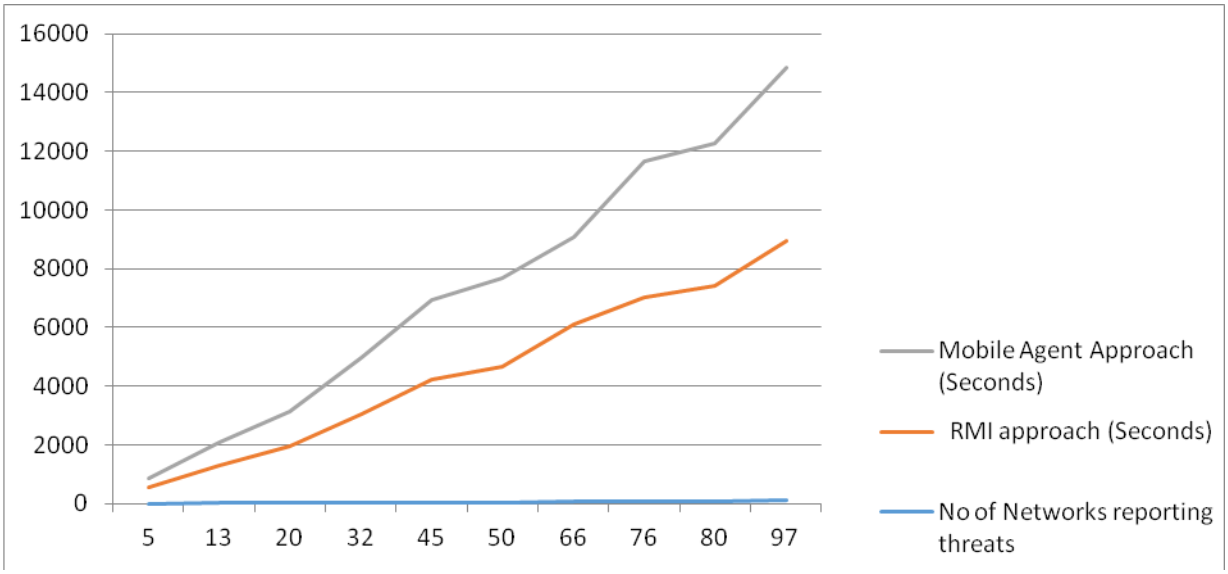
No of Networks reporting threats	RMI approach (Kb/sec)	Mobile Agent Approach (Kb/sec)
5	1551360	61440
13	4033544	159744
20	6205440	245760
32	9928700	393216
45	13962200	552960
50	15513600	614400
66	20478000	811008
76	23580700	933888
80	24821800	983040
97	30096400	1191940



Bandwidth Consumption by RMI and MA approaches

The model fault tolerance for RMI and MA approaches

No of Networks reporting threats	RMI approach (Seconds)	Mobile Agent Approach (Seconds)
5	570.01	303.01
13	1290.02	787.81
20	1920.03	1212.03
32	3000.05	1939.25
45	4170.06	2727.06
50	4620.07	3030.07
66	6060.09	2969.47
76	6960.11	4605.71
80	7320.11	4848.11
97	8850.14	5878.34



Fault tolerance of the model using RMI and MA approaches

5. SUMMARY AND CONCLUSION

The challenge of effectively managing complexity and sophistication of emerging network threats motivated this paper. The paper therefore presented a proactive approach to secure the confidentiality, availability and integrity of network information data by its accurate and timely detection of novel threats for quick investigation, information sharing, and prevention. This would be achieved through appropriate methodology of mobile agents as applied.

5.1 RECOMMENDATIONS:

i. Individuals and organizations should see the responsibility of keeping the networks data and information safe as a joint effort
ii. All LANs must connect to the server for the purpose of information sharing and network security.
iii. Organizations may adopt this model to ensure the integrity and confidentiality of information

REFERENCES

Aridor, Y and Lange DB (1998), Agent Design patterns; Elementary of Agent Application Design, In proceeding of the second international conference on Autonomous Agent (Agent 98) , ACM press, PP 108-115.

Ayofe A.N,and Irwin B (2010), cyber security; challenge and the way Forward computer science and Telecommunications 29 (6), 56-69.

Farouzen and Fagan (2003) Computer Network protocol

Kamaruzamin M, mohd A, mohd S, Mohammed A.K and Mohd R.M (2011) mobile Agents in infrasion Detection system: Review and Analysis Modern and Applied science 5 (6), 218-231.

Lipmann R and Cunningham S (2000), Improving intrusion detection performance using key word selection and neutral networks, computer network 34 (4), 594-603.

Tanaebaum (2006) Computer Network and security

Volmar T and manic M (2009), computationally Efficient neutral network intrusion security awareness, 2nd international symposium on Resilient control system.

Wamala, F (2011), the ITU national cyber security guide, international Telecommunication union (ITU)