Volume 2, Issue 8, August 2012 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Study of Attack Prevention Methods for DDOS Attacks In Manets

Mukesh Kumar, Naresh Kumar

Department of computer science & Enginmering,
U.I.E.T. Kurukshetra University, Kurukshetra
Haryana, India

Abstract— Ad-hoc network is the network comprised of wireless nodes. It is basically infrastructure less network which is self configured i.e. the connections are established without any centralized administration. MANET has no clear line of defence so it is accessible to both legitimate network users and malicious attackers. In the presence of malicious nodes, one of the main challenges in MANET is to design the robust security solution that can prevent MANET from various DDOS attacks. Different mechanisms have been proposed using various cryptographic techniques to countermeasures these attacks against MANET. These mechanisms are not suitable for MANET resource constraints, i.e., limited bandwidth and battery power because they introduced heavy traffic load to exchange and verifying keys. Therefore ad hoc networks have their own vulnerabilities that cannot be always tackled by these wired network security solutions. Distributed Denial of Service (DDoS) attacks have also become a problem for users of computer systems connected to the Internet. Particularly, the researchers have examined different DDOS attacks and some detection methods like profile based detection, specification based detection as well as existing solutions to protect MANET protocols.

Keywords— MANET, DDOS attack, Security, Prevention Methods Malicious node.

1. Introduction

Ad-hoc network is the network comprised of wireless nodes. It is basically infrastructure less network which is self configured i.e. the connections are established without any centralized administration [1,2]. A mobile ad hoc network (MANET) is a spontaneous network that can be established with no fixed infrastructure. This means that all its nodes behave as routers and take part in its discovery and maintenance of routes to other nodes in the network i.e. nodes within each other's radio range communicate directly via wireless links, while those that are further apart use other nodes as relays. Its routing protocol has to be able to cope with the new challenges that a MANET creates such as nodes mobility, security maintenance, quality of service, limited bandwidth and limited power supply. These challenges set new demands on MANET routing protocols. There are different major issues and sub-issues involving in MANET such as routing, multicasting/broadcasting, location service, clustering, mobility management, TCP/UDP, IP addressing, multiple access, radio interface, bandwidth management, power management, security, fault tolerance, QoS/multimedia and standards/products. Currently, routing, power management, bandwidth management, radio interface, attacks and security are hot topics in MANET research [1] [3]. Recent wireless research indicates that the wireless MANET presents a larger security problem than conventional wired and wireless networks. Distributed Denial of Service (DDoS) attacks have also become a problem for users of computer systems connected to the Internet. A DDoS attack is a distributed, large-scale attempt by malicious users to flood the victim network with an enormous number of packets. This exhausts the victim network of resources such as bandwidth, computing power, etc. The victim is unable to provide services to its legitimate clients and network performance is greatly deteriorated[2][5]. In this paper, we look into various methods for prevention of DDoS attacks. The rest of the paper is organized as follows. The next section discusses the DDOS attacks in MANETS and different types of DDOS Attacks. In section 3 we discussed attack detection methods in MANET. In section 4, we present various defence mechanisms against DDoS attacks. We conclude in Section 5.

2. DDOS Attacks in MANETs

Distributed denial of Service attacks usually occurs in MANETS or in wireless networks. It is an attack where multiple systems comprised together and target a single system causing a denial of service (DoS)[2,5]. The target node is flooded with the data packets that system shutdowns, thereby denying service to legitimate users.

A Denial of Service (DoS) attack is an attack with the purpose of preventing legitimate users from using a specified network resource such as a website, web service, or computer system [7]. A DDoS attack is a distributed, large-scale attempt by malicious users to flood the victim network with an enormous number of packets. This exhausts the victim network of resources such as bandwidth, computing power, etc. The victim is unable to provide services to its legitimate clients and network performance is greatly deteriorated. Or in another way we can say that a Distributed Denial of Service (DDoS) attack is a coordinated attack on the availability of services of a given target system or network that is launched indirectly through many compromised computing systems. The services under attack are those of the “primary victim”, while the compromised systems used to launch the attack are often called the “secondary victims.” The use of secondary victims in a DDoS attack provides the attacker with the ability to wage a much larger and more disruptive attack while remaining anonymous since the secondary victims actually perform the attack making it more difficult for network forensics to track down the real attacker[6].

The current mobile adhoc networks allow for many different types of attacks. Although the analogous exploits also exist in wired networks but it is easy to fix by infrastructure in such a network. Current MANets are basically vulnerable to two different types of DDoS attacks: active DDoS attacks and passive DDoS attacks [4]. Active DDoS attack is an attack when misbehaving node has to bear some energy costs in order to perform the threat. On the other hand, passive DDoS attacks are mainly due to lack of cooperation with the purpose of saving energy selfishly [8]. Nodes that perform active DDoS attacks with the aim of damaging other nodes by causing network outage are considered as malicious while nodes that make passive DDoS attacks with the aim of saving battery life for their own communications are considered to be selfish [9] [10]. The attacks are classified as modification, impersonation, fabrication, wormhole and lack of cooperation [1].

2.1 Modification Attack :

Modification is a type of attack when an unauthorized party not only gains access to but tampers with an asset. For example a malicious node can redirect the network traffic and conduct DoS attacks by modifying message fields or by forwarding routing message with false values. In figure 1, *M* is a malicious node which can keep traffic from reaching *X* by continuously advertising to *B* a shorter route to *X* than the route to *X* that *C* advertises[11]. In this way, malicious nodes can easily cause traffic subversion and DoS by simply altering protocol fields: such attacks compromise the integrity of routing computations. Through modification, an attacker can cause network traffic to be dropped, redirected to a different destination or to a longer route to reach to destination that causes unnecessary communication delay.

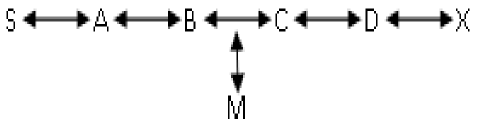

Figure 1: Adhoc network and a malicious node

Consider the following figure 2. Assume a shortest path exists from ***S*** to ***X*** and, ***C*** and ***X*** cannot hear each other, that nodes ***B*** and ***C*** cannot hear other, and that ***M*** is a malicious node attempting a denial of service attack. Suppose ***S*** wishes to communicate with ***X*** and that ***S*** has an unexpired route to ***X*** in its route cache. ***S*** transmits a data packet toward ***X*** with the source route ***S*** --> ***A*** --> ***B*** --> ***M*** --> ***C*** --> ***D*** --> ***X*** contained in the packet’s header. When ***M*** receives the packet, it can alter the source route in the packet’s header, such as deleting ***D*** from the source route. Consequently, when ***C*** receives the altered packet, it attempts to forward the packet to ***X***. Since ***X*** cannot hear ***C***, the transmission is unsuccessful[11].

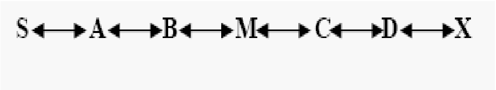

Figure 2: Adhoc network with DoS attack

2.2 Impersonation Attacks :

As there is no authentication of data packets in current adhoc network, a malicious node can launch many attacks in a network by masquerading as another node i.e. spoofing. Spoofing is occurred when a malicious node misrepresents its identity in the network (such as altering its MAC or IP address in outgoing packets) and alters the target of the network topology that a benign node can gather. As for example, a spoofing attack allows forming loops in routing packets which may also result in partitioning network. Here the scenario is described in details.

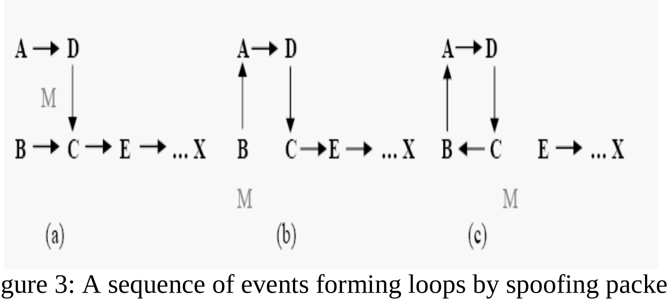

Figure 3: A sequence of events forming loops by spoofing packets

In the above fig. 3(a), there exists a path between five nodes. ***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 figure 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 figure 3(c). Thus ***X*** is unreachable from the four nodes in the network.

2.3 Fabrication Attacks :

Fabrication is an attack in which an unauthorized party not only gains the access but also inserts counterfeit objects into the system. In MANET, fabrication is used to refer the attacks performed by generating false routing messages. Such kind of attacks can be difficult to verify as they come as valid constructs, especially in the case of fabricated error messages that claim a neighbour cannot be contacted[12]. Consider the figure 1. Suppose node ***S*** has a route to node ***X*** via nodes ***A, B, C,*** and ***D.*** A malicious node ***M*** can launch a denial-of-service attack against ***X*** by continually sending route error messages to ***B*** spoofing node ***C,*** indicating a broken link between nodes ***C*** and ***X. B*** receives the spoofed route error message thinking that it came from ***C. B*** deletes its routing table entry for ***X*** and forwards the route error message on to ***A,*** who then also deletes its routing table entry. If ***M*** listens and broadcasts spoofed route error messages whenever a route is established from ***S*** to ***X, M*** can successfully prevent communications between ***S*** and ***X***[11]**.**

2.4 Wormhole Attacks :

Wormhole attack is also known as tunnelling attack. A tunnelling attack is where two or more nodes may collaborate to encapsulate and exchange messages between them along existing data routes. This exploit gives the opportunity to a node or nodes to short-circuit the normal flow of messages creating a virtual vertex cut in the network that is controlled by the two colluding attackers. In the figure 4, ***M1*** and ***M2*** are two malicious nodes that encapsulate data packets and falsified the route lengths.

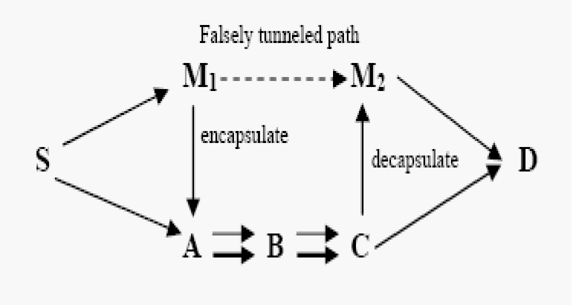

Figure 4: Path length spoofed by tunnelling.

Suppose node ***S*** wishes to form a route to ***D*** and initiates route discovery. When ***M1*** receives a *RREQ* from ***S, M1*** encapsulates the *RREQ* and tunnels it to ***M2*** through an existing data route, in this case {***M1*** --> ***A*** --> ***B*** --> ***C*** --> ***M2***}. When ***M2*** receives the encapsulated *RREQ* on to ***D*** as if had only travelled {***S*** --> ***M1*** --> ***M2*** --> ***D***}. Neither ***M1*** nor ***M2*** update the packet header. After route discovery, the destination finds two routes from ***S*** of unequal length: one is of 5 and another is of 4. If ***M2*** tunnels the *RREP* back to ***M1***, ***S*** would falsely consider the path to ***D*** via ***M1*** is better than the path to ***D*** via ***A***. Thus, tunnelling can prevent honest intermediate nodes from correctly incrementing the metric used to measure path lengths.

2.5 Lack of Cooperation :

Mobile Ad Hoc Networks (MANETs) rely on the cooperation of all the participating nodes. The more nodes cooperate to transfer traffic, the more powerful a MANET gets. But one of the different kinds of misbehaviour a node may exhibit is selfishness. A selfishness node wants to preserve own resources while using the services of others and consuming their resources. This can endanger the correct network operation by simply not participating to the operation or by not executing the packet forwarding. This attack is also known as the selfish attack or lack of cooperation.

3. Attack Detection Methods In MANET :

There are various detection mechanisms such as Profile based detection and Specification based detection are described below [13] [10]:

3.1 *Profile-based detection :*

Profile-based detection is also called behaviour-based detection. Profile-based detection defines a profile of normal behaviour and classifies any deviation of that profile as an anomaly. The assumption of this type of detection is that attacks are events distinguishable from normal legitimate use of system resources. Although this type of anomaly detectors are able to detect novel attacks, they are prune to high false positive rate due to the difficulty of clear segmentation between normal and abnormal activities and the use of insufficient or inadequate features to profile normal behaviours [14].

3.2 *Specification-based detection*

Specification-based detection defines a set of constraints that describe the correct operation of a program or protocol and monitors the execution of the program with respect to the defined constraints. It has been show that specification-based techniques live up to their promise of detecting known as well as unknown attacks, while maintaining a very low rate of false positives. Since, the increasing popularity of wireless networks to that of wired networks, security is being considered as a major threat in them. Wireless networks exposes a risk that an unauthorized user can exploit and severely compromise the network. There can be different possible attacks in wireless network viz., active and passive attacks. So there is a need for secured wireless system to analyze and detect number of attacks [14].

4. Defense Mechanisms :

According to paper [9,10,13] defense mechanisms to DDoS attacks are classified into two broad categories: local and global. As the name suggests, local solutions can be implemented on the victim computer or its local network without an outsider's cooperation. Global solutions, by their very nature, require the cooperation of several Internet subnets, which typically cross company boundaries.

4.1 *Local Solutions*: - Protection for individual computers falls into three areas.

4.1.1 *Local Filtering:* In this scheme we filter the packet at the local router level and detect them. The timeworn short-term solution is to try to stop the infiltrating IP packets on the local router by installing a filter to detect them. The stumbling block to this solution is that if an attack jams the victim's local network with enough traffic, it also overwhelms the local router, overloading the filtering software and rendering it inoperable. [9].

4.1.2 *Changing IPs:* A Band-Aid solution is to change the victim's IP address. As the whole process of changing the IP address is completed, all routers will be informed of that change and now if the attacker send infected packets than the edge router will drop the packets.

4.1.3 *Creating Client Bottlenecks:* The objective behind this approach is to create bottleneck processes on the zombie computers, limiting their attacking ability.

4.2 *Global Solutions*

Clearly, as DDoS attacks target the deficiencies of the network/Internet as a whole, local solutions to the problem become futile. Global solutions are better from a technological standpoint. The real question is whether there is a global incentive to implement them.

4.2.1 *Improving the Security of the Entire Internet:* Improving the security of all computers linked to the Internet would prevent attackers from finding enough vulnerable computers to break into and plant daemon programs that would turn them into zombies.

4.2.2 *Using Globally Coordinated Filters:* The strategy here is to prevent the accumulation of a critical mass of attacking packets in time. Once filters are installed throughout the network/Internet, a victim can send information that it has detected an attack, and the filters can stop attacking packets earlier along the attacking path, before they aggregate to lethal proportions. This method is effective even if the attacker has already seized enough zombie computers to pose a threat [9].

4.2.3 *Tracing the Source IP Address:* The goal of this approach is to trace the intruders' path back to the zombie computers and stop their attacks or, even better, to find the original attacker and take legal actions. If tracing is done promptly enough, it can help to abort the DDoS attack. Catching the attacker would deter repeat attacks. However, two attacker techniques hinder tracing: IP spoofing that uses forged source IP addresses, The hierarchical attacking structure that detaches the control traffic from the attacking traffic, effectively hiding attackers even if the zombie computers are identified.

5. Conclusion :

DDoS attacks make a networked system or service unavailable to legitimate users. Loss of network resources causes economic loss, work delays, and loss of interaction between network users. In this paper we discussed distributed denial of services (DDoS).

Different DDoS attacks such as flooding, wormhole, modification, impersonation, fabrication, modification, selfish or lack of cooperation attacks are discussed. Some detection methods like profile-based detection and specification-based detection are examined. The existing solutions such as local filtering, changing IPs and creating client bottlenecks are local solutions and global solutions are improving the security of the entire Internet, using globally coordinated filters and tracing the source IP address to protect MANET protocols were described.

REFRENCES:

[1] Kamanshis Biswas and Md. Liakat Ali; Security Threats in Mobile Ad Hoc Network; Master Thesis; Thesis no: MCS- 2007:07; March 22, 2007.

[2] Stephen M. Specht and Ruby B. Lee; Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures; Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems, 2004 International Workshop on Security in Parallel and Distributed Systems, pp. 543-550; September 2004.

[3] Vesa Kärpijoki; Security in Ad Hoc Networks; Helsinki University of Technology; HUT TML 2000.

[4] C. Patrikakis, M. Masikos and O. Zouraraki, Distributed Denial of Service Attacks, The Internet Protocol Journal, Vol. 7, No. 4, Dec 2004.

[5] Felix Lau, Stuart H. Rubin, Michael H. Smith and Ljiljana TrajkoviC; Distributed Denial of Service Attacks; pp 2275- 2280/2004 IEEE.

[6] Stephen M. Specht "Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures" Sep. 2004.

[7] David Karig and Ruby Lee, “Remote Denial of Service Attacks and Countermeasures,” *Princeton University Department of Electrical Engineering Technical Report CEL2001- 002*, Oct 2001.

[8] J. Mirkovic and P. Reiher, A Taxonomy of DDoS Attack and DDoS Defense Mechanisms, ACM Sigcomm Computer Communications Review, Vol. 34, No. 2, Apr 2004.

[9] Hwee-Xian Tan and Winston K. G. Seah; Framework for Statistical Filtering Against DDOS Attacks in MANETs; Proceedings of the Second IEEE International Conference on Embedded Software and Systems; 2005.

[10] Xianjun Geng and Andrew B. Whinston; Defeating Distributed Denial of Service Attacks; February, 2000.

[11] 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

[12] P. Michiardi, R. Molva, “*Ad hoc networks security,”* IEEE Press Wiley, New York, 2003.

[13] S. Kannan, T. Maragatham, S. Karthik and V.P. Arunachalam; A Study of Attacks, Attack Detection and Prevention Methods in Proactive and Reactive Routing Protocols; International Business Management, 2011.

[14] Neeraj Sharma, B.L. Raina, Prabha Rani et. al “Attack Prevention Methods For DDOS Attacks In MANETS” AJCSIT 1.1 (2011) pp. 18-21.

Mukesh Kumar received his B.Tech in Computer Science from S.K.I.E.T, Kurukshetra in 2010. He is presently pursuing his M.Tech Computer Science & Engineering from U.I.E.T., Kurukshetra University, Kurukshetra. His research interests include Computer Networking, Theory of Computation and Data Structure.

Naresh Kumar received his B.Tech & M.Tech degree in Computer Science & Engineering. He is presently working as Assistant professor in U.I.E.T., Department of Kurukshetra University, Kurukshetra. His research interests are in Computer Networking, Graph theory and Neural network.