DDoS attack Defense Mechanism using Trusted Nodes in MANETs

Divya Gautam
Department of CSE
Amity University, Gwalior, Madhya Pradesh

ABSTRACT

In mobile adhoc networks the hosts are always moving and make communication network randomly.This provides high flexibility but a lot many challenges for adhoc networks against malicious attacks. In this paper, we are using mobility as a boon to design the defense strategy to mitigate DDoS in adhoc networks. In DDos attacks normally attacker attacks on a specific target node. After a certain period of attacking time, the attacker will give up if the target node is not identified. In this defence mechanism, high redundancy is taken in consideration and selecting a trusted node. The target node will function normally and assuming that attacker will stop attacking in the absence of target node. By using NS-2 simulator we have proved that the given defence mechanism is effective and low cost.

***Keywords*—DDoS Attack Mitigation, MANETs, Redundancy,Protection Node.**

1. INTRODUCTION

Mobile adhoc networks are inherently susceptible to security problems. The intrusion on the transmission medium is easier than for wired networks and it is possible to conduct denial of service attacks by scrambling the used frequency bands. The ad hoc context increases the number of potential security vulnerabilities. Ad hoc networks cannot benefit from the security services offered by dedicated equipment such as firewalls, authentication servers and so on. The security services must be distributed, cooperative and consistent with the available bandwidth. 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 an extremely large volume of packets to a target machine through the simultaneous cooperation of a large number of hosts that are distributed throughout the network. The attack traffic consumes the bandwidth resources of the network or the computing resource at the target host, so that legitimate requests will be discarded. A bandwidth depletion attack is designed to flood the victim network with unwanted traffic that prevents legitimate traffic from reaching the victim system. A resource depletion attack is an attack that is designed to tie up the resources of a victim system. This type of attack targets a server or process at the victim making it unable to legitimate requests for service. Any amount of resources can be exhausted with a sufficiently strong attack. The only viable approach is to design defense mechanism that will detect the attack and respond to it by dropping the excess traffic. The DoS attacks that target resources can be grouped into three broad scenarios. 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. Consider the case where a node continuously sends an executable flooding packet to its neighborhoods 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. A malicious node may continuously send a bogus packet to a node with the intention of consuming the victim’s battery energy and preventing other nodes from communicating with the node. The use of localized monitoring can help in detecting such nodes and preventing their consequences. 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. This consumes the resources of all neighbors that communicate, overloads the network, and results in performance degradations. Such attacks can be prevented based on our proposed congestion based defense scheme.

2. Related Work

XiapuLuo et al [1] 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 [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. Xiaoxin Wu et al [6] 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 YipingZhong [8] have presented a new DOS attack and its defense in 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 MadjidMerabti [9] 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 [11] 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. Gahng-SeopAhn et al [12] have proposed SWAN, a stateless network model which uses distributed control algorithms to deliver service differentiation in mobile mobile ad hoc networks in a simple, scalable and robust manner. GirirajChauhan and Sukumar Nandi [13] proposed a QoS aware on demand routing protocol that uses signal stability as the routing criteria along with other QoS metrics. 3 Proposed Defense Technique In this paper, we propose a new defense mechanism which consists of a flow monitoring table (FMT) at each node. It contains flow id, source id, packet sending rate and destination id. Sending rates are estimated for each flow in the intermediate nodes. The updated FMT is sent to the destination along with each flow. After monitoring the MAC layer signals the destination sends the Explicit Congestion Notification (ECN) bit to notify the sender nodes about the congestion. The sender nodes, upon seeing these packets with ECN marking, will then reduce their sending rate. If the channel continues to be congested because some sender nodes do not reduce their sending rate, it can be found by the destination using the updated FMT. It checks the previous sending rate of a flow with its current sending rate. When both the rates are same, the corresponding sender of the flow is considered as an attacker. Once the DDoS attackers are identified, all the packets from those nodes will be discarded.

The two phases of the proposed scheme are Bandwidth querying phase and Data transmission phase. In bandwidth querying phase the control messages sent are Bandwidth query request and Bandwidth query reply. The request packet includes the source IP address, destination IP address, type of the message, flow ID, and requested data rate which is stored in the bottleneck bandwidth (BnBW) field. In Bandwidth querying phase of the proposed scheme, the node’s FMT information along a path is computed. An intermediate node updates its FMT using the BnBW value stored in the reply packet after receiving a REPLY message on the reverse path, and then forwards the REPLY to the next node. The available bandwidth ABWj is checked first. The reservation of bandwidth for the flow can be made if the value of ABWj is greater than or equal to the BnBW value in the REPLY packet. Else, the BnBW value in the REPLY packet is overwritten with the smaller value of ABWj. Next, the current BnBW value in the REPLY packet is added to the reserved rate RRij, associated with the in-out stream. A FMT entry is created with an assigned rate value ARij, set equal to the BnBW value of the REPLY packet, if the stream (i, j) was previously inactive. Subsequently, the REPLY packet is forwarded to the next node on the reverse path. Finally, based on the value of the BnBW field, the source establishes the real-time flow when the REPLY packet reaches the source node.

3. DDOS ATTACK IN MOBILE AD HOC NETWORKS

The authors S.A.Arunmozhi,Y.Venkataramani in 2011 proposed that the mobile ad hoc networks are highly vulnerable to distributed denial of service(DDoS) attacks due to its unique characteristics like open network architecture, shared mobile medium and stringent resource constraints. The tcp throughput heavily and decreases the quality of service(QoS) to end systems gradually rather than refusing the clients from the services in a complete manner. In this paper, there is a discussion about DDoS attacks and proposed a protected scheme which helps to improve the performance of the ad hoc networks. The proposed ptotect mechanism which uses the medium access control (MAC) layer information which detect the attackers. The status values of MAC layer that can be used for detection are Frequency of receiving RTS/CTS packets, Frequency of sensing a busy channel and RTS/DATA retransmissions. Once the attackers are identified, all the packets from those nodes will be stopped. The network resources are made available to the legal users.

4. USING TARGET CUSTOMER BEHAVIOUR

The authors K.Kuppusamy ,S.Malathi in 2012 proposed that the possibility of sharing information through networking has been growing in geometrical progression. The network attacks are to be noted in this connection, on other hand, DDoS attacks are also rising in equal parts. Sharing of information is carried out by means of client and server. The client requested for data to the server and the server provided the response to the client-request. Here the client can violate the server performance by sending anomaly requests. As a result,the server performance is degraded. In This paper discussions about best degradation of the performance which can be prevented using some kind of algorithm proposed in the methodology in which manner. In this work the blocking is done using a different types of mechanism based on category of a client.

5. IP BROADCAST USING DISABLE TECH.

The authors Mukesh Kumar and Naresh Kumar in 2013 proposed that Ad-hoc network is the network consisted of mobile nodes. This network is infrastructure less which is self configured i.e. the connections are made without any centralized administration. MANET has no clear line of defense so it is accessible to both legal network users and harmful attackers. When malicious nodes are present ,one of the main challenge in MANET which designs the robust security solution that can prevent MANET from different DDOS attacks. Different mechanisms are proposed using different cryptography techniques to measure these attacks against MANET. These mechanisms are not suited for MANET resource constraints, i.e., limited bandwidth and battery power due to huge load of traffic which is introduced to exchange and verifying keys. Therefore ad hoc networks have their own vulnerabilities that cannot be ever handled by these wired network security solutions. Distributed Denial of Service (DDoS) attacks also becoming a problem for computer users, which are connected to the Internet. In this paper, a technique is proposed that can prevent a specific type of DDoS attack. The proposed scheme is distributed which has the ability to prevent from Distributed DoS (DDoS) attack. The performance of the proposed scheme in a terms of simulations which shows the proposed scheme to provide a better solution than existing schemes.

6. PREVENTION OF ATTACKS IN MOBILE NETWORKS

The authors BalaVeeravatnam, D. SugunaKumari, P. Sowmya in 2015 proposed in the network environment most of the time there could be more chances of the attacks. It means mostly it does not guarantee about the packets can be easily transfer on the network. It degrades network performance . To overcome this problem of network traffic and performance implementing a Packet Hiding Scheme that can be securely sent packets on thenetwork. While eavesdropping and message injection can be prevented using cryptography method. It has been shown to actualize severe Denial-of-Service attacks against networks. In the simplest form of jamming, the interferes with the reception of messages by transmitting a continuous jamming signal or several short jamming pulses. Generally, jamming attacks are considered under an external threat model, in which the jammer is not part of the network. In this paper, there is a developing and surveying on the two schemes that prevent real-time packet classification by combining Cryptography Puzzles and SHCS. In this, there is analyzing the security of methods and evaluate their computational and system overhead.

7. CONCLUSION

In this paper, we have presented an overview of DOS and DDoS defense schemes. Security is one of the most important feature for deployment in Mobile Adhoc Network. The different types of attacks and tools have been represented for the implementation of the DDoS attacks Distributed Denial of Service attacks are more complex and serious problem, and as a result, several approaches have been proposed to detect them. This paper discussed the various methods available in the literature with regard to various defense mechanisms for DoS and DDoS attacks on MANET.

REFERENCES:

1.XiapuLuo, Edmond W.W.Chan,RockyK.C.Chang: Detecting Pulsing Denial-of-Service Attacks with Nondeterministic Attack Intervals, EURASIP Journal on Advances in Signal Processing (2009).

2. Gahng-SeopAhn, Andrew T. Campbell, AndrasVeres, Li-Hsiang Sun:SWAN: Service Differentiation in Stateless Wireless Ad Hoc Networks, in Proceedings of IEEE Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM, Vol. 2 (2002).

3. Wei-Shen Lai, Chu-HsingLin , 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).

4. ShabanaMehfuz, Doja,M.N.: Swarm Intelligent Power-Aware Detection of Unauthorized andCompromised Nodes in MANETs", Journal of Artificial Evolution and Applications (2008).

5. Nagesh,H.R.,ChandraSekaran,K.: Design and Development of Proactive Models for Mitigating Denial-of-Service and Distributed Denial-of-Service Attacks, International Journal of Computer Scienceand Network Security, Vol. 7, No.7 (2007).

6. 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).

7. SugataSanyal, Ajith Abraham, DhavalGada, RajatGogri, PunitRathod, ZalakDedhia,NiraliMody: Security Scheme for Distributed DoS in Mobile Ad Hoc Networks, ACM, Newyork,USA (2004).

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

9. John Haggerty, Qi Shi, MadjidMerabti: Statistical Signatures for Early Detection of Flooding Denial-Of service Attacks , Springer, 2005, Vol. 181, pp. 327-341 (2005).

10. Giovanni Vigna, SumitGwalani, KavithaSrinivasan: An Intrusion Detection tool for AODV-based Ad hoc Wireless Networks, in Proceedings of the Annual Computer Security Applications Conference, pp.16-27 (2004).

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

12. Yang Xiang, Wanlei Zhou, MorshedChowdhury: A Survey of Active and Passive Defense Mechanisms against DDoS Attacks, Technical reports, Computing series, Deakinuniversity,Schoolof Information Technology(2004).

13. GirirajChauhan,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).

14.BalaVeeravatnam, D. SugunaKumari, P. Sowmya" Preventing Black Hole Attacks in Mobile Networks" Volume 5, Issue 11, November 2015.

15.Mukeshkumar “DETECTION AND PREVENTION OF DDOS ATTACK IN MANET’S USING DISABLE IP BROADCAST TECHNIQUE” International Journal of Application or Innovation in Engineering & Management (IJAIEM). Volume 2, Issue 7, July 2013.

16.SaurabhRatnaparikhi ,AnupBhange “ DDOS Attacks on Network; Anomaly Detection using Statistical Algorithm” Volume 2, Issue 12, December 2012. [4] K.Kuppusamy and S.Malathi“ Prevention of Attacks under DDoS Using Target Customer Behavior” Vol. 9, Issue 5, No 2, September 2012.

17.S.A.Arunmozhi “DDoS Attack and Defense Scheme in Mobile Ad hoc Networks” International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May 2011.

18.Wentao Liu “Research on DoS Attack and Detection Programming ” Third International Symposium on Intelligent Information Technology Application,2009.

19. Wei Ren and Dit-Yan Yeung “Pulsing RoQDDoS Attack and Defense Scheme in Mobile Ad Hoc Networks” International Journal of Network Security, Vol.4, No.2, PP.227-234, Mar. 2007.

20. Stephen M. Specht “Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures” International Journal of Advanced Research in Computer Science and Software Engineering Sep. 2004.