Digital Innovations & Contemporary Research in SCIENCE, ENGINEERING & TECHNOLOGY

Vol. 6. No. 4, Dec, 2018

Article Citation Format
Nwaocha, V.O. & Oloyede, A.O.(2018)
Towards the Development of a Multi-Agent Intrusion Detection System for Distributed Denial of Service Attacks.
Journal of Digital Innovations & Contemp Res. In Sc., Eng & Tech. Vol. 7, No. 3. Pp 115-120
Article DOI: dx.doi.org/10.22624/AIMS/DIGITAL/V4N4P10

Article Progress Time Stamps
Article Type: Research Article
Manuscript Received: 14th Oct, 2018
Review Type: Blind
Final Acceptance: 19th November, 2018
DOI Prefix: 10.22624

Towards the Development of a Multi-Agent Intrusion Detection System for Distributed Denial of Service Attacks

[1]Nwaocha, V.O. & [2]Oloyede A.O.
Department of Computer Science, National Open University of Nigeria, Abuja, FCT, Nigeria
[2]Department of Computer Sciences, Caleb University, Imota, Lagos State, Nigeria.
E-mail: ogochukwuvee@gmail.com; ayglo55@yahoo.com

ABSTRACT

The Mobile ad-hoc network (MANET) is a technology that is gaining popularity. This network actually has a great potential to be employed in the industry, academia and critical settings, yet its application has been hampered by one of the most pernicious cyber threats known as the distributed denial of service attack. Preventive techniques, such as encryption and authentication, devised for defending these networks are not sufficient. Although intrusion detection systems have been widely deployed in the MANET settings, yet they have not been quite effective due to a number of limitations such as low detection rate of false alarm and communication overhead. We set out a research agenda in this paper whose focus is on the design and implementation of an enhanced Multi-agent Intrusion Detection system for countering Distributed Denial of Service (DDoS) attacks in a mobile ad hoc network setting. Our intention is to harvest inputs that will enable us gravitate towards the realization of the research focus

Keywords: Development, Multi-Agent Intrusion Detection System, Distributed Denial of Service Attacks

1. INTRODUCTION

The proliferation of wireless mobile devices has revolutionized the world, leading to the popularity of the mobile ad hoc networking technology [I]. This emergence of the popularity 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 Smartphone, 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 [2]. A mobile ad hoc network (MANET) is simply described as an autonomous collection of wireless mobile devices that communicated and cooperate with each other in a distributed manner in order to provide the necessary network functionality in the absence of a fixed infrastructure [3]. It consists of a group of independent network mobile devices that are linked over various wireless links.

2. RESEARCH BACKGROUND & LITERATURE

Normally, mobile ad hoc networks operate on a constrained bandwidth, have dynamic network topologies and enable device to seamlessly link up without pre-existing communication infrastructure. Due to the ease and speed with which MANETs are established, they are widely used anytime and anywhere such as in shopping malls, mobile offices, cafes and school settings [4]. Wireless mobile ad hoc networks have been gainfully employed in University campuses, airports, hotels and conference settings because they fascinated collaboration and provide efficient communication. Consequently, the opportunities due to the application of MANETs are enormous. On the other hand, they have high risks and possibilities of attacks, therefore security issues impose various challenges to the application of mobile ad hoc networks. Besides, securing, this network has become even more intricate due to the fact that mobile devices constituting MANETs, have limited processing and memory resources [5]. The fact that MANETs do not have a clear entry point makes the implementation of perimeter-based defense mechanisms impractical.

Moreover, preventive solutions such as authentication and encryption developed for the protection of mobile ad-hoc network is the denial of service (DOS) attack. A denial of service attack is an explicit malicious attempt to render a service, system or network unusable by its legitimate user [7]. These attacks can lead to the clogging up of so much memory on the target system or causes the target system to reboot or even crash. When the traffic of a denial of service (DOS) attack emanates from multiple sources, it is referred to as a Distributed Denial of Service (DDOS) attack [8]. By using multiple attack sources, the power of a DDOS attack is amplified and the problem of defense is made more complex. The impact of DDOS attacks can vary from minor inconvenience to users of a web site to severe financial losses for institutions that rely on their online availability to carry out their businesses.

In contrast to other forms of intrusion, a denial of service attack does not require the attacker to gain physical access or entry into the targeted server, Typically, a DDOS attack is coordinated across many systems all controlled by a single attacker, commonly referred to as a 'master'. Prior to the attack, the master compromises a large number of hosts, without their owners' knowledge. And install software that will later enable the coordinated attack. These compromised hosts, called zombies, are then used to perform the actual attack [9]. Distributed denial of service attacks exhaust host resources; take up a lot of bandwidth, making the victim host unable to accept normal network requests, resulting in substantial economic losses. In a typical DDOS attack, a huge number of compromised hosts are amassed to send useless packets to the victim, which is deprived of gaining access to the internet or its resources. DDOS attacks affect the regular functioning of organizations causing huge losses worth billions of dollars. For this reason, organizations are trying their best to curtail such losses by countering DDOS attacks.

A denial-of-service (DOS) attack directed against one or more network resources often floods the target with an overwhelming number of synchronous (SYN), Internet Control Message Protocol (ICMP), or User Datagram Protocol (UDP) packets or with an overwhelming number of Syn fragments. Depending on the attackers' intent and the extent and success of previous intelligence gathering efforts, the attackers might single out a specific host, or might aim at random hosts across the targeted network, Either approach has the potential of upsetting the service to a single host or to the entire network, depending on how critical the role of the victim is to the rest of the network [10]. Surveys carried out by the world's largest DDOS mitigation service, known as the Prolexic Company, indicates that majority (90-94%) of DDOS attacks are performed using Transmission Control Protocol. In the first quarter (Q1) of 2012, attackers used more network layer attacks than application layer attacks (Layer 7).

The three most common forms of DDOS attacks are Transmission Control Protocol Synchronous (TCPSYN) floods, User Datagram Protocol (UDP) floods and Internet Control Message Protocol (ICMP) floods. Typical application layer attacks are GET Floods and POST Floods. According to the figures provided by Prolexic, 73.4% were infrastructure attacks and 26.6% were application layer attacks [11].The very first large-scale DDOS attack through the public Internet occurred in August 1999 on a network used by faculty and students at the University of Minnesota. This attack shut down the network for more than two days [12]. Currently, a good number of educational institutions who provide Internet access still experience frequent downtime due to DDOS attacks. Hence, the convenience of the Internet comes at the cost of the security risk. In other words, while the Internet has facilitated the provision of crucial services in educational and financial institutions, it has equally served as a means of diffusing network attacks. Consequently, most organizations and institutions have had to face the challenge of securing their networks from various forms of intrusions, while accommodating the influx of staff, students' and faculty devices [13].

In spite of the fact that several efforts have been made to design intrusion detection systems for MANETs, yet most of these approaches have neither been effective nor reliable and have been unable to adequately consider the requirements for a mobile ad hoc network. Thus, while many intrusion detection schemes exist, yet their effectiveness leaves much to be desired. Related works have revealed that conventional intrusion detection systems developed for wired networks are not well suited for MANETs and have a number of drawbacks [14]. These drawbacks include: High rates of false alarms, low detection rate and high communication overheads. Hence defending against DDOS attacks and protecting the access of legitimate user to networks has attracted attention from both the industry and the academia.

On the other hand, multi-agent systems [15] and data mining [16] have emerged as promising fields of research for developing distributed intrusion detection systems. Studies have shown that these technologies have the potential to improve the performance of intrusion detection systems and thus can be employed in the development of intrusion detection systems. In this ubiquitous, age where nearly everyone owns at least one mobile device [17]. The issue of protecting data stored and exchanged among these devices and through trendy services for use by countless mobile users has become critical. Based on the fact that these mobile devices are further expanding in their abilities to intercommunicate, simple static methods are no longer adequate in providing security to these computational scenarios.

3. STATEMENT OF THE PROBLEM

The distributed nature and the huge volume of distributed denial of service (DDOS) attacks make them quite difficult to detect, particularly in mobile ad hoc networks. At the Yaba College of Technology (YCT) network, DDOS attacks emanate from distributed sources and are difficult to deal with, since malicious traffic are not easily distinguished from legitimate traffic. Unfortunately, security mechanisms originally deployed for detecting attacks on the YCT network have been infective in detecting DDOS attacks. Besides, studies have shown that other more recent intrusion systems have low detection rates, have huge communication overheads and are not feasible for detecting DDOS attack and therefore obstructs legitimate user access to the network resources [19]. These drawbacks constitute the key issues which the proposed system was designed to resolve.

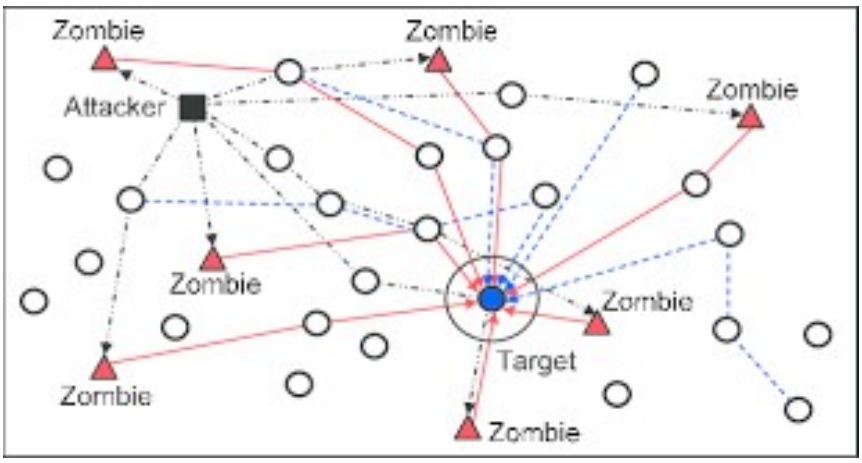

Fig. 1: DDOS Attack Scenarios

4. RESEARCH DIRECTION

Based on the foregoing, this paper presents the framework for the development of a distributed intrusion detection system that integrates the desirable features of the multi-agent methodology with data mining techniques in order to make the intrusion system more autonomous and efficient. In order to address the snags in existing intrusion detection systems, cooperative, distributed intrusion detection architecture that takes into account the unique features of MANET and facilitates accurate detection of distributed attacks was designed. Algorithms were adapted for averting Internet protocol (IP) Spoofing, as well as detecting 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 attacks on a mobile ad hoc network.

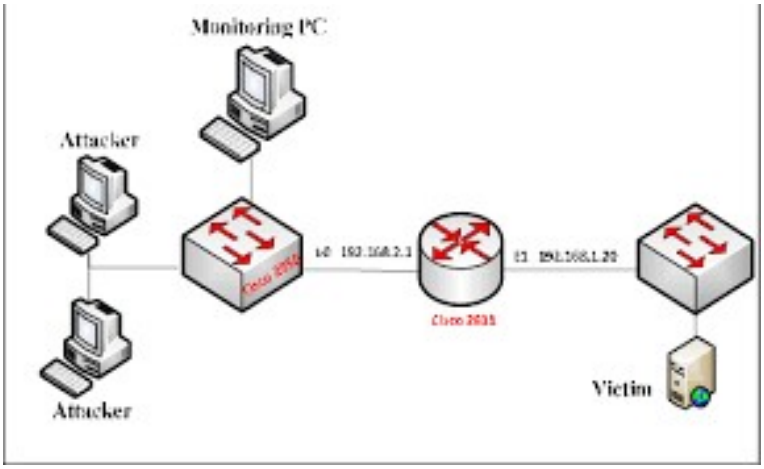

Fig. 2: TCP SYN Flood Scenario

The aim of this research is to develop a multi- agent intrusion detection system for countering distributed Daniel of services (DDOS) attacks in mobile ad-hoc networks. In order to attain this goal, the following objectives were set:

i. To design a distributed architecture that will cater for the resource-constrained features of the mobile ad hoc network;
ii. To present a multi-agent framework for intrusion detection of DDOS
iii. To adapt the cumulative sum (CUSUM) algorithm for averting Internet Protocol (IP) spoofing, as well as for detecting three prevalent forms of DDOS flooding attacks namely: Transmission Control Protocol Synchronize (TCP SYN) flood, User Datagram Protocol (UDP) flood and Internet Control Message Protocol (ICMP) flood attacks;
iv. To implement a prototype of the proposed system;
v. To evaluate the performance of the implemented system.

4.1 Proof of Concepts

As a proof of concept, TCPSYN, and UNP and ICMP flood attacks were launched into the newly developed system. The performance of the Multi-agent Intrusion Detection System was compared with the performance of four other agent-based intrusion detection systems. The results of the test clearly revealed that the Multi-agent Intrusion Detection System had very high attack detection accuracy for TCP SYN, UDP and ICMP flood attacks respectively. The false alarm rates and the communication overheads of the novel system were equally found to be considerably low when compared to the other four existing system.

5. RESEARCH SIGNIFICANCE

The effort to mitigate Distributed Denial of Service (DDOS) attacks is a crucial network security challenge. Hence, the outcome of this research will contribute significantly come up with more robust solution in highly dynamic environment such as mobile ad hoc network. Providing a distributed framework that would handle an efficient detection of DDOS attacks is imperative for curtailing the DDOS flooding attacks pose to organization and end user [20]. The outcome of this study will serve as a useful guide for Network Administrators and expedite the task of Internet Service Providers who will be better able to offer uninterrupted Internet service to subscribers. Currently various social service rely on the network applications and communications. These services include forecasting travel itineraries, reporting information about severe weather or potential disaster, electronic commerce, online medical diagnostics and scheduling emergency management events, etc.

6. CONCLUDING REMARKS

Any denial of service can cause enormous damage, not only loss of money but may also loss of human lives. Hence, in order to forestall undue losses in, institutions and private homes, it is desirable that businesses install the multi-agent intrusion detection system on their networks. Maintaining top level security is imperative for sustaining a trusted and safe setting necessary for information exchange amongst various originations. Thus, enterprises require an effective DDOS attack countering scheme that ensures continuous availability of their critical business resources. This is the thrust of this research.

REFERENCES

[1] Zhang, Y., Lee, W., & Huang, Y.(2003). Intrusion Detection Techniques for Mobile Wireless Networks. (pp. 3-4).
[2] Weiser, M. (1991). The Computer for the Twenty-First Century, Scientific American.
[3] Corson, M.S., Maker & Cernicione, J.H. (1999). Inter-based Mobile Ad Hoc Networking, IEEE Internet Computing. (pp. 63-70).
[4] Mishra, A., & Ketan, M. (2003). Security in Ad hoc Wireless Networks in the Handbook of Ad hoc Wireless Networks CRC Press LLC.
[5] Papadimitoas, P., & Zygmunt, J.H. (2003). Securing Mobile Ad Hoc Networks in the Proceedings of Ad Hoc Wireless Networks. CRC Press LLC.
[6] Naumann, I., Hogben, G., Fritsch, L., Benito, R., Dean, R. (2008). Security Issues in the Context of Authentication Using Mobile Devices (Mobile eID). European Network and Information Security Agency (ENISA).
[7] Gupta, P., & Kirkire, M. (2013). Intrusion Detection in Manet. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering.Vol. 2, Issue 4.
[8] Garber, L. (2000).Technology News: "Denial-of-Service Attacks Rip the Internet". Retrieved from: ftp://im1.im.tku.edu.tw/assistant/bearhero/00839316.pdf
[9] Incapsula (2013). DDOS Protection Services Distributed Denial of Service Attack (DDOS) http://www.incapsula.com/DDOS/DDOS-attacks/
[10] Puri, R. (2003). Bots and Botnet – an overview. Retrieved from: http://www.giac.org/practical/GSEC/Ramneek Puri GSEC.pdf
[11] Todd, B. (2000). Distributed Denial of Service Attacks. Retrieved from: http://www.linuxsecurity.com/resource files/intrusion detection/ DDOS–whitepaper.html
[12] Prolexic Company (2012). Distributed Denial of Service Attack. Retrieved from: http://www.eHow.com.
[13] J. Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDOS attack and DDOSdefence mechanisms, ACM SIGCOMM Computer Communications Review, vol.34, no. 2 (pp. 39).
[14] Nwaocha, V.O., & Inyiama, H.C. (2013). "Securing Enterprise Networks: A Multi-agent Based Distributed Intrusion Detection Approach". International Journal of Computational Intelligence and Information Security, Vol. 4, No. 6. ISSN: 1837-7823
[15] Zhou, L., & Haas, Z. (1999). Securing Ad hoc Networks, IEEE Transaction on Networks, Vol. 13, no. 6. (pp. 24-30).
[16] Wooldridge.M. (2009). An Introduction to Multi-agent Systems - Second Edition. John Wiley and Sons
[17] Fayyad, U., Piatetsky-Shapiro, G., & Smyth, P.(1996). The KDD Process of Extracting Useful Knowledge from Volumes of Data. Communications of the ACM, 39(11). (pp 27–34).
[18] Nwaocha, V.O.(2013). Mobile Learning: Potential Enabler of Open and Distance Learning in Sub-Saharan Africa". 7th Pan-Commonwealth Forum on Open Learning (PCF7).
[19] R. Gopalakrishna, R., & Spafford, E.H.(2001). 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.
[20] Nwaocha, V.O., & Inyiama, H.C. (2011). Establishing an Effective Combat Strategy for Prevalent Cyber-Attacks". International Journal of Computer Science and Information Security,Vol. 9, No. 5.