ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 5, Issue 3, pp: (1-5), Month: July - September 2017, Available at: www.researchpublish.com

Packet Filtering Method for DDoS Attack Detection Based on Traffic Analysis

R.Sindhu Nayaki[1], A.Senthil Kumar[2]

[1]Research Scholar, [2]Asst.Professor, Dept.of Computer Science, Tamil University, Thanjavur, Tamilnadu, India

Abstract: **Denial-of-Service (DoS) and Distributed Denial-of Service (DDoS) attacks account for one third of all service downtime incidents. Current DoS/DDoS attacks are not only limited to knocking down online services, but they also disguise other malicious attacks such as delivering malware, data-theft, wire fraud and even extortion. Detection of these attacks is predominantly based on the packet data and metrics derived only from packets. This work proposes a host based DDoS detection framework called BRAIN: Behavior based Adaptive Intrusion detection in Networks. BRAIN leverages already available Hardware Performance Counters in modern processors to model the application behavior using low-level hardware events. BRAIN combines network statistics and modelled application behavior to detect DDoS attacks using machine learning. Our experiments show that BRAIN can detect multiple types of DDoS attacks, including those are undetectable by existing tools with an accuracy of 99.8% and a false alarm rate of 0%.**

Keywords: **Wireless mobile ad-hoc network, security goal, security attacks, defensive mechanisms, challenges, DDoS attack.**

1. INTRODUCTION

Mobile ad hoc network (MANET) is a group of two or more devices or nodes or terminals with a capability of wireless communications and networking which makes them able to communicate with each other without the aid of any centralized system. This is an autonomous system in which nodes are connected by wireless links and send data to each other. As we know that there is no any centralized system so routing is done by node itself. Due to its mobility and self routing capability nature, there are many weaknesses in its security. To solve the security issues we need an Intrusion detection system, which can be categorized into two models: Signature-based intrusion detection [1] and anomaly-based intrusion detection. In Signature-based intrusion detection there are some previously detected patron or signature are stored into the data base of the IDS if any disturbance is found in the network by IDS it matches it with the previously saved signature and if it is matched than IDS found attack. But if there is an attack and its signature is not in IDS database then IDS cannot be able to detect attack. For this periodically updating of database is compulsory. To solve this problem anomaly based IDS[2] is invented, in which firstly the IDS makes the normal profile of the network and put this normal profile as a base profile compare it with the monitored network profile. The benefit of this IDS technique is that it can be able to detect attack without prior knowledge of attack. Intrusion attack is very easy in wireless network as compare to wired network. One of the serious attacks to be considered in ad hoc network is DDoS attack. A DDoS attack is a large scale, coordinated attack on the availability of services at a victim system or network resource. The DDoS attack is launched by sending huge amount of packets to the target node through the co-ordination of large amount of hosts which are distributed all over in the network. At the victim side this large traffic consumes the bandwidth and not allows any other important packet reached to the victim.

2. RELATED WORK

The new DOS attack, called Ad Hoc Flooding Attack(AHFA), can result in denial of service when used against on-demand routing protocols for mobile ad hoc networks, such as AODV & DSR. Wei-Shen Lai et al [3] have proposed a scheme to monitor the traffic pattern in order to alleviate distributed denial of service attacks. Shabana Mehfuz1 et al [4] have proposed a new secure power-aware ant routing algorithm (SPA-ARA) for mobile ad hoc networks that is inspired from ant colony optimization (ACO) algorithms such as swarm intelligent technique. Giriraj Chauhan and Sukumar Nandi [5] proposed a QoS aware on demand routing protocol that uses signal stability as the routing criteria along with other QoS metrics. Xiapu Luo et al [6] have presented the important problem of detecting pulsing denial of service (PDoS) attacks which send a sequence of attack pulses to reduce TCP throughput. Xiaoxin Wu et al [7] proposed a DoS mitigation technique that uses digital signatures to verify legitimate packets, and drop packets that do not pass the verification Ping. S.A.Arunmozhi and Y.Venkataramani [8] proposed a defence scheme for DDoS attack in which they use MAC layer information like frequency of RTD/CTS packet, sensing a busy channel and number of RTS/DATA retransmission. Jae-Hyun Jun, Hyunju Oh, and Sung-Ho Kim [9] proposed DDoS flooding attack detection through a step-by-step investigation scheme in which they use entropy-based detection mechanism against DDoS attacks in order to guarantee the transmission of normal traffic and prevent the flood of abnormal traffic. Qi Chen, Wenmin Lin, Wanchun Dou, Shui Yu [10] proposed a Confidence-Based Filtering method (CBF) to detect DDoS attack in cloud computing environment. In which anomaly detection is used and normal profile of network is formed at non attack period and CBF is used to detect the attacker at attack period.

3. ATTACK ON AD HOC NETWORK

There are various types of attacks on ad hoc network which are describing following: 3.1 Wormhole The wormhole attack is one of the most powerful presented here since it involves the cooperation between two malicious nodes that participate in the network [11]. One attacker, e.g. node A, captures routing traffic at one point of the network and tunnels them to another point in the network, to node B, for example, that shares a private communication link with A. Node B then selectively injects tunnelled traffic back into the network. The connectivity of the nodes that have established routes over the wormhole link is completely under the control of the two colluding attackers. The solution to the wormhole attack is packet leashes. 3.2 Blackmail This attack is relevant against routing protocols that use mechanisms for the identification of malicious nodes and propagate messages that try to blacklist the offender [12]. An attacker may fabricate such reporting messages and try to isolate legitimate nodes from the network. The security property of non-repudiation can prove to be useful in such cases since it binds a node to the messages it generated [13]. 3.3 Routing Table Poisoning Routing protocols maintain tables that hold information regarding routes of the network.

In poisoning attacks the malicious nodes generate and send fabricated signaling traffic, or modify legitimate messages from other nodes, in order to create false entries in the tables of the participating nodes [14]. For example, an attacker can send routing updates that do not correspond to actual changes in the topology of the ad hoc network. Routing table poisoning attacks can result in the selection of non optimal routes, the creation of routing loops, bottlenecks, and even portioning certain parts of the network. 3.4 Replay A replay attack is performed when attacker listening the conversation or transaction between two nodes and put important massage like password or authentication message from conversation and use this in future to make attack on the legitimate user pretending as real sender. 3.5 Location Disclosure Location disclosures is an attack that targets the privacy requirements of an ad hoc network. Through the use of traffic analysis techniques [15] or with simpler probing and monitoring approaches, an attacker is able to discover the location of a node, or even the structure of the entire network. 3.6 Black Hole In a black hole attack a malicious node injects false route replies to the route requests it receives, advertising itself as having the shortest path to a destination [16]. These fake replies can be fabricated to divert network traffic through the malicious node for eavesdropping, or simply to attract all traffic to it in order to perform a denial of service attack by dropping the received packets. 3.7 Denial of Service Denial of service attacks aim at the complete disruption of the routing function and therefore the entire operation of the ad hoc network [14]. Specific instances of denial of service attacks include the routing table overflow and the sleep deprivation torture. In a routing table overflow attack the malicious node floods the network with bogus route creation packets in order to consume the resources of the participating nodes and disrupt the establishment of legitimate routes.

The sleep deprivation torture attack aims at the consumption of batteries of a specific node by constantly keeping it engaged in routing decisions. 3.8 Distributed Denial of Service A DDoS attack is a form of DoS attack but difference is that DoS attack is performed by only one node and DDoS is performed by the combination of many nodes. All nodes simultaneously attack on the victim node or network by sending them huge packets, this will totally consume the victim bandwidth and this will not allow victim to receive the important data from the network. 3.9 Rushing Attack Rushing attack is that results in denial-of-service when used against all previous on-demand ad hoc network routing protocols [17]. For example, DSR, AODV, and secure protocols based on them, such as Ariadne, ARAN, and SAODV, are unable to discover routes longer than two hops when subject to this attack. develop Rushing Attack Prevention (RAP), a generic defence against the rushing attack for on-demand protocols that can be applied to any existing on-demand routing protocol to allow that protocol to resist the rushing attack. 3.10 Masquerade It is an intruder who gain the privilege of any one system as an authenticate user by stolen user password, through finding security gaps in programs, or through bypassing the authentication mechanism. 3.11 Passive Listening and traffic analysis The intruder could passively gather exposed routing information. Such an attack cannot effect the operation of routing protocol, but it is a breach of user trust to routing the protocol. Thus, sensitive routing information should be protected. However, the confidentiality of user data is not the responsibility of routing protocol.

EXISTING SYSTEM:

Most host-based DDoS detection mechanisms employ rate based filtering approaches, which set a threshold for a certain network parameter to detect and mitigate DDoS attacks. The threshold used in most of these mechanisms is a static number predefined by the user. This makes the detection vulnerable to threshold learning attacks; an attacker can learn the threshold and craft the DDoS attack to send malicious traffic with a rate below the threshold. Hence, these attacks can persistently affect the victim for several days and evade detection.

PROPOSED SYSTEM:

BRAINs attack detection is based on the characterization of hardware and the application. The fundamental concept behind the design of BRAIN is that the host hardware will behave differently during an attack on the application and during normal operation. To accurately differentiate the host hardware behaviour during load and attack, we need to correlate HPC statistics with network and application statistics. The set of features involved in DDoS detection will include statistics from three categories-

Hardware Statistics: HPCs are a set of special-purpose registers built into a modern microprocessor’s performance monitoring unit to store the counts of hardware-related activities. HPC values from different hardware events are used to characterize the host behaviour.

Network Statistics: Network parameters like number of concurrent active connections and unique users that affect the HPC values.

Application Statistics: Parameters like number of unique users concurrently accessing the application to determine the load on the application.

4. PROBLEM STATEMENT DDOS

Attack is the main problem in all ad hoc scenario i.e. in MANAT and as well as in wireless sensor networks. In the Paper with reference no. [18] Has an intrusion detection system in wireless sensor network which uses the anomaly intrusion detection system in which IDS uses two intrusion detection parameters, packet reception rate (PRR) and inter arrival time (IAT). But only these two parameters are not completely sufficient for intrusion detection in wireless sensor network and as well as in MANET. If we also add other parameters into it to make it works more accurately. So in our proposal we use different intrusion detection parameters in mobile Ad hoc networks. We assume that a mobile ad hoc network contains two or more than two mobile devices that are communicate from each other through intermediate nodes, each node contain routing table , in our proposal we use AODV routing protocol in all normal module attack module and IDS (intrusion detection system) for prevention through attack. In this paper we simulate the three different condition results normal time, Attack time and IDS.

5. CONCLUSION

The proposed mechanism eliminates the need for a centralized trusted authority which is not practical in ADHOC network due to their self organizing nature. The results demonstrate that the presence of a DDOS increases the packet loss in the network considerably. The proposed mechanism protects the network through a self organized, fully distributed and localized procedure. The additional certificate publishing happens only for a short duration of time during which almost all nodes in the network get certified by their neighbours. After a period of time each node has a directory of certificates and hence the routing load incurred in this process is reasonable with a good network performance in terms of security as compare with attack case. We believe that this is an acceptable performance, given that the attack prevented has a much larger impact on the performance of the protocol. The proposed mechanism can also be applied for securing the network from other routing attacks by changing the security parameters in accordance with the nature of the attacks.

REFERENCES

[1] F. Anjum, D. Subhadrabandhu and S. Sarkar. Signature based intrusion detection for wireless Ad-hoc networks," Proceedings of Vehicular Technology Conference, vol. 3, pp. 2152-2156, USA, Oct. 2003.

[2] D. E. Denning, An Intrusion Detection Model," IEEE Transactions in Software Engineering, vol. 13, no. 2, pp. 222-232, USA, 1987.

[3] Wei-Shen Lai, Chu-Hsing Lin , Jung-Chun Liu , HsunChi Huang, Tsung-Che Yang: Using Adaptive Bandwidth Allocation Approach to Defend DDoS Attacks, International Journal of Software Engineering and Its Applications, Vol. 2, No. 4, pp. 61-72 (2008)

[4] ShabanaMehfuz, Doja,M.N.: Swarm Intelligent PowerAware Detection of Unauthorized and Compromised Nodes in MANETs”, Journal of Artificial Evolution and Applications (2008).

[5] Giriraj Chauhan,Sukumar Nandi: QoS Aware Stable path Routing (QASR) Protocol for MANETs, in First International Conference on Emerging Trends in Engineering and Technology,pp. 202-207 (2008).

[6] Xiapu Luo, Edmond W.W.Chan,Rocky K.C.Chang: Detecting Pulsing Denial-of-Service Attacks with Nondeterministic Attack Intervals, EURASIP Journal on Advances in Signal Processing (2009).

[7] Xiaoxin Wu, David,K.Y.Yau, Mitigating Denial-ofService Attacks in MANET by Distributed Packet Filtering: A Game theoretic Approach, in Proceedings of the 2nd ACM symposium on Information, computer and communication security, pp 365-367 (2006)

[8] S.A.Arunmozhi, Y.Venkataramani “DDoS Attack and Defense Scheme in Wireless Ad hoc Networks” International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May 2011, DOI: 10.5121/ijnsa.2011.3312.

[9] Jae-Hyun Jun, Hyunju Oh, and Sung-Ho Kim “DDoS flooding attack detection through a step-by-step investigation” 2011 IEEE 2nd International Conference on Networked Embedded Systems for Enterprise Applications, ISBN: 978-1-4673-0495-5,2011.

[10] Qi Chen , Wenmin Lin , Wanchun Dou , Shui Yu ” CBF: A Packet Filtering Method for DDoS Attack Defence in Cloud Environment”, 2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing. ISBN: 978-0-7695-4612-4.2011

[11] Yih-Chun Hu, Adrian Perrig, and David B. Johnson., “Packet Leashes A Defense against Wormhole Attacks in Wireless Ad Hoc Networks” In Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003), April 2003

[12] Patroklos g. Argyroudis and donal o’mahony, “Secure Routingfor Mobile Ad hoc Networks”, IEEE Communications Surveys & Tutorials Third Quarter 2005.

[13] Karan Singh, R. S. Yadav, Ranvijay International Journal of Computer Science and Security, Volume (1): Issue (1) 56

[14] I. Aad, J.-P. Hubaux, and E-W. Knightly, "Denial of ServiceResilience in Ad Hoc Networks," Proc. MobiCom, 2004.

[15] K. Balakrishnan, J. Deng, and P.K. Varshney, "TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks" Proc. IEEE Wireless Comm. and Networking Conf. (WCNC '05), Mar. 2005.

[16] Mohammad Al-Shurman and Seong-Moo Yoo, Seungjin Park, "Black Hole Attack in Mobile Ad Hoc Networks" ACMSE'04, April 2-3, 2004, Huntsville, AL, USA.

[17] Yih-Chun Hu, Adrian Perrig, David B. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols" WiSe 2003, September 19, 2003, San Diego, California, USA.

[18] Ponomarchuk, Yulia and Seo, Dae-Wha, "Intrusion Detection Based On Traffic Analysis in Wireless Sensor Networks" IEEE 2010.

[19] Network Simulator- ns-2. http://www.isi.edu/ nsnam /ns/. [20] Yang, H., Luo, H., Ye, F., Lu, S., & Zhang, L. (2004), Security in mobile ad hoc networks: Challenges and solutions, IEEE Wireless Communications, 11(1), 38-47.