A REVIEW OF DENIAL OF SERVICE (DOS) ATTACKS IN WIRELESS AD HOC NETWORKS AND ITS COUNTERMEASURES

[1]LOKHANDE S.N., [2]DR. KHAMITKAR S.D. ,[1]MEKEWAD S.R.

[1] Assistant Prof, School of Computational Sciences,SRTM University, Nanded (MS) India
[2] Associate Prof, School of Computational Sciences,SRTM University, Nanded (MS)India

lokhande_sana@rediffmail.com

ABSTRACT *:In this paper we describes what is Denial of Service (DoS) attacks , how they can be carried out in wireless Ad Hoc networks, and existing defenses against them. Completely reliable protection against DoS attacks is, however, not possible. There will always be vulnerable hosts in the network, and many attack mechanisms are based on ordinary use of protocols. Defense in depth is thus needed for mitigation or prevention of the DoS attacks. This paper describes briefly some defense mechanisms currently available or proposed to defend against DoS attacks in wireless ad hoc network. We also describe limitations of existing IDS/IPS to detect and prevention of these attacks in wireless ad hoc networks. The aim is to make aware of DoS attacks in ad hoc network and implement possible defenses*

KEYWORDS : DoS, DDoS, Ad hoc networks, IDS, Security,

1. INTRODUCTION

An ad hoc network is a collection of wireless mobile nodes dynamically forming a temporary network without the use of any existing infrastructure or centralized administration. Due to the resource constraints, dynamic network topology, open network architecture, and shared transmission media wireless network are prone to different types of attacks. If the complexity of a system is high, then there are more possibilities to be exploited for attack purposes. Due to limited processing power, transmission bandwidth, and lifetime of batteries there is a restriction on handling the attacks in such networks. Dynamic network topology places a burden on routing protocols when trying to achieve short reaction and convergence times. Open network architecture and shared transmission media make it possible to join a network without a physical connection. Any of these vulnerabilities can be exploited in a Denial of Service (DoS) attack to prevent or delay legitimate access to services [1]. Security is an important issue for any network, the main network security attributes are availability, confidentiality, integrity, authentication, and non-repudiation [1].

In this paper we focus on DoS attacks in wireless Ad Hoc networks. Different types of DoS attacks in wireless Ad Hoc network, impact of DoS attacks on the performance of Ad Hoc networks and the existing countermeasures.

2. DOS ATTACK AND ITS EFFECTS

A Denial of Service (DoS) attack is one that attempts to prevent the victim from being able to use all or part of his/her network connection or resources. DOS attacks attempt show several characteristics:

- Restrain legitimate network traffic by flooding the network with useless traffic.
- Deny access to a service by disrupting connections between two wireless nodes.
- Blocking the access of a particular individual to available services.
- Disrupting the specific system or service in the network.
- DOS attacks targets bandwidth, energy resource, storage space and processing power of resources.

In comparison with wired networks, DoS attacks in wireless Ad Hoc Network may not only bring damage to the victim node, but may also degrade the performance of the whole network because nodes have limited battery power and the network can easily be congested due to the limited bandwidth available as compared to wired networks.

3. DOS ATTACK SCENARIOS

The DoS attacks that target resources can be grouped into three broad scenarios [2]. The first attack scenario targets Storage and Processing Resources. This is an attack that mainly targets the memory, storage space, or CPU of the service provider. For example if a node continuously sends an executable flooding packet to its neighbor nodes and to overload the storage space and deplete the memory of that node. This prevents the node from sending or receiving packets from other legitimate nodes.

The second attack scenario targets energy resources, specifically the battery power of the service provider.

Since wireless nodes operate by battery power, energy is an important resource in wireless ad hoc networks. A malicious node may continuously send a bogus packet to a node with the intention of consuming the nodes battery energy and preventing other nodes from communicating with the node.

The third attack scenario targets bandwidth. Consider the case where an attacker located between multiple communicating nodes wants to waste the network bandwidth and disrupt connectivity. The malicious node can continuously send packets with bogus source IP addresses of other nodes, thereby overloading the network. This consumes the resources of all neighbors that communicate, overloads the network, and results in performance degradations.

4. EXISTING DEFENSE FOR DOS IN WIRELESS AD HOC NETWORK

Intrusion detection can be classified based on audit data as either host based or network based. A network-based IDS captures and analyzes packets from network traffic while a host-based IDS uses operating system or application logs in its analysis. Based on detection techniques, IDS can also be classified into three categories as [3].Anomaly detection systems, Misuse detection systems and Specification based detection systems.

In ad hoc networks, a mobile node or host may depend on other node(s) to route or forward a packet to its destination [4]. The security of these nodes could be compromised by an external attacker or due to the selfish nature of other nodes. This would create a severe threat of Denial of Service (DoS) and routing attacks where malicious nodes combine and deny the services to legitimate nodes. In this section we briefly describes the existing defense mechanisms used against DoS attacks in wireless ad hoc networks. Capkun et al have developed some solutions using a concept that they introduce, called Maximum Degree Algorithm (MDA), for preventing denial of service (DoS) due to poor key management. Avoine et al [5] have developed a cryptography-based fair key exchange model called Guardian Angel. This model uses a probabilistic approach without involving a trusted third party in key exchange. Techniques for Intrusion Resistant Ad Hoc Routing Algorithms (TIARA) was proposed by Ramanujam et al to detect and eliminate DoS [6].This model presents a new approach for building intrusion resistant ad hoc networks in the wake of DoS attacks using wireless router extensions. This approach relies on extending the capabilities of existing ad hoc routing algorithms to handle intruders without modifying the existing routing algorithms. This scheme proposes a new network layer mechanism for detecting and recovering from intruder induced malicious faults that work in concert with existing ad hoc routing algorithms and augment their capabilities. Hu et al [7] have developed a DSDV based secure routing method called SEAD (Secure Efficient Ad hoc Distance vector). This method uses efficient one-way hash functions and does not use symmetric cryptographic operations in the protocol in order to support the nodes of limited CPU processing capability and to guard against Denial of Service (DoS) attacks. The primary reason for this is due to the fact that the nodes in an wireless ad hoc network are unable to verify asymmetric signatures quickly enough for routing protocols to decide on the routing path.

Another preventive solution for DoS attacks in wireless ad hoc networks is proposed by Luo et al [8].In this solution they distribute the functionality of authentication servers, thus enabling each node in the network to collaboratively self-secure themselves. This is achieved by using the certificate-based approach. This scheme supports ubiquitous security for wireless mobile nodes, scales to network size, and is robust against adversary break ins. In this method centralized management is minimized and the nodes in the network collaboratively self-secure themselves. This scheme proposes a suite of fully distributed and localized protocols that facilitate practical deployment. It also features communication efficiency to conserve the wireless channel bandwidth and in dependency from both the underlying transport layer protocols and the network layer routing protocols.

Watchdog and Pathrater these two techniques were proposed by Marti, Giuli, and Baker [9] Watchdog and Pathrater, to be added on top of the standard routing protocol in wireless ad hoc networks. The standard is Dynamic Source Routing protocol (DSR). A Watchdog identifies the misbehaving nodes by eavesdropping on the transmission of the next hop. A Pathrater then helps to find the routes that do not contain those nodes. In DSR, the routing information is defined at the source node. This routing information is passed together with the message through intermediate nodes until it reaches the destination. Therefore, each intermediate node in the path should know who the next hop node is. In addition, listening to the next hop's transmission is possible because of the characteristic of wireless networks if node A is within range of node B, A can overhear communication to and from B.

The Watchdog and Pathrater model assumes that there are no priori trust relationships. Performance of model is bound to suffer when trusted node lists in ad hoc networks are also taken into account. Also, in this model, all the simulations are based on Constant Bit Rate (CBR) data with no reliability requirements. The analysis should be extended to explain how the routing extensions perform with TCP flows common to network applications [9].

Buchegger and LeBoudec[10] proposed an extension to DSR protocol called CONFIDANT (Cooperation Of Nodes, Fairness In Dynamic Ad-hoc NeTworks), which is similar to Watchdog and Pathrater. Each node observes the behaviors of neighbor nodes within

its radio range and learns from them. This system also solves the problem of Watchdog and Pathrater such that misbehavior nodes are punished by not including them in routing and not helping them on forwarding packets. Moreover, when a node experiences a misbehaving node, it will send a warning message to other nodes in the network, defined as friends, which is based on trusted relationship.

CORE,Michiardi and Molva [11] presented a technique to detect a specific type of misbehaving nodes, which are selfish nodes, and also force them to cooperate. This technique is based on a monitoring system and a reputation system, which includes both direct and indirect reputation from the system. In another word, CORE prevents false accusation, thus, it also prevents a Denial of Service (DoS) attack, which cannot be done in CONFIDANT. The negative rating is given to a node only from the direct observation when the node does not cooperate, which results in the decreased reputation for that node. The positive rating, in contrast, is given from both direct observation and positive reports from other nodes, which results in the increased reputation. CORE can then be said to have two components, the watchdog system and the reputation system. The watchdog modules, one for each function, work the same way as in the previous two schemes above. For the reputation system, it maintains several reputation tables, one for each function and one for accumulated values for each node. Therefore, if there is a request from a bad reputation node, the node will be rejected and not be able to use the network.

A cluster-based cooperative intrusion detection system has been presented by Huang and Lee [12].In this approach, IDS is not only able to detect an intrusion, but also to identify the attack type and the attacker, whenever possible, through statistical anomaly detection. Various types of statistics or features, which are proposed in their previous work, are evaluated from a sampling period by capturing the basic view of network topology and routing operations, as well as traffic patterns and statistics, in the normal traffic. Hence, attacks could be identified if the statistics deviate from the precomputed values.

Xiapu Luo et al [16] have presented the important problem of detecting Pulsing Denial of Service (PDoS) attacks which send a sequence of attack pulses to reduce TCP throughput. Wei-Shen Lai et al [17] have proposed a scheme to monitor the traffic pattern in order to alleviate distributed denial of service attacks. Shabana Mehfuz1 et al [18] 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. Xiaoxin Wu et al [19] proposed a DoS mitigation technique that uses digital signatures to verify legitimate packets, and drop packets that do not pass the verification.Ping Yi, Zhoulin Dai,Shiyong Zhang and Yiping Zhong [20] have presented a new DoS attack and its defense in wireless ad hoc networks. 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. John Haggerty, Qi Shi and Madjid Merabti [21] have proposed a new approach that utilizes statistical signatures at the router to provide early detection of flooding Denial of Service attacks. Wei Ren, Dit-Yan Yeung, Hai Jin, Mei Yang [22] have proposed a defense scheme that includes both the detection and response mechanisms. In this paper the detection scheme that monitors MAC layer signals and a response scheme based on Explicit Congestion Notification (ECN) marking are discussed. But, the method of monitoring the sending rates of the nodes is not discussed. Hence identifying the attacking nodes becomes a problem. It may also result in increase of false positives and false negatives. Giriraj Chauhan and Sukumar Nandi[23] proposed a QoS model. There are three steps in handling a malicious node. First step identify that a node is mishandling the packets intentionally. Second, the identity of the malicious node must be determined. The third step is to isolate the malicious node from the network or cope with the issue.

5. LIMITATIONS OF EXISTING SOLUTIONS:

In this section we briefly elaborate the limitations of some existing countermeasures which are specified for prevention of DoS attacks in wireless ad hoc networks. The Guardian Angel model is not a comprehensive security scheme and does not take into account the attacks like packet forwarding and denial of service or routing attacks [5].

The SEAD approach does not incorporate mechanisms to detect and expose nodes that advertise routes but do not forward packets [7].In the Beacon scheme, scalability is an issue if there are large numbers of nodes compared to the available bandwidth. The proposed model assumes all nodes in a network share a symmetric key used only for beacon authentication. In addition to problems with scalability, every agent and mobile node at the site has to know the network authentication key. The Watchdog and Pathrater model assumes that there are no apriority trust relationships. Performance of model is bound to suffer when trusted node lists in ad hoc networks are also taken into account. Also, in this model, all the simulations are based on Constant Bit Rate (CBR) data with no reliability requirements. The analysis should be extended to explain how the routing extensions perform with TCP flows common to network applications [9]. The CONFIDANT protocol assumes that nodes are authenticated and that no node can pretend to be another in order to get rid of a bad reputation [10].The scheme CORE considers only attacks from selfish nodes but not from active intruders. Hence the scheme needs to be extended and tested for intruder attacks as well. Also

there is no definition of formal method to analytically prove robustness of CORE[11] .The solution for attack by selfish nodes, presented in Nuglets model is focused just on packet forwarding attacks. This model also does not address application level issues like mutual provision of information services in an ad hoc network.

Since the ARIADNE model does not possess the optimizations of DSR, the resulting protocol is less efficient than the highly optimized version of DSR that runs in a trusted environment [13] .An important aspect of OSRP scheme is that the algorithm can be used to detect a fault. However, it is difficult to design such a scheme that is resistant to a large number of adversaries. The method suggested in this paper uses a fixed threshold scheme. This scheme does not explore other methods, such as adaptive threshold or probabilistic schemes which may provide superior performance and extensibility. Also this scheme does not provide means of protecting routing against traditional denial of service attacks [14] .

6. CONCLUSION

In this survey paper, we try to scrutinize the security issues in the wireless ad hoc networks. Due to the mobility and open media nature, the wireless ad hoc networks are much more prone denial of service. As a result, the security needs in the wireless ad hoc networks are much higher than those in the wired networks.

It has been observed that the existing IDS/IPS performs poorly in detection as well as the false positive rate is higher. It has recently been observed that Denial of Service (DoS) attacks are targeted even against the IDS. Thus, IDS themselves needs to be protected. IDS should also be able to distinguish an attack from an internal system fault.

The identification of intruder and appropriate response techniques to protect Wireless Ad Hoc Network from DoS attacks is still a challenging issue. The need to coordinate intrusion detection and response techniques and the need to respond and control the identified attacks effectively, require further research.

7. REFERENCES:

1. Safdar Ali Soomro et l “Denial of Service Attacks in Wireless Ad hoc Networks” Journal of Information & Communication Technology Vol. 4, No. 2, 2010.

2.Mieso K. Denko “ Detection and Prevention of Denial of Service Attacks in Mobile Ad Hoc Networks using reputation based Incentive Scheme“ Systematics ,Cybernetics and Information ,vol.3,No.4

3. A. Mishre, K. Nadkarni and A. Patcha , “Intrusion Detection in wsireless Ad Hoc Networks”, IEEE Wireless Communications, Vol. 11, Issue 1, PP. 48-60 , Feb. 2004.

4. S.P. Alampalayam, A. Kumar and S. Srinivasan “ Mobile Ad Hoc Networks security- A taxonomy” in proceedings of ICACT conference, 2005,

5. G. Avoine and S. Vaudenay, “Cryptography with guardian angels: Bringing civilization to pirates” ACM mobile computing and communications review, Vol. 7 No.1, pp. 74-94 Jan-03.

6.A.A. Ramanujam,J.Bonney,R,Hagelstrom and K.Thurber,”Techniques for Intrusion resistant Ad Hoc Routing Algorithms (TIARA)” in proceedings of MILCOM Conference,2000.

7. Y.Hu,D.B.Johnson and A.Perrig,” SEAD: Secure Efficient distance vector routing for mobile wireless ad hoc networks” in proceedings of fourth IEEE workshop on mobile computing systems & Applicatons,pp3-13, 2002.

8.H.Luo and S.Lu,Ubiquitous and robust authentication services for ad hoc wireless networks” Dept. of Computer Science,UCLA Technical report TR200030,2000.

9. Sergio Marti,T.J.Giuli,Kevin Lai and Mary Baker, “Mitigating routing misbehavior in mobile ad hoc networks “in proceedings of the 6th annual international conference on mobile computing and networking(MobiCom’00) Bostan 2000,pp255-265.

10.S.Buchegger and J Boudec, “Performance analysis of the CONFIDANT protocol: Cooperation of nodes fairness in Distributed AdHoc Networks “in proceedings of MobiHoc conference,2002

11.P.Michiardi and R.Molva, “CORE:A Collaborative REputation mechanisms to enforce node cooperation in mobile ad hoc networks in proceedings of Communication and Multimedia Security Conference, pp. 107-121,2002.

12. Y.Huang and W.Lee “A cooperative intrusion detection system for ad hoc networks “in proceedings of ACM workshop on security of Ad Hoc and Sensor Networks,2003.

13. Y.Hu ,A Perrig and D.B.Johnson, “Ariadne : A secure on demand routing protocol for ad hoc networks “in proceedings of the 8th Annual International Conference on Mobile Computing and Networking, pp.12-23, 2002.

14.B.Awerbuch,D.Holmer,C,Nita Rotaru and H.Rubens “An on demand secure routing protocol resilient to byzantine failures,” in proceedings of ACM workshop on wireless Security,pp.21-302002.

15..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.

16.Wei-Shen Lai, Chu-Hsing Lin , Jung-Chun Liu , Hsun-Chi 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.

17.Shabana Mehfuz, Doja,M.N.: Swarm Intelligent Power-Aware Detection of Unauthorized and Compromised Nodes in MANETs", Journal of Artificial Evolution and Applications,2008.

18.Xiaoxin Wu, David,K.Y.Yau, Mitigating Denial-of-Service 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.

19.Ping Yi, Zhoulin Dai, Shiyong Zhang, Yiping Zhong: A New Routing Attack in Mobile Ad Hoc Networks, International Journal of Information Technology, Vol. 11, No.2,2005.

20.John Haggerty, Qi Shi, Madjid Merabti: Statistical Signatures for Early Detection of Flooding Denial-Of service Attacks , Springer, 2005, Vol. 181, pp. 327-341,2005.

21.Wei Ren, Dit-Yan Yeung, Hai Jin, Mei Yang: Pulsing RoQ DDoS Attack and Defense Scheme in Mobile Ad Hoc Networks, International Journal of Network Security, Vol. 4, No.2, pp. 227-234 (2007)

22.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.