BOOK CHAPTER | Alternative Engineering Desigsn
dx.doi.org/10.22624/AIMS/REBK2022-P15

Design Methodology For The Development Of A Multi-Agent Intrusion Detection System For Countering Distributed Denial Of Service (Ddos) Attacks In Mobile Ad-Hoc Networks.

Nwaocha, V.O.
Department of Computer Science, National Open University of Nigeria, Abuja, Nigeria
Department of Computer Science, Lagos State University, Ojoo, Lagos State, Nigeria
E-mails: ogochukwuvee@gmail.com; ayglo55@yahoo.com

ABSTRACT

The proliferation of wireless mobile devices has revolutionized the world, leading to the popularity of the mobile ad hoc networking technology [1]. This emergence of the mobile ad hoc network (MANET) has facilitated the drift from personal computing to ubiquitous computing in our society. Today, mobile devices such as smartphones, laptops, notebooks and tablets are fast becoming an integral part of man's life and a good number of those in the academia and industry now access the Internet on-the-go, through a wide range of mobile devices. In this paper, we provide our design methodology for the development of a multi-agent intrusion detection system for countering distributed denial of service (DDOS) attacks in mobile ad-hoc networks.

Keywords: DDOS, Mult-agent intrusion detection, security, MANET, Attacks.

1. INTRODUCTION

Choosing a well-defined agent-oriented development approach is critical for the effective development of the anticipated system. Given the fact that object-oriented methodologies cannot be directly applied in developing agent-based systems, various agent-oriented software development methodologies have been proposed for developing multi-agent systems. Some of the prominent agent-oriented software development methodologies include: Gaia, Tropos [98] and MASE [99]. The Multi-agent Systems Engineering (MASE) methodology was employed for the system development. The general operation of the MASE follows the phases detailed in Figure 1.

Typically, the MASE analysis phase comprises three steps: capturing goals, applying use cases, and refining roles. While the design phase consists of four steps: Creating Agent Classes, Constructing Conversations, Assembling Agent Classes, and System Design.

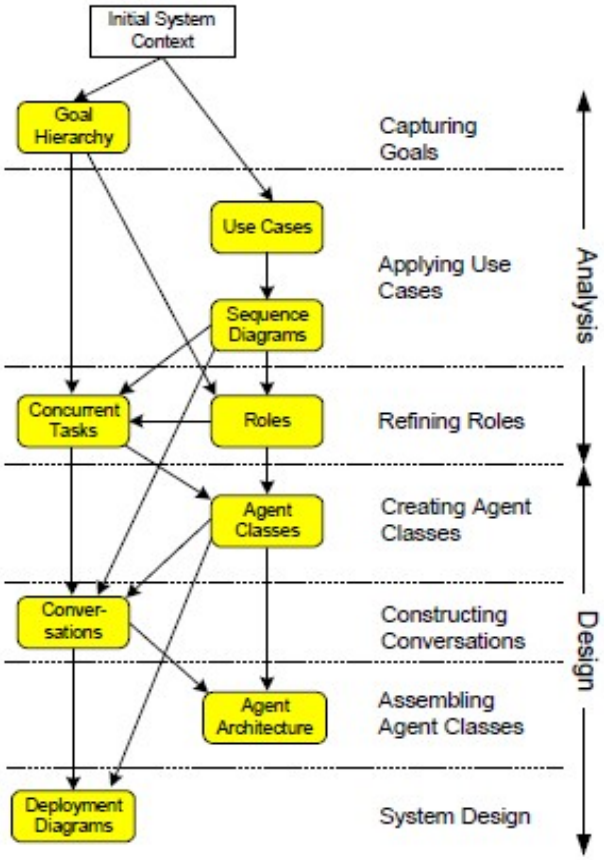

Figure 1: MASE Development Phases [99]

2. DESCRIPTION OF THE EXISTING SYSTEM

The targeted institution was the Yaba College of Technology commonly referred to as "Yaba Tech". This college was founded in 1947 as Nigeria's first higher educational institution. Currently it has a student enrolment of over 16,000. Yaba College of Technology (YCT) is one of the leading academic institutions, recognised as a centre of excellence with nine world-class schools and a number of acclaimed departments [100]. According to the decree establishing the college, its main objectives are to provide full time and part-time education and training in Technology, Commerce, Management and Applied Science, in accordance with Nigeria's need for development.

Meanwhile, the recent admission policies of Nigerian Universities have been unacceptable to the public, given the fact that many applicants go through a lot of difficulties while seeking admission since there are limited spaces in the Universities. Each year, thousands of applicants sit for the Joint Admissions and Matriculation Board(JAMB) examinations and less than twenty per cent (20%) on the average gain admission into the universities [101].

In order to facilitate the accomplishment of its core mission, Yaba College of Technology (YCT) employs the Internet, which serves as the hub of the administrative and academic activities at the college. The YCT network is widely available across the campus to Students, Lecturers and other Administrative Staff who readily access this network via portable devices. Amongst the portable devices, the most commonly used at the Yaba College of Technology are laptops. While the YCT network has brought great benefit to the campus, it has also made critical systems more susceptible to malicious network attacks. Among the different threats that have been witnessed on the YCT network, viruses and distributed denial of service attacks have been the most prevalent.

As part of the effort to protect its network, firewall and anti-virus were installed on the YCT network to serve as Intrusion Prevention Systems. Firewall allows only for the desired Internet Protocol (IP) addresses and ports to send traffic through it, but is unable to determine whether the traffic is a normal or nefarious one. Therefore, firewall has certain benefits, but it obviously lacks the ability to detect attacks. On the other hand, intrusion detection system on detect attacks by monitoring the network traffic. When an intrusion activity occurs in a network, an alert is generated by IDS which prompts the network administrator for instigating and action to block or mitigate the attack.

Although these schemes provide some level of security, they have been found to be deficient in a number of ways and do not provide sufficient protection against Distributed Denial of Service (DDOS) attacks. Consequently, the college has witnessed frequent downtime due to DDOS attacks.

Another challenge faced by this institution is related to the centralised network management model based on client-server model which is no longer suitable for the present heterogeneous and ubiquitous setting on campus. Therefore an intrusion detection system with distributed management architecture that supports multiple agents is proposed to tackle the issue of the centralised management architecture. Given the distributed nature of DDOS attacks and the multiple entry points of intrusion on the campus mobile ad hoc network, a multi-agent based solution was sought in order to achieve a more effective and inclusive intrusion detection. Consequently, this thesis presents network architecture and entities suitable for specific institutional requirements. The proposed system is built in a modular and flexible way which makes it easy for future-expansion.

2.1 Analysis of the existing system

The analysis of the current system entailed determining the structural requirements based on the components interrelationships in order to eliminate redundancies. A number of steps were taken in order to effectively explore the existing system.

3. METHODOLOGY

3.1 Data Gathering

Primary sources of data gathered from the Yaba College of Technology network include; direct observation, discussions and interviews, while the secondary sources of data were from books, journals, Internet among other resources. The selection of the study area was based on the availability of the network and other resources.

3.2 Data Analysis

A critical analysis of the existing system was undertaken with a view to identifying the problems, and subsequently designing a system that will elicit a prompt response to intrusion detected or suspected. To make certain that the end product meets the specification of users as well as to ascertain their requirements and expectations, meetings were scheduled with the prospective users, who are the Network Administrators in the Institution.

Prior to embarking on this project, a preliminary survey was carried out within the Yaba College of Technology. The Faculty, Students as well as ICT support personnel of this institution were interviewed. Findings from the survey indicated the prevalence of manifold attacks, especially distributed denial of service (DDOS) attacks on the YCT network evidenced by the frequency of the down times. Other forms of intrusions include traces of viruses and worms emerging from private systems. It was thus established that there was an essential need for an effective solution that will protect the systems on the network.

The backscatter analysis technique was employed for estimating the prevalence of different attacks. Figure 3. 2 shows the backscatter monitoring platform deployed on the YCT network.

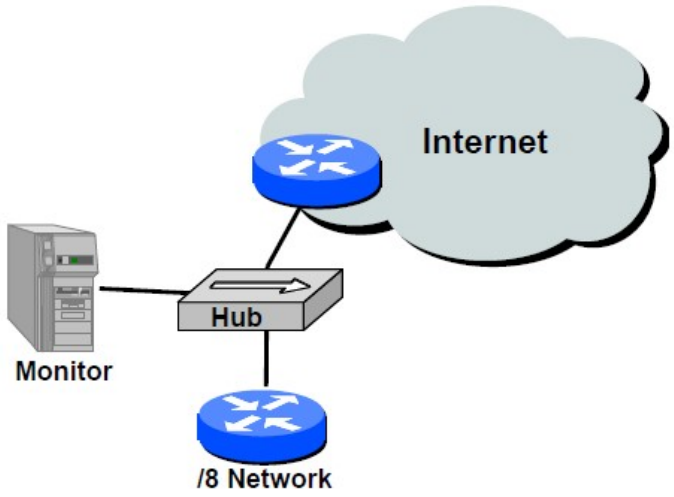

Fig 2: The Backscatter Monitoring Platform

The infrastructure employed in monitoring the network consisted of a PC configured to capture all Ethernet traffic, and attached to a shared hub at the router terminating this network. This setup is depicted in Figure 3.4. During the course of this investigation, the upstream router filtered some traffic meant for the network. However, this had no significant impact on our results. It was equally observed that small portions of our address prefix were occasionally "hijacked" by inadvertent route advertisements elsewhere in the Internet.

On the whole, three traces were gathered while carrying out this investigation in 2014, each trace roughly spanning a one month period, beginning from May 1st and extending to July 31st, while isolating the inbound portion of the network.

Subsequently, the overall frequency of attacks observed in the gathered traces is shown, and the attacks are classified according to both the type of attack and the type of victim.

Table 1: Summary of the Backscatter Database

Unique victim IDs	**1,942**	**1,821**	**2,385**
Attacks	**4,173**	**3,878**	**4,754**

Unique victim IDs	**2,835**	**2,601**	**2,613**
Attacks	**56,173**	**50,745**	**52,454**

Unique victim Ins	**3,147**	**3,034**	**3,849**
Attacks	**112,457**	**102,204**	**110,025**

On the whole, results of the analysis indicate widespread DDOS attacks across the institution. The size and length of the attacks were observed to be heavy-tailed, with a huge number of extensive attacks constituting a significant fraction of the overall attack volume.

3.3 Limitations of the existing system

To facilitate the accomplishment of its core task, Yaba College of Technology employs the Internet, which serves as the hub of the administrative and academic activities at the institution. It is through Internet-mediated support services that students enjoy support from this institution.

On the other hand, Yaba College of Technology has had to face the challenge of keeping its networks secure from invasions, particularly denial of service attacks (DOS) attacks while accommodating the regular influx of learner, faculty and staff-owned devices through which they carry out a wide range of both authorised and unauthorised activities from diverse network locations. The impact of these prevalent attacks on the YCT network has often led to excessive downtime for the thousands of users on the network.

Currently, the institution subscribes to an external vendor, for the provision of network security by means of intrusion detection system. However, a recent analysis of the institution's online transaction data highlighted the extent to which some hosts within the College network had already been compromised thus demonstrating the inefficiency of the security solution.

The drawbacks identified were as follows:

i. High rate of false alarms
ii. Limited attack detection coverage
iii. Passive response to attack as administrator is left to take required action
iv. High network overloads
v. Limited extensibility

4. REQUIREMENTS

Researchers have defined a set of desirable characteristics for an intrusion detection system along two themes: functional and performance requirements. Following from the analysis of the security scheme deployed on the Yaba College of Technology network and the identification of the limitations in the existing security system deployed on YCT's network, the requirements for the projected system were carefully specified.

4.1 Functional requirements

Cognisant of the precise requirements for detecting DDOS attacks in mobile ad hoc networks, the following functional requirements were specified for the system:

i. The system should record accurate information associated with detected events;
ii. It should be able to obtain the complete list of alerts discovered within a certain period configured by the network administrator;
iii. It ought to detect the three prevalent forms of DDOS attacks namely: Transmission Control Protocol Synchronize (TCP SYN) flood, User Datagram Protocol (UDP) flood and Internet Control Message Protocol (ICMP) flood
iv. The system ought to allow the network administrator generate an updated report;
v. It should be able to minimise the consumption of network resources.

4.2 Performance requirements

Based on the criteria for developing an ideal intrusion detection system [102], the anticipated system should support the following requirements:

i. The intrusion detection system (IDS) should perform its operation without increasing overhead loads;
ii. Intrusion should be detected in real-time and reported instantly in order to curtail the damage to the network;
iii. It ought to be scalable in order to handle additional computational and communication load;
iv. The IDS should not introduce a new weakness in the mobile ad hoc network;
v. It should run continuously and remain transparent to the system and users.
vi. It must be fault-tolerant in the sense that it must be able to recover to the previous state, and resume the operations before the crash.
vii. IDS should not only detect but also smartly respond to detected intrusions;
viii. It should inter-operate with other intrusion detection systems to collaboratively detect intrusions.

4.3. Identification of agent classes

In line with the MASE development steps, a set of multiple agents were employed in the multi-agent intrusion detection system, in order to detect and respond to DDOS attacks more effectively:

i. Monitor agents
ii. Analyzer agents
iii. Universal agents
iv. Response agents

4.4 Specification of agent roles

By ascertaining the precise agents to be used in the multi-agent intrusion detection system, their corresponding responsibilities were detailed.

The different agent types and their responsibilities are listed in Table 2.

Table 2: The Different Agent Types And Their Responsibilities

S/N	Agent Type	Responsibility
1	Monitor agents	Captures raw network traffic Gathers system log files and data packets Forwards captured network traffic to analyser agents Sends report of valid IP address to universal agents
2	Analysis agents	Examines data from monitor agents Applies detection rules in order to identify specific forms of intrusions or suspicious data Sends appropriate commands to the response agents based on precise forms of attacks such as DDOS flooding attacks
3	Universal agents	Requests for private information to confirm node identity; Instructs monitor agents to allow traffic to and from registered nodes; Checks reports and eliminates nodes whose IP address is not listed in the valid IP address report
4	Response agents	Blocks the source of DDOS flooding attack Terminates unacknowledged requests Ignores random port requests Ignores unidentified pings

4. The Multi-agent Intrusion Detection Process

This section details the processes which represents the mechanism by which the multi-agent intrusion detection system detects and responds to intrusion.

When a node requests to connect to the network, the universal agent (U_a), demands that the node provides its private (secret) details. If the node makes its private records available, providing the HMAC value, the universal agent transmits a message indicating the success of the registration process, which is a form of authentication.

Normally, the transmitted message details the following:

The survival period of time, given as **SST**.
The SST expresses the period within which the private details will be valid;
The total number of bytes, N, permitted to and from each node; this is given as:
N = Bn/Hn where Bn is the total assigned bandwidth which is available and Fin is the total number of available nodes in the network

After successfully establishing the treaty scheme, the nodes are permitted to transmit and receive only N bytes of data at a specific period of time. Subsequently, the universal agent informs the monitor agent to authorize the traffic to and from the registered node.

Meanwhile, the monitor agent maintains a table containing internet protocol (IP) addresses of registered nodes as well as the timer values (T_1, T_2 ...T_n) of all the nodes.

The following rules ought to be maintained in the course of the multi-agent intrusion detection:

All nodes are required to transmit their timer values at regular intervals to the monitor agents.

The monitor agents then verify these timer values and determine the threshold. The threshold is given as: ┌ **= T**$_1$ —T_0.

Subsequent T values must be equal to the threshold.

In other words, verify that T_3-T_2= ┌

If not verify whether T_4 -T_3= ┌

In the event that T_4 -T_3 = ┌**;** then the monitor agent does not permit that node to be a part of the network. It equally obstructs all traffic to and from the node.

The treaty scheme is established by means of the node's timer values. Any node attempting to join the network must primarily, make a request to be connected. In order to forestall any form of unauthorised access, each node must be registered with the universal agent before joining the network. Hence, attackers are unable to spoof the valid user's IP address.

Each universal agent maintains a Host Profile table which consists of information about each host (H1, H_2,…H_n). Table 3.

Table 3. Universal Agent

		Host Prof le Table			
	IP Address	Private(Secret) Information			
Host Name		IP	MAC	Private (Secret)	T

5. CONCLUDING REMARKS

The host profile table comprises of three fields namely: the host name, host IP address, private details about the host. In the same way, the private details consists of the following: IP address of nodes, Mac address of nodes, secret key that changes periodically after the survival period elapses, the timer values of the nodes

BIBLIOGRAPHY/WORKS CITED/CONSULTED

[1] Y. Zhang, W. Lee and Y. Huang, Intrusion Detection Techniques for Mobile Wireless Networks, Page Numbers (3-4), (2003).

[2] M. Weiser, The Computer for the Twenty-First Century, Scientific American, (1991).

[3] M.S. Corson, J.P. Maker and J.H. Cernicione. Inter-based Mobile Ad Hoc Networking, IEEE Internet Computing, pages 63-70. (1999).

[4] A. Mishra and M. Ketan. Security in Ad hoc Wireless Networks in the Handbook of Ad hoc Wireless Networks CRC Press LLC (2003).

[5] P. Papadimitoas and J.H. Zygmunt, Securing Mobile Ad Hoc Networks in the Proceedings of Ad Hoc Wireless Networks . Chapter 31. CRC Press LLC. (2003)

[6] Naumann I, Hogben G, Fritsch L, Benito R , Dean R.Security Issues in the Context of Authentication UsingMobile Devices (Mobile eID), European Network andinformation Security Agency (ENISA), (2008.)

[7] P. Gupta and M. Kirkire. Intrusion Detection in Manet. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering.Vol. 2, Issue 4, April (2013).

[8] L. Garber. Technology News: "Denial-of-Service Attacks Rip the Internet". (2000). Retrieved from: ftp://im1.im.tku.edu.tw/assistant/bearhero/00839316.pdf

[9] Incapsula. DDOS Protection Services Distributed Denial of Service Attack (DDOS) http://www.incapsula.com/DDOS/DDOS-attacks/ (2013)

[10] R. Puri, Bots and Botnet – an overview, Aug. 08, 2003, [online] http://www.giac.org/practical/GSEC/Ramneek Puri GSEC.pdf

[11] B. Todd, Distributed Denial of Service Attacks, Feb. 18, 2000,[online] http://www.linuxsecurity.com/resource files/intrusion detection/ DDOS–whitepaper.html

[12] Prolexic Company. Distributed Denial of Service Attack, http://www.eHow.com. (2012)

[13] J. Mirkovic and P. Reiher, A taxonomy of DDOS attack and DDOSdefence mechanisms, ACM SIGCOMM Computer Communications Review, vol.34, no. 2,pp. 39 (2004).

[14] V.O. Nwaocha and H.C. Inyiama. "Securing Enterprise Networks: A Multi-agent Based Distributed Intrusion Detection Approach". International Journal of Computational Intelligence and Information Security, Vol. 4, No. 6. (2013) ISSN: 1837-7823

[15] L. Zhou and Z. Haas, —Securing Ad hoc Networksll, IEEE Transaction on Networks, Vol. 13, no. 6, 1999, pp. 24-30.

[16] M. Wooldridge. An Introduction to Multi-agent Systems - Second Edition. John Wiley and Sons, 2009.

[17] U. Fayyad, G. Piatetsky-Shapiro, and P. Smyth. The KDD Process of Extracting Useful Knowledge from Volumes of Data. Communications of the ACM, 39(11):27–34, 1996.

[18] V.O. Nwaocha. "Mobile Learning: Potential Enabler of Open and Distance Learning in Sub-Saharan Africa". Book of Abstracts. 7th Pan-Commonwealth Forum on Open Learning (PCF7). (2013).

[19] R. Gopalakrishna and E.H. Spafford. A Framework for Distributed Intrusion Detection using Interest Driven Cooperating Agents. In Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection, Davis, CA, USA, 2001.

[20] V.O. Nwaocha and H.C. Inyiama. "Establishing an Effective Combat Strategy for Prevalent Cyber-Attacks". International Journal of Computer Science and Information Security,Vol. 9, No. 5, 2011

[21] J. P. Macker, V.D. Park, M.S. Corson, "Mobile and Wireless Internet Services: Putting the Pieces Together", to appear on Communication Magazine, June 2001

[22] S. Giordano. ' Mobile Ad-Hoc Networks'ISBN 0-471-XXXXX-X Copyright © 2000 Wiley[Imprint], Inc.

[23] B. Wu et al, —A Survey of Attacks and Preventionsin Mobile Ad Hoc Networks,‖ Wireless/MobileNetwork Security, Springer, Vol 17, 2006.

[24] S. Murthy and J.J. Garcia-Luna-Aceves, "An Efficient Routing Protocol for Wireless Networks", ACM Mobile Networks and App. J., Special Issue on Routing in Mobile

[25] S. Corson, et al. "An Internet MANET Encapsulation Protocol (IMEP) Specification", IETF internet draft, Aug. 1999.

[26] C.Siva Ram Nurthy and B.S. Manoj. "Ad hoc wireless networks Architectures and Protocols". Ie Prentice Hall, 2004.

[27] T. Clausen, P. Jacquet, and L. Viennot, "Comparative Study of Routing Protocols for Mobile Ad hoc Networks". Med-Hoc-Net'02, Sardegna, Italy, September 2002.

[28] Xiaoyan Hong; Kaixin Xu; Gerla, M. "Scalable routing protocols for mobile ad hoc networks". IEEE Network , Volume: 16 Issue: 4 , July-Aug. 2002, pp: 11 -21

[29] A. Iwata, C.-C. Chiang, G. Pei, M. Gerla, and T.-W. Chen, "Scalable Routing Strategies for Ad Hoc Wireless Networks". IEEE Journal on Selected Areas in Communications, Special Issue on Ad-Hoc Networks, Aug. 1999, pp.1369-79. Communication Networks, Oct. 1996, pp. 183-97.

[30] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad hoc Networks", IEEE Communication Societies (INFOCOM 2003), IEEE Press, pp. 1976-1986, 2003

[31] Amitabh Mishra, "Security and Quality of Service in Ad hoc Wireless Networks" ISBN- 13 978-0-521-87824-1 Handbook.

[32] T. White and B. Pagurek, "Towards multi-swarm problem solving in networks", Proc. Third International Conference on Multi-Agent Systems (ICMAS '98), pp. 333- 340.(1998)

[33] S. Toner, and D. O'Mahony, "Self-Organising Node Address Management in Ad hoc Networks". Personal Wireless Communications, IFIP-TC6 8th Int'l. Conf. (2003), pp. 476-483.

[34] Gagandeep, Aashima and P. Kumar. "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review". International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, (2012).

[35] P. Papadimitratos and J. Haas. Securing mobile ad hoc networks In Handbook of Ad Hoc Wireless Networks. CRC Press, pp 31. (2002).

[36] S. M. Specht and R.B, Lee, "Distributed Denial of Service: Taxonomies of Networks, Attacks, Tools, and Countermeasures," Princeton University Department of Electrical Engineering Technical Report CE-L2003-03, (2003)

[37] J.K. Houle. "Trends in Denial of Service Attack Technology". CERT Coordination Center, Carnegie Mellon Software Engineering Institute. (2001.)

[38] David Karig and Ruby Lee, "Remote Denial of Service Attacks and Countermeasures," Princeton University Department of Electrical Engineering Technical Report CEL. (2001).

[39] Y. Xiao, X. Shen and D, Du. " Wireless Network Security". Springer, Vol 1, 2007.

[40] W. Lou and Y. Fang, A Survey of Wireless Security in Mobile Ad Hoc Networks: Challenges and Available Solutions. Ad Hoc Wireless Networks, edited by Academic Publishers, pp. 319-364. (2003).

[41] M. Wooldridge.'An introduction to multi-agent systems". John Wiley and Sons; 2002.

[42] V.D. Gligor. "Security of emergent properties in ad-hoc networks. In: Proceedings of the international workshop on security protocols; 2004.

[43] Weiss G. Multi-agent systems: a modern approach to distributed artificial intelligence.. The MIT Press; (1999).

[46] C. Krügel and T. Toth, "A Survey on Intrusion Detec-tion Systems," TU Vienna, Austria, 2000.

[47] A. K. Jones and R. S. Sielken, "Computer System Intru-sion Detection: A Survey," University of Virginia, 1999.

[46] K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," NIST 800-94, Feb 2007.

[47] N. Deb, M. Chakraborty and N. Chaki. "The Evolution of IDS Solutions in Wireless Ad-hoc Networks to Wireless Mesh Networks". International Journal of Network Security and Its Applications (IJNSA), Vol.3, No.6, (2011)

[48] Marco Conti, Body, Personal and Local Ad Hoc Wireless Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 1), CRC Press LLC, 2003.

[49] P. Albers and O. Camp, "Security in ad hoc networks: A general intrusion detection architecture enhancing trust based approaches," in Proceedings of First International Workshop on Wireless Information Systems, pp. 1-12. (2002).

[50] C.C. Xenakis, C. Panos and I. Stavrakakis, " A comparative evaluation of intrusion detection architectures for mobile ad hoc networks". Computer. Security, 30: 63-80.(2011).

[51] G.A. Jacoby, and N.J. Davis, " Mobile host-based intrusion detection and attack identification. IEEE Wireless Commun., 14: 53-60. (2007).

[52] K. Nadkarni, and A. Mishra. "A novel intrusion detection approach for wireless ad hoc networks. Proceedings of the IEEE Wireless Communications and Networking Conference, Volume 2, March 21-25, 2004, Atlanta, Georgia, USA., pp: 831-836.(2004)

[53] A.P. Lauf, R.A. Peters and W.H. Robinson." A distributed intrusion detection system for resource-constrained devices in ad hoc networks. J. Ad Hoc Networks, 8: 253-266.(2010)

[54] Wang, W., H. Man and Y. Liu. "A framework for intrusion detection systems by social network analysis methods in ad hoc networks". Secure CommunicationNetworks, 2: 669-685. (2009).

[55] Bose, S. S. Bharathimurugan and A. Kannan, 2007. Multi-layer integrated anomaly intrusion detection system for mobile ad hoc networks. Proceedings of the International Conference on Signal Processing, Communications and Networking, February 22-24, Chennai, pp: 360-365. (2007).

[56] Razak, S.A., S.M. Furnell, N.L. Clarke and P.J. Brooke. "Friend-assisted intrusion detection and response mechanisms for mobile ad hoc networks". Ad Hoc Networks, 6: 1151-1167.2008).

[57] Ramachandran, C., S. Misra and M.S. Obaidat, 2008. FORK: A novel two-pronged strategy for an agent-based intrusion detection scheme in ad-hoc networks. Comput. Commun., 31: 3855-3869.

[58] Sun, B., K. Wu and U.W. Pooch, 2003. Routing anomaly detection in mobile adhoc networks. Proceedings of the 12th IEEE International Conference on Computer Communications and Networks, October 20-22, 2003, Santa Clara, CA., USA., pp: 25-31.

[59] Ma, C.X. and Z.M. Fang, 2008. A novel intrusion detection architecture based on adaptive selection event triggering for mobile ad-hoc networks. Proceedings of the IEEE 2nd International Symposium on Intelligent Information Technology and Security Informatics, January 23-25, 2008, Moscow, pp: 198-201.

[60] Otrok, H., N. Mohamm, L. Wang, M. Debbabi and P. Bhattacharya, 2008. A game-theoretic intrusion detection model for mobile ad hoc networks. Comput. Commun., 31: 708-721.

[61] Marchang, N. and R. Datta, 2008. Collaborative techniques for intrusion detection in mobile ad-hoc networks. Ad Hoc Networks, 6: 508-523.

[62] X. Yang, D. Wetherall, T. Anderson. TVA: A DOS-limiting network architecture. IEEE/ACM Trans Networking. 16(6):1267-1280. (2008)

[63] J. Mirkovic, A. Hussain, S. Fahmy, P. Reiher, R.K.Thomas.Accurately measuring denial of service in simulation and testbed experiments. IEEE Trans Dependable Secure Comput:2(3):216-232.(2009).

[64] H. Safa, M.Chouman,H. Artail and M.Karam A collaborative defense mechanism against SYN flooding attacks in IP networks. J Netw Comput Appl 31(4):509–534. (2008).

[65] B. Xiaoa, W. Chenb, Y. Hec. 'An autonomous defense against SYN flooding attacks: detect and throttle attacks at the victim side independently'. Journal of Parallel DistrubutedComputing.68:456–470. (2008).

[66] B. Xiaoa, W. Chenb, Y. Hec. 'An autonomous defense against SYN flooding attacks: detect and throttle attacksat the victim side independently'. Journal of Parallel Distrubuted Computing. 68:456–470. (2008).

[67] P.P.C. Lee, T. Bu and T. Woo. On the detection of signaling DOS attacks on 3G/Wimax wireless networks.Comput Netw 53(15):2601–2616. (2009)

[68] R. Swaminathan, M.Uysal, A. Nucci, E.Knightly. DDOS-Shield: DDOS-Resilient scheduling to counter application layer attacks. IEEE/ACM Trans Networking 17(1):26– 39. (2009)

[69] Geneiatakis D, Vrakas N, Lambrinoudakis C. ' Utilizing bloom filters for detecting flooding attacks against SIPbased services'. Journal of Computer Security 28(7):578–591. (2009)

[70]. Hwang, K., Dave, P., and Tanachaiwiwat, S. "Net Shield: Protocol anomaly detection with datamining against DDOS attacks". Proceedings of the 6th International Symposium on Recent Advances in Intrusion Detection, Pittsburgh, PA, 8-10 September, pp. 8–10. Springer-verlag. (2003)

[71] Z. Chen, Zand A. Delis,. "An inline detection and prevention framework for distributed denial of service attacks." Computer. Journal. 50, 7–40. (2007)

[72] K. Lee, J.Kim. K. Kwon,, Y. Han, and S.Kim,."DDOS attack detection method using cluster analysis. Expert Systems with Applications, "34, 1659–1665. (2008)

[73]. V. Sekar, N. Dueld, O. Spatscheck, J. Merwe, and H. Zhang,. "LADS: large-scale automated DDOS detection system." Proceedings of the annual conference on USENIX Annual Technical Conference, Boston, MA, 30 May-3 June, pp. 16– 29. USENIX Association. (2006)

[74]. H. Rahmani, N. Sahli, and Kammoun, F "Joint entropy analysis model for DDOS attack detection." Proceedings of the 5th International Conference on Information Assurance and Security - Volume 02, Xian, China, 18-20 August, pp. 267–271. IEEE CS. . (2009)

[75]. Y. Xiang, , K. Li, and Zhou, W. "Low- rate DDOS attacks detection and traceback by using new information metrics." IEEE Transactions on Information Forensics and Security, 6, 426–437. (2011)

[76]. C.E. Shannon, "A mathematical theory of communication." Bell system technical journal, 27, 397– 423. (1948).

[77]. J. Francois, I. Aib, and R. Boutaba,. "Fire Col: A collaborative protection network for the detection of flooding DDOS attacks." IEEE/ACM Transaction on Networking, 20, pages-1828–1841. (2012)

[78]. N. Jeyanthi, and N.C.S.N. Iyengar, "An entropy based approach to detect and distinguish DDOS attacks from flash crowds in VoIP networks." International Journal of Network Security, 14, 257– 269. (2012)

[79]. Li, M. and Li, M. "A new approach for detecting DDOS attacks based on wavelet analysis." Proceedings of the 2nd International Congress on Image and Signal Processing, Tianjin, China, 17-19 October, pp. 1–5. IEEE. (2009)

[80] R. Zhong, and G. Yue DDOS detection system based on data mining." Proceedings of the 2nd International Symposium on Networking and Network Security, Jinggangshan, China, 2-4 April, pp. 062–065. Academy Publisher. (2010).

[81]. R. Agrawal, and R. Srikant, "Fast algorithms for mining association rules in large databases." Proceedings of the 20th International Conference on Very Large Data Bases, Santiago de Chile, Chile, 12-15 September, pp. 487–499. Morgan Kaufmann. (1994).

[82] S. Stolfo, A.L. Prodromidis, S. Tselepis, W. Lee, D.W. Fan, and P.K. Chan. JAM: Java Agents for Meta-Learning over Distributed Databases. In Ptoceedings of the 3rd International Conference on Knowledge Discovery and Data Mining, Newport Beach, California, pages 74–81, 1997.

[83] G. Helmer, J.S.K. Wong, V.G. Honavar, and L. Miller. Automated Discovery of Concise Predictive Rules for Intrusion Detection. Journal of Systems and Software,60(3):165–175, 2002.

[84] C.L. Lui, T.C. Fu, and T.Y. Cheung. Agent-Based Network Intrusion Detection System Using Data Mining Approaches. In Proceedings of the 3rd International Conference on Information Technology and Applications, Sydney, Australia, pages 131–136, 2005.

[85] Y.F. Zhang, Z.Y. Xiong, and X.Q. Wang. Distributed Intrusion Detection Based on Clustering. In Proceedings of the Fourth International Conference on Machine Learning and Cybernetics, Guangzhou, pages 2379–2383, 2005.

[86] M. Reh´ak, M. Pechoucek, P. Celeda, J. Novotny, and P. Minarik. CAMNEP: Agent-Based Network Intrusion Detection System. In Proceedings of the 7th International Conference on Autonomous Agents and Multi-agent Systems, Estoril, Portugal, pages 133–136, 2008.

[87] E. J. Palomo, E. Dom´ınguez, R. M. Luque, and J. Mu noz. A Self-Organized Multi-agent System for Intrusion Detection. In Proceedings of the 4th International Workshop on Agents and Data Mining Interaction, Budapest, Hungary, pages 84–94, 2009.

[88] M.-L. Shyu and V. Sainani. A Multi-agent-based Intrusion Detection System with the Support of Multi-Class Supervised Classification. In Data Mining and Multi-agent Integration, pages 127–142. Springer-Verlag, 2009.

[89] E. Alpadin, " Introduction to Machine Learning". MIT Press.(2010).

[90] H.B. Debar,M.Siboni, "A neural network component for an intrusion detection system. Computer Society Symposium on Research in Security and Privacy. IEEE,Oakland,CA,pp.240–250. (1992).

[91] Z. Zhang, J. Li, C. Manikopoulos, J.Jorgenson, J.Ucles. "HIDE: a hierarchical network intrusion detection system using statistical preprocessing and neural network classification. In: Proceedings of the IEEE Workshop on Information Assurance and Security United States Military Academy.IEEE, WestPoint, NY, pp. 85–90.(2001).

[92] J.A. Renjit, K.L.Shunmuganathan, ".Multi-Agent-Based Anomaly Intrusion Detection. Inf.Secur.J.GlobalPerspect.20,185–193. (2011).

[93] E. Mosqueira-Rey, A. Alonso-Betanzos, B. DelRío, J.Piñeiro, " Amisuse Detection Agentfor Intrusion Detectionina Multi-agent Architecture,Agentand Multi-Agent Systems:Technologiesand Applications. LectureNotesin Computer Science.Springer,Berlin/Heidelbergpp.466–475.(2007).

[94] Dasgupta, D.,Gonzalez,F.,Yallapu,K.,Gomez,J.,Yarramsettii,R.CIDS:an agent-basedintrusiondetectionsystem.Comput.Secur.24,387–398. (2005)

[95] Vakili, G., Khorsandi, S. Coordination of cooperation policies in a peer-to-peer system using swarm-based RL. J. Network Computer Application. (2011).

[96] Fisch, Jänicke, M., Kalkowski, E., Sick, B., 2012. Learning from others: exchange of classification rules in intelligent distributed systems. Artif. Intell, http://dx.doi. org/10.1016/j.artint.2012.04.002.

[97] S. Stafrace, .K. N. Antonopoulos. 'Military tactics in agent-based sinkhole attack detection for wireless ad hoc networks'. Comput. Commun. 33, 619–638. (2010).

[98] S. A. Deloach, M.F. Wood and C. Sparkman. Multi-agent Systems Engineering International Journal of Software Engineering and Knowledge Engineering Vol. 11, No. 3 (2001)

[99] Yaba College of Technology. The Centre for Information Technology and Management (CTIM). Accessed January 2011. http://portal.yabatech.edu.ng/

[100] K. P. Bakwaph. "Admission Crisis In Nigerian Universities : The Challenges Youth And Parents Face In Seeking Admission"Seton Hall University Dissertations and Theses (ETDs). Paper 1908. (2013)

[101] A. Patcha and J.M. Park. An Overview of Anomaly Detection Techniques: Existing Solutions and Latest Technological Trends. Computer Networks, 51:3448–3470, 2007.

[102] IETF AAA Working Group, "Mobile IP AAA Requirements," IETF RFC2977. (2000).

[103] A. Dennis and B.H. Wixom. Systems Analysis and Design. An Applied Approach 11, No. 3. John Wiley and Sons. (2000)

[104] Sommerville, I. Software Engineering, Eighth edition. Addison-Wesley publishers. (2006).

[105] "SQLyog MySQL GUI 12.02 Released". Webyog. Retrieved 7 November 2014.

[106] D.W. Huang, P. Lin and C.H. Gan. "Design and performance study for a mobility management mechanism (WMN)using location cache for wireless mesh networks. IEEE Trans Mob Comput 7(5):546-556. 2008

[107] K. Hwang, M. Cai, Y. Chen, and M. Qin. " Hybrid Intrusion detection with weighted signature generation overanomalous internet episodes. IEEE Trans Dependable Secure Comput 4(1):41-55. 2007.

[108] A. Patel, M. Taghavi, K.Bakhtiyari, J. Celestino. An intrusion detection and prevention system in cloud computing:.Appl.36,25–41.(2013).

[109] F. Bellifemine, C. Giovanni, T. Tizian, "JADE Programmer's GUIDE, JADE 4.0". (TILAB, formerly CSELT) University of Parma. (2010).

[110] A. Doxtater, J.C. Foster, T. Kohlenberg and M. Rash. Snort 2.1 Intrusion Detection, Second Edition. Syngress Publishing Inc. pp. 6-11. (2004)

[111] G. Riley and T. Henderson, "The ns-3 network simulator," in Modeling and Tools for Network Simulation, Springer, Berlin, Germany, 2010.

[112] S. Pastrana, A. Mitrokotsa, A, Orfila and P.Peris-Lopez. "Evaluation of classification algorithms for intrusion detection in MANETs". Knowledge-based Systems. Elsevier Publishers. (2012).

[113] L. Portnoy, E. Eskin, and W. S. J. Stolfo. Intrusion Detection with Unlabeled Data using Clustering. In Proceedings of ACM CSS Workshop on Data Mining Applied to Security (DMSA-2001), Philadelphia, PA, 2001.