A Low Rate DDoS: A Security Threat in Mobile Adhoc Networks

Sunitha M.S[*], Sayyid Abrar[**]

Department of Computer Science and Engineering, Dayananda Sagar College of Engineering.

Abstract- Network security is soft spot in wired or wireless networks, MANETS pose number of nontrivial challenges to the security design, such as shared wireless medium, dynamically changing topology etc.DoS and DDoS are two of the most harmful threats to the network. MANETS are more vulnerable to these attacks. In this paper we discuss about the low-rate DDoS attack is of serious concern since it has the ability to conceal the attack traffic with normal traffic, and also we discuss various security types of attacks in MANETS.
Index Terms: MANETS, DoS, low-rate DDoS, attacks.

1. Introduction

The Mobile Ad Hoc Network (MANET) is a infrastructure less, self-organizing, and adaptive gathering of independent mobile nodes, which are communicating over wireless links, Each node in a MANET is free to move independently in any direction, and will therefore change its links to other nodes frequently. Each must forward traffic unrelated to its own use, and therefore be a router. Due to unpredictable topology wireless shared medium, heterogeneous resources and stringent resources constraints MANETS are more prone to physical security threats when compared to wired networks. Nodes that perform attacks with the aim of damaging other network outage are considered as malicious and active attack, while nodes that aim to save battery life for their own communication are considered to be selfish and called as passive attacks. MANET is characterized by limited resources such as bandwidth, battery power, and storage space. Unlike traditional networks, MANETs are more vulnerable to DoS attacks due to limited resources that force nodes to be greedy in resource utilization. The malicious nodes compromise with other nodes to drop the forwarding packets causing repeated retransmission of the same packets. Battery power and limited band width is the critical issue in MANETS, if the battery power is used up due to malicious attacks, the victim will not able to provide the network services.
A DDoS attack is a distributed, large-scale attempt by malicious nodes to flood the victim network with an enormous number of packets. This exhausts the victim network of resources such as band width, processing speed, battery power etc. The victim is unable to provide service to legitimate clients and network performance is highly deteriorated.

2. TYPES OF ATTACKS

MANETS are prone to different types of attacks due to its wireless medium and dynamically changing topology, MANETS are basically vulnerable due to two types of attacks: active and passive attacks [1]. Active attack is an attack when a misbehaving node has to bear to some energy cost in order to perform the threat. On the other hand passive attacks are mainly due lack of co-operation with an intention of saving energy selfishly. The attacks in MANETS are classified as modification, impersonation, fabrication, wormhole and lack of co operation [2].

2.1 Attacks using modification

An attack through which an unauthorized node gains access to the network or shared resources and tries to tamper the routing messages in the network is known as attack using modification.

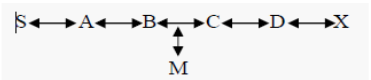


Figure 2.1: Ad hoc network and a malicious node

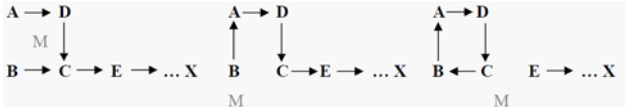
In figure 2.1 a malicious node M can keep traffic from reaching X by continuously advertising to B a shorter route to X than the route to X the the node C advertises[5].A malicious node may attempt to redirect the network traffic and conduct denial-of-service attack by tampering message fields or by forwarding routing messages with false values. In Dos attack, the malicious node causes the network traffic to drop and redirect the network traffic to a different destination thereby creating unnecessary delay in communication.

2.2 Attacks using impersonation

In this attack, a malicious node establish attack in a network by pretending like the other node in the network. A malicious node misrepresents its identity in the network by altering MAC or IP address of outgoing packets known

Manuscript received November 5, 2012
Manuscript revised November 20, 2012

as spoofing and may also form loops in routing packets resulting in network partitioning.



(a) (b) (c)

Figure 2.3: A sequence of events forming loops by spoofing packets

A path exists between five nodes in figure 2.3(a). A can hear B and D, B can hear A and C, D can hear A and C, and C can hear B, D and E. M can hear A, B, C, and D while E can hear C and next node in the route towards X. A malicious node M can learn about the topology analyzing the discovery packets and then form a routing loop so that no one nodes in his range can reach to the destination X. At first, M changes its MAC address to match A's, moves closer to B and out of the range of A. It sends a message to B that contains a hop count to X which is less than the one sent by C, for example zero. Now B changes its route to the destination, X to go through A as shown in the fig. 2.3(b). Similarly, M again changes its MAC address to match B's, moves closer to C and out of the range of B. Then it sends message to C with the information that the route through B contains hop count to X which is less than E. Now, C changes its route to B which forms a loop as shown in fig. 2.3(c). Thus X is unreachable from the four nodes in the network.

2.3 Attacks through fabrication

In MANET, an attack performed by generating fake routing messages is known as fabrication. An attack through fabrication is difficult to verify as they come as valid constructs [4]. In figure 2.2 S node has a route to X through the nodes A, B, C and D. A malicious node M can establish a denial-of-service attack against X by spoofing node C and thereby continually sending route error messages to B , indicating a broken link between nodes C and X. Node B deletes its routing table entry by seeing the spoofed route error messages thinking it came from node C. Malicious node M succeeds in preventing the communication between node S and X by broadcasting spoofed route error messages whenever a route is established .

2.4 Lack of cooperation

In MANETs cooperation of nodes is important and packet forwarding in MANETs rely on the cooperation of the nodes participating in routing. If any node do not cooperate for routing and behaves selfishly to save its battery power for its own communication then it endangers the correct network operations and such attacks are known as black-hole attack.

3. DDoS ATTACKS

DoS is an attack which makes network resources unavailable to the legitimate users. The motive and target of a DoS attacks varies generally from small to large network users. In DoS attack the perpetrators of DoS attack floods the target machine [1] or node in a network. The perpetrators of a DoS attack sends more requests their by increasing the volume of traffic to the targeted node in the network.

DDoS is a kind DoS attack in which one or more compromised nodes in a network collectively targets and attacks a particular node in the network. DDoS are combative and it is developed constantly to attack the target machine co-ordinatively. The are two types of DDoS attacks high rate and low-rate. In high rate SYN flooding based DDoS attacks are possible, in this attack a large number of spoofed SYN packets to the victim node which can exaust the processing capacity of the node, causing all of new incoming legitimate SYN request to be dropped. A low-rate DDoS is a type of DDoS attack where the malicious node send attack traffic or drop forwarding packets at a very low rate, this type of attack has capacity to elude the detection system.

Flooding, wormhole, modification, fabrication, impersonation, lack of co-operation attacks have been considered various forms of DDoS attacks. Many detection methods such as profile-based and specification based have been have been implemented to detect DDoS attacks in MANETS, global co-ordinated filters and IP tracing improves the security in MANETS against DDoS[2].`

4. Low rate DDoS Attack

A Low Rate distributed denial of service attack (DDoS) is a serious threat to MANET since it has ability to conseal the traffic because it is much like normal traffic, a low rate DDoS attack is a intelligent attack as the attacker can send packets or drop packets at a very low rate. when the malicious nodes in a MANET drop packets at a very low rate or send the route discovery packets in network, purposefully to exhaust the band width, processing capacity of the node in a network or power battery of the node. since MANETS operate in a low band width and has limited power battery this type of attack can cause serious threat to the network.

5. CONCLUSION

In wired network the low-rate DDoS is considered as serious threat[3], since several detection mechanism such as signature based and anomaly based have not been proven the best solution for low-rate DDoS attack. In

MANETS the low-rate DDoS attack is a serious threat since there is no complete solution to prevent and detect low rate DDoS, because it is much like normal traffic

References

[1] Secrecy Throughput of MANETs Under Passive and Active Attacks Yingbin Liang, Member, IEEE, H. Vincent Poor, Fellow, IEEE, and Lei Ying, Member, IEEE

[2] Andrim Piskozub; Denial of Service and Distributed Denial of Service Attacks; TCSET-02; Lviv – Shavsko, Ukraine; February 18-23, 2002. .

[3] Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics Yang Xiang, Member, IEEE, Ke Li, and Wanlei Zhou, Senior Member, IEEE

[4] P. Michiardi, R. Molva, "Ad hoc networks security," IEEE Press Wiley, New York, 2003.

[5] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, E.M. Belding Royer, "Secure routing protocol for ad hoc networks," In Proc. of 10th IEEE International Conference on Network Protocols, Dept. of Comput.Sci., California Univ., Santa Barbara, CA,USA. 12-15 Nov. 2002, Page(s): 78- 87, ISSN: 1092-1648

Sunitha M S received B.E. degree in Information Science and Engineering from NIE Mysore, Visveswaraya Technological University in 2006 and M.Tech from Dayananda Sagar College of Engineering in Computers Networks and Engineering, VTU in 2009. Her research interest includes network, information security and MANETS. She is currently working as a Lecturer at Dayananda Sagar College of Engineering. Has a teaching experience of over 4 years in the field of Computer Science.

He is completed his B.E from Visveswaraya Technological University. He is currently pursing Masters of Technology from Dayananda Sagar College of Engineering in Computers Networks and Engineering. His research interests include routing in Manets and preventing the possible attacks in Manets.