IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

An Enhanced Network Monitoring System using Multi-Agent based Technology

John-Otumu Adetokunbo M[1], Ojieabu Clement E[2], Oshoiribhor Emmanuel O[3]

ICT Directorate, Ambrose Alli University, Ekpoma, Nigeria[1]

Department of Electrical/ Electronics Engineering, Ambrose Alli University, Ekpoma, Nigeria[2]

Department of Computer Science, Ambrose Alli University, Ekpoma, Nigeria[3]

Abstract: This paper aims to present a multi-agent based system for monitoring nodes in network environment. The models developed for the proposed system defines certain deliberative agents that interact together in order to achieve the objectives and requirements of the multi-agent organization, and integration of fault services, security services and configuration services in a single solution platform. The developed model tends to resolve certain challenges like port conflict, hard disk space, memory consumption, and most especially interoperability issue faced by network administrators with respect to installing more than one network monitoring application to monitor and manage a network environment. The proposed multi-agent based network monitor was developed using Core Java, HTML, Hypertext Preprocessor (PHP), JavaScript, JQuery, and MySQL. The developed system was rated highest amongst five different off-the-shelve network based application after system evaluation was conducted.The proposed system is recommended for usage in any local area network.

Keywords: LAN, Multi-agent system, Network monitor, fault, intrusion, configuration

I. INTRODUCTION

Traditional monitoring and evaluation of nodes with a view to resolving problems, and ensuring optimal performance and efficiency normally involve the physical movement of the network administrator from one computer system to another [1, 2] According to [3] the manual monitoring of nodes in a network environment by network administrators can be a very huge task and cannot satisfy the requirements of the modern complex network system.

It became very clear and obvious that the manual monitoring and management of a network environment cannot meet the complex modern day network requirements. The shortcomings of this manual approach have necessitated the need for different diagnostic tools for monitoring and managing a network environment. The diagnostic tools for network management generally can be both hardware and software based, and the software-based tools can be in any of the three forms; standalone, client-server and agent based applications. These tools are designed to perform some specific functions only. For example some network monitoring and analysis tools can be for only fault management in a computer network, some can only perform the task of monitoring and detecting intrusion in networks, some for the purpose of sniffing IP packets only, some for managing bandwidth, some for managing software resources only in a network environment, etc. Though a plethora of techniques have been reported in some of the literatures we reviewed on agent-based software approaches for network management using static agents which are stationary and would not need to move from one node to another in order to execute its objective [3], and mobile agent that has the ability to move or migrate from one node to another in a network environment in order to perform a given task on behalf of the administrator [1]. Different agent-based technologies have been used by different researchers in the field of computer networks and security in achieving a single task in network management e.g. [4, 5, 6, 7, 8, 9, 10] for intrusion detection in networks, [1] for managing bandwidth in computer network, [3] for monitoring software resources in a network environment, [2] mobile agent for monitoring and evaluating users activities in a network environment, etc.

We are proposing a software based approach for monitoring nodes in a network environment using multi-agent based system to carry out different network management services.With the increasing nature of computer network due to network services oriented demand; most network administrators may often need to install two or more software diagnostics or monitoring tools on their network in order to monitor their network environment effectively.

These different applications or platforms may sometimes cause problems such as follows:

i. Port conflict
ii. Memory allocation conflict / consumption
iii. Harddisk drive space consumption
iv. Bandwidth consumption
v. Software diagnostic applications interoperability issue, etc

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

These problems identified above may cause the network administrator to be less efficient in terms of monitoring the network environment status. However, [3] recommends that network administrators will function more efficiently if agent-based network monitoring system is designed to include configuration management, fault management and security management in a single platform. The situation above has therefore created a gap in knowledge which this research work intends to fill; that is, to integrate and configure different network monitoring services into one solution platform. The major aim of this study is to develop a single automated platform for setting up and executing different services for monitoring nodes in a network environment using a multi-agent based approach.

II. LITERATURE REVIEW

The true concept of agent and multi-agent based technology originated from artificial intelligence [11, 12]. Multi-agent based system can be seen as a system that is a loosely coupled network troubleshooter or solution provider that works together to solve issues that is beyond the capability of an individual agent [13].
Thus the roots of the concept date back to the 1950s when artificial intelligence (AI) was born. Software agents are secret software detectives that provide a general computing platform for executing task like information gathering, information filtering and searching, online shopping, personal assistant, etc. Software agent can exist as a single entity or in collaboration with other agents in the same environment to carry out some specific task which can be referred to as multi-agent system.
Multi-agent system properties and agent properties according to [14, 15] are adaptability, autonomy, pro-activity amongst others.Applications of multi-agent based technology are in different areas.[16] designed a multi-agent system for network security management. The focus of [16] research work concerns one critical security management issue, that is intrusion detection. However, this approach provides a flexible integration of multi-agent technique in a classical network to enhance its protection level against inherent attacks.[17] developed a multi-agent system implementation for network management based on SNMP Protocol.The multi-agent system consisted of several agents whose main aim was to facilitate the effort of network management according to the established policies; the agents were built using the JADE platform.

III. METHODOLOGY

Our proposed automated network monitoring system will integrate configuration services, fault management services and security services into a single software platform in order to monitor nodes in a network environment effectively using multi-agent based approach as recommended by [3].

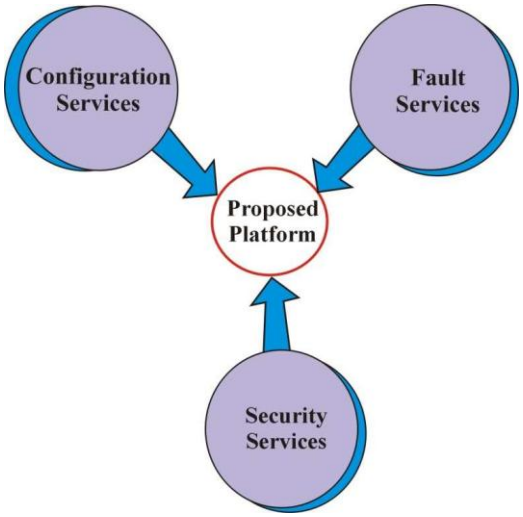

Figure 1: Our proposed automated network monitor framework

Figure 1 shows the diagram of our proposed automated network monitor system framework. The framework integrates three different network services into a single domain for monitoring a computer network using multi-agent based system.
The multi-agent will work together in the same domain in order to carry out the three specific network services within the single solution platform. Our multi-agent based approach is represented as follows:
AMP = {MAS, S, N}
Where:

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

AMP = Agent Management Platform
M AS = Multi-Agent System which consists of eight agents cooperating and communicating within an environment defined by S and N.
S = a set of processing nodes in which the agents perform services
N = a network switch that connects processing nodes and allows communication between them.
The set of processing nodes is denoted as S = {S_1, S_2, S_3, S_4, …, S_i, … , S_n}.

Each node S_1 can provide an operating environment for the agents.
A network switch N connecting nodes from S is represented by an undirected graph,
N = (S, E)
E is the set of links which could be network cables or wireless connection established to form the network.
E = {l_1, l_2, l_3, …, l_n} where l_1 = {N, S_1} which represents a link between the network switch N to node S_1.

The agents in the Multi-Agent System (MAS) = {svrA, cA, mA, fdA, idA, shA, nA, sA}
Where: svrA= server_agent
cA = client_agent
mA = mobile_agent
fdA = fault_detection_agent
idA = intrusion_detection_agent
shA = shutdown_agent
nA = notification_agent
sA = security_agent

These agents interact with each other by performing some kind of elementary services to achieve a set of goal.
The functionality of the multi-agents in a single platform is also defined by a set of elementary services (ES) supported by the system.
ES = {es_1, es_2, es_3, …,es_n}

Here, elementary services (ES) is defined as the basic services an agent can perform as requested by the system / network administrator.

The following are the elementary services performed by the agents:
(i) The server_agent (svrA) = {establish connection to all client_agent, monitor all nodes, create a platform for cooperation amongst agents, send event occurrence to notification agent, receive regular updates from the client_agent}
This is represented by (sA) = {es_1, es_2, es_3, es_4, es_5}
(ii) The client_agent (cA) = {gather information about nodes, transmit information to server agent for update, perform shutdown action on node, transmit event to notification agent}
This is represented by (cA) = {es_1, es_2, es_3, es_4}
(iii) The fault_detection_agent (fdA) = {probe all the nodes continuously, monitor nodes status, detect faulty nodes, transmit event to the notification agent}
This is represented by (fdA) = {es_1, es_2, es_3, es_4}
(iv) The intrusion_detection_agent (idA) = {monitor nodes, detect anomaly intrusion, update information, transmit event to the notification agent}
This is represented by (idA) = {es_1, es_2, es_3, es_4}
(v) The shutdown_agent (shA) = {receives message from server_agent, performs shutdown action, sends message to notification agent}
This is represented by (shA) = {es_1, es_2, es_3}
(vi) The notification_agent (nA) = {receives messages from other agents, sends a near real-time event occurrence via screen alert system, and sms alert system}
This is represented by (nA) = {es_1, es_2, es_3}
(vii) The security_agent (sA) = {creates a secured end-to-end communication between the server and the clients agents by encrypting and decrypting messages before and after transmission}
This is represented by (sA) = {es_1, es_2}
(viii) The mobile_agent (mA) = {executes shut down operations, update profiled records}
This is represented by (mA) = {es_1, es_2}

Figure 2 shows our proposed multi-agent based system architecture having eight agents cooperating in the same domain to perform network monitoring services in order to meet our major aim. The functions of the various agents are as follows:

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

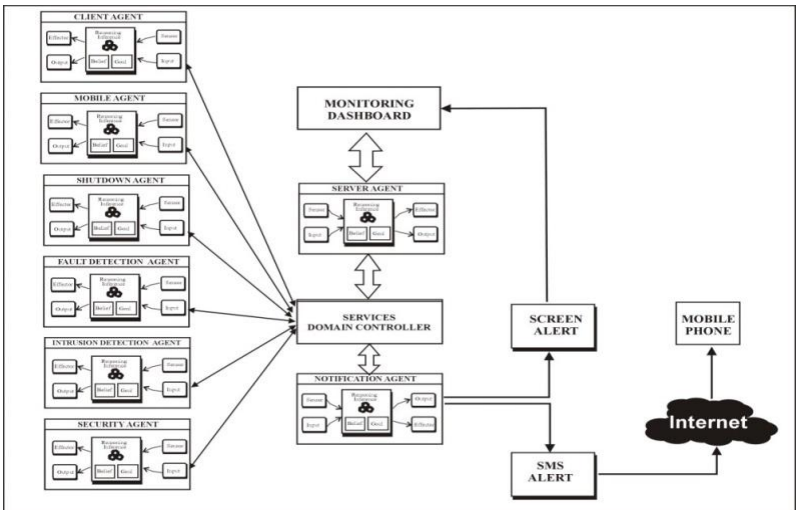

Figure 2: Proposed multi-agent based system architecture

Server Agent
The server agent is a backend static agent. It executes only on the network administrator's system where the agent management system is installed and resides. It is used to perform the initial configuration processes, network probing, data gathering, analysis and mining functions by the network administrator. It can accept and send requests to and fro other agents. It sends messages to the report handler for onward transmission to the network administrator's screen notification system and also integrates with web services for sms alert via mobile phone. The directory facilitator controls and coordinates all the agents operations and processes, while the messaging subsystem assist in agent communications.

Client Agent
The client agent is a static agent installed on all the computers on the computer network. It helps to fetch vital information about each computer it is resident on and also pass instructions to the client operating system to execute specific task like shutdown operation. It also helps to gather update information about each computer or client node for onward transmission to the server agent using the mobile agent.

Fault Detection Agent
The fault detection agent is designed as a reactive agent that monitors the entire profiled nodes on the local area network in order to detect nodes active or inactive status using an active probing system and rule based technique for classification. The fault detection mechanism flags an alert message indicating fault detected through the notification agent (screen / sms alert) as soon as any system status changes state from active to inactive. This change of status can be as a result of system shutdown or network cable problem.

Intrusion Detection Agent
The intrusion detection agent is a detection mechanism for detecting anomaly node(s) in the network environment. The agent is trained to be intelligent for the intrusion detection task using the Fuzzy ART techniques. The system constantly monitors the network traffic, gathers and analyzes live data patterns from all devices on the network. The data pattern about any device on the network is compared against the normal threshold value for normalcy or anomaly intrusion classification as the case may be. All intrusion information are logged and screen / sms alert messages are also sent to the network administrator.

Notification Agent
The notification agent performs the function of sending a near real-time alert message of all network event occurrences as screen alert message on the network monitor dashboard and short message service (sms) to the network administrator's mobile phone.

Shutdown Agent
The shutdown agent is an autonomous and reactive agent designed to shutdown all profiled nodes with active status on the network using a pre-scheduled time. It gives the computer users a time grace of 1 minuteto save their jobs before executing the shutdown command.

Security Agent
The security agent creates a secureend-to-end communication between the server agent and the client agentresident in each node on the network by encrypting and decrypting messages (node name, ip address, mac address, and system

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

name) before and after transmission to prevent malicious agents from getting hold of sensitive information using a double DES algorithm.

Service Domain Controller
The service domain controller is directly in-charge of monitoring and controlling all the agents' services in the domain. It must first be started before activating any other agent.

Mobile Agent
The mobile agent is the messaging agent that can be dispatched from the service domain controller to other nodes in the network environment. It helps to monitor each node on the network, deliver shutdown command operation to each client agent and update records between the client and server agents. We designed the mobile agent to use the remote object command for its internal operations.

IV. IMPLEMENTATION AND TESTING

In system implementation, our proposed architectural designs were converted into implementable program codes using the following programming languages: Hypertext Preprocessor (PHP), JavaScript, JQuery, Hypertext Markup Language, Core Java and MySQL. The sub-components of the system were built and integrated to form the complete network monitoring software prototype based on the strength of the chosen programming languages.

Table 1: System specification for testing the developed network monitor

Processor	Intel® Core™ i7-2640M CPU@ 2.80GHz, 2.80GHz
Memory	4GB
Hard Disk Drive Space	500GB
Network Interface Card (NIC)	Gigabit Fast-Ethernet NIC
Operating system (Server-Node)	Microsoft Windows 7 (64-Bit)
Operating system (Client-Node)	Microsoft Windows 7 (32/64-Bit) Microsoft Windows XP (32-Bit)
Network Switch	D-Link DES-1024D 10/100 Fast Ethernet (24-Ports Non-management switch)
Wireless Router	TP-Link 300Mbps Wireless N USB ADSL2 + MODEM ROUTER
Network Cable	CAT 6 UTP

Table 1 shows the system specification for deploying and testing the proposed multi-agent based network monitoring application.
The system testing provides a documented basis for ensuring that the developed software prototype will perform its functions as required. It ensures that the system output is in line with the initial aim and objectives; and this plays an important role of verification and validation in software prototype development.

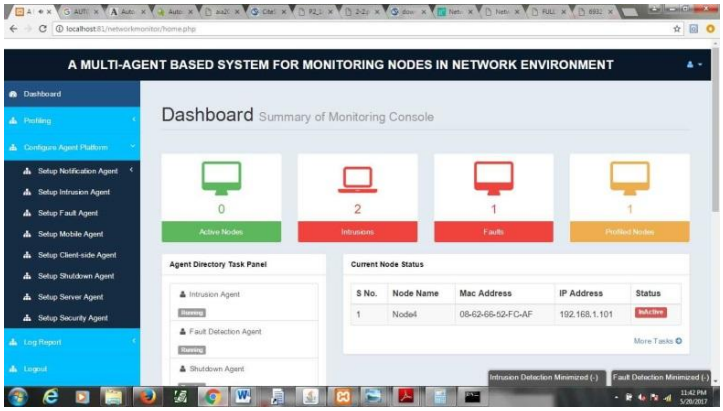

Figure 3: Developed Network Monitor (web interface home page)

Figure 3 shows the developed network monitor (web interface home page). From this web interface; the network administrator can profile new node on the network, activate / deactivate the multi-agents task, view logs of intrusion and faults detected, view current node, fault and intrusion status, view screen notification alert messages of intrusion and fault detected and finally logout.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

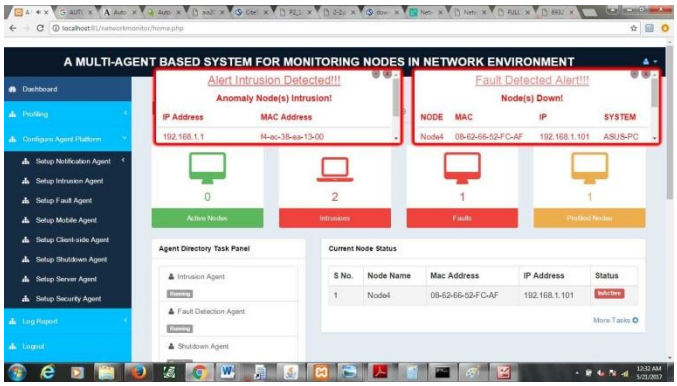

Figure 4: Developed Network Monitor Prototype with screen notification alert

Figure 4 shows the screen notification alert messages of the anomaly node intrusion and fault detected on the developed network monitor web interface.

V. SYSTEM EVALUATION

In this section, we evaluated our proposed multi-agent based network monitoring applicationagainst five different off-the-shelve network monitoring application based on their system features.

Table 2a: Evaluation based on system features

System Features	Our Proposed Network Monitor	Microsoft Network Monitor	Advanced IP Scanner	Fiddler Network Monitor	The Dude Network Monitor	PRTG Network Monitor
Web based interface	YES	NO	NO	YES	YES	YES
Remote Control	YES	NO	YES	NO	YES	NO
SMS Alert	YES	NO	NO	NO	NO	YES
Screen Alert	YES	YES	YES	YES	YES	YES
Speed	YES	YES	YES	YES	YES	YES
Reliability	YES	YES	YES	YES	YES	YES
Email Alert	NO	NO	NO	NO	NO	YES
User friendly interface	YES	YES	YES	YES	YES	YES
Configuration services	YES	YES	YES	YES	YES	YES
Security services	YES	NO	NO	YES	NO	NO
Fault services	YES	NO	NO	NO	NO	NO
Agent-based	YES	NO	NO	NO	YES	NO

Table 2a shows a list of six different network monitoring software and twelve system features used as criteria for evaluation. “Yes” or “No” response of the system features is filled against each software as it applies to it based on close interaction and observation with each of the software under examination.

Table 2(b) is a deduced from Table 1(a) based on the “Yes” / “No” values captured.
Here, “Yes” = “1”
“No” = “0”
The percentage rating for each network monitoring application is calculated based on the data represented in Table 2(b). The percentage rating for each application is calculated as follows:

$$\text{Percentage rating} = \frac{\text{Number of passed system features}}{\text{Total number of system features}} \text{x} \frac{100}{1}$$

Table 2(b) also revealed that our proposed network monitoring application has the highest rating with 91.67% for system features as indicated, next is the Dude and PRTG Network Monitors which both rated 66.67% for second position, followed by Fiddler Network Monitor which rated 58.33% for the third position, also followed by Advanced IP Scanner which rated 50% for the fourth position and finally, Microsoft Network Monitor which rated 41.67%

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

Table 2b: Percentage ratings of the applications based on system features

System Features	Our Proposed Network Monitor	Microsoft Network Monitor	Advanced IP Scanner	Fiddler Network Monitor	The Dude Network Monitor	PRTG Network Monitor
Web based interface	1	0	0	1	1	1
Remote Control	1	0	1	0	1	0
SMS Alert	1	0	0	0	0	1
Screen Alert	1	1	1	1	1	1
Speed	1	1	1	1	1	1
Reliability	1	1	1	1	1	1
Email Alert	0	0	0	0	0	1
User friendly interface	1	1	1	1	1	1
Configuration services	1	1	1	1	1	1
Security services	1	0	0	1	0	0
Fault services	1	0	0	0	0	0
Agent-based	1	0	0	0	1	0
No. of Passed features	**11**	**5**	**6**	**7**	**8**	**8**
Total No. of features	**12**	**12**	**12**	**12**	**12**	**12**
Percentage rating	**91.67**	**41.67**	**50.00**	**58.33**	**66.67**	**66.67**

Table 2c: Summary of Table 2b

Our Proposed Network Monitor (%)	Microsoft Network Monitor (%)	Advanced IP Scanner (%)	Fiddler Network Monitor (%)	The Dude Network Monitor (%)	PRTG Network Monitor (%)
91.67	41.67	50.00	58.33	66.67	66.67

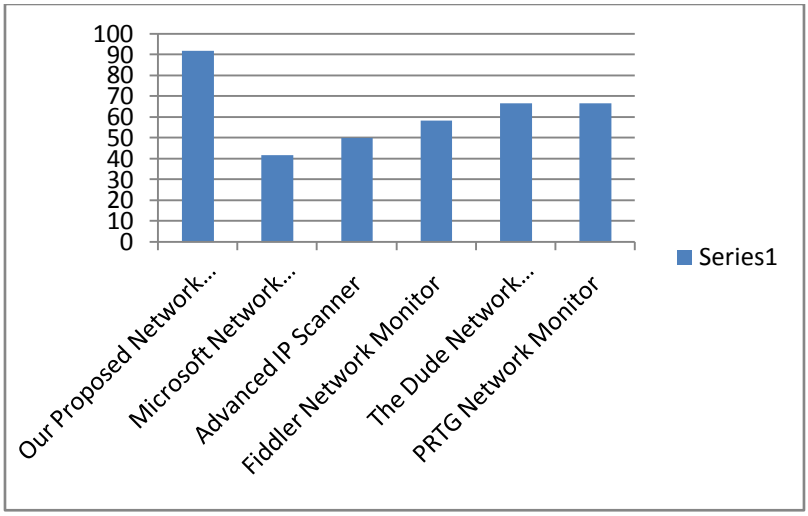

Figure 5: Graphical representation of Table 2c

VI. CONCLUSION

The analysis and design of our proposed network monitoring application using multi-agent model is highly efficient. The Ontology of fault, intrusion detection and configuration services integration into a single platform using MAS for network environment is an important representation to solve network administrator's problems.

The proposed developed system could be relatively compared against some off-the-shelvesoftware solutions in terms of response time and speed. In future, network monitoring / management solutions need to be very intelligent and flexible in order to reduce burden on network administrators and resources. More network services require seamless integration in a single solution platform using multi-agent technology architecture.

REFERENCES

[1] Imianvan, A. A. (2009). Development of Mobile Agent for Evaluating the Use of Bandwidth in a Computer Network, PhD Thesis, Department of Computer Science, Federal University of Technology, Akure. In (Akinyokun, O. C., Ekuewa, J. B., and Arekete, S. A., 2014) Development of agent-based system for monitoring software resources in a network environment, Artificial Intelligence Research, Published by Sciedu Press, Vol. 3, No. 3
[2] Arekete, S. A. (2013). Development of a Mobile Agent for monitoring and Evaluation of Activities of Users in a Network Environment, PhD Thesis, Department of Computer Science, Federal University of Technology, Akure, In (Akinyokun, O. C., Ekuewa, J. B., and Arekete, S. A., 2014) Development of agent-based system for monitoring software resources in a network environment, Artificial Intelligence Research, Published by Sciedu Press, Vol. 3, No. 3
[3] Akinyokun, O. C., Ekuewa, J. B., and Arekete, S. A. (2014). Development of agent-based system for monitoring software resources in a network environment, Artificial Intelligence Research, Published by Sciedu Press, Vol. 3, No. 3
[4] Singh, M., and Sodhi, S. S. (2007). Distributed Intrusion Detection using Aglet Mobile Agent Technology, In Proceedings of National Conference on Challenges and Opportunities in Information Technology, Mandi-Gobindgarh, pp. 148-152
[5] Chaudhary, V. K., and Upadhyay, S. K. (2013) Distributed intrusion detection system using sensor based mobile agent technology, International Journal of Innovations in Engineering and Technology (IJIET), Vol. 3(1), pp. 220-226
[6] Sen, J. (2010). An Agent-Based Intrusion Detection System for Local Area Networks, International Journal of Communication Networks and Information Security (IJCNIS), Vol. 2(2)
[7] Jansen, W., Lell, P., Karygiannis, T., and Marks, D. (1999). Applying Mobile Agents to intrusion detection and response, NIST Interim Report (IR)-6416.Association of Computing Machinery.
[8] Jansen, W. (2002) Intrusion detection with mobile agents. ELSEVIER, Computer communications, 25(1)
[9] Chan, P. C., and Wei, V. K., (2002). Preemptive distributed intrusion detection using mobile agents. Proceedings of the eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises.
[10] Dasgupta, D., Gomez, J., Gonzalez, F., Kaniganti, M., Yallapu, K., and Yarramsettii, R. (2003). MDS: Multilevel Monitoring and Detection System, In the Proceedings of the 15th Annual Computer Security Incident Handling Conference, pp. 22-27, The Westin, Ottawa, Ontario, Canada
[11] Weiss (1999) Multi-Agent Systems, MIT Press
[12] Wooldridge, M. (2002) An Introduction tomulti-agent systems. John Wiley & Sons Limited England, ISBN: 0-471-49691-X
[13] Jennings, N. R., and Wooldridge, M. J. (1998). Application of Intelligent Agent: Foundations, Applications and Markets, pp. 3-28, Secaucus, NJ, Springer-Verlag, Berlin.
[14] Chang, Y. S., Yang, C. T., and Luo, Y. C. (2011) An Ontology based Agent Generation for Information Retrieval on Cloud Environment. J. UCS, **17**(8): p. 1135-1160.
[14] Teixeira de Oliveira,R. F. "Gestion des Réseaux avec Connaissance des Besoins: Utilisation des Agents Logiciel", PhD thesis, Eurécom institute, France, 1998.
[15] Guessoum, Z. andBriot, J. P. "From Active Object to Autonomous Agents", IEEE Concurrency, Volume 7(3), pp. 68-78, July/September, 1999.
[16] Boudaoud, K. and Zahia, G. (2000). A Multi-agents System for Network Security Management. Sixth IFIP Conference on Intelligence in Networks (SmartNet'2000), Vienna, Austria, September 18 - 22, 2000
[17] Duque M. N.D., Mejía S. M.H., Isaza G., and Morales A. (2009). Multiagent System Implementation for Network Management Based on SNMP Protocol. In: Corchado J.M., Rodríguez S., Llinas J., Molina J.M. (eds) International Symposium on Distributed Computing and Artificial Intelligence 2008 (DCAI 2008). Advances in Soft Computing, Vol. 50. Springer, Berlin, Heidelberg

BIOGRAPHIES

John-Otumu Adetokunbo Mac Gregor is currently pursuing Ph.D in Computer Science atEbonyi State University, Abakaliki, Nigeria. He obtained his M.Sc(Info Tech) from National Open University of Nigeria and M.Sc (Computer Science) from Ambrose Alli University, Ekpoma, Nigeria. He is a Senior Technologist in the Directorate of Information and Communication Technology, Ambrose Alli University, Ekpoma, Nigeria. He is a registered member of the Nigeria Computer Society (NCS) and also a Chartered Information Technology Professional registered with the Computer Professionals Registration Council of Nigeria (CPN). His research interest includes computer communication systems, agent computing and multi-agent based systems, network security and soft computing. He has published over 17 articles in both local and international Journals.

Engr. (Dr.) Ojieabu Clement Eghosa holds a Ph.D in Communication Engineering, M.Eng in Electronic & Telecommunication Engineering and B.Eng in Electrical/Electronic Engineering. He is an Associate Professor of Communication Engineering at the Department of Electrical/Electronic Engineering, Ambrose Alli University, Ekpoma. He is a registered engineer with the Council for the Regulation of Engineering in Nigeria (COREN). His research interest includes Data communication and security, intelligent systems and satellite communication systems. He has published over 30 articles in both local/international journals and conference proceedings.

Dr. Oshoiribhor Emmanuel Osaze holds a Ph.D in Computer Science from Ambrose Alli University, Ekpoma, Nigeria, M.Sc., and B.Sc. (Hons) Computer Science from University of Benin, Nigeria. He is a Lecturer in the Department of Computer Science, Ambrose Alli University, Ekpoma, Nigeria. He is a registered member of Nigeria Computer Society (NCS). His research interest includes Data Mining, Artificial Intelligence, and Software Engineering He has published over 16 articles in both local and international Journals.