

# Review of Detection and Prevention Policies for Distributed Denial of Service Attack in MANET

Preeti, Yogesh Chaba, Yudhvir Singh  
Deptt of CSE, GJUST, Hisar

*Abstract-An ad hoc network is a collection of wireless mobile nodes that forms a temporary network without any centralized administration. While early research effort assumed a friendly and cooperative environment and focused on problems such as wireless channel access and multihop routing, security has become a primary concern in order to provide protected communication between nodes in a potentially hostile environment. 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. In this paper, we have studied the vulnerability of MANETs to DDoS attacks and provide an overview of detection and prevention of DDoS attacks in MANET (Mobile Ad hoc Network).*

## I. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) in [1,3] are multi-hop wireless networks that do not require any central administration or existing infrastructure. All nodes in the

In this paper, we look into various methods for detection and prevention of DDoS attacks. The rest of the paper is organized as follows. The next section discusses the features of MANETs which make them vulnerable to security attacks. In section 3, we show the effects of DDoS on MANETs and next section discusses effects of DDoS attacks on network performance. In section 5, we present various defense mechanisms against DDoS attacks. We conclude in Section 6.

## II SECURITY ISSUES IN MANETS

MANETs are a unique class of wireless multi-hop network comprising of autonomous mobile nodes. This causes the network topology to be dynamically changing, which gives rise to a wide range of characteristics such as transient links, unpredictable resource availability and complex route maintenance. In addition, nodes in MANETs have limited battery life, which is expended by packet transmission and reception. Although security threats exist in both wired and wireless networks, the inherent nature of wireless networks such as MANETs results in them being more vulnerable to attacks. In the following, we describe how some of these MANET features [2] cause the network to be more susceptible to threats.

network act as hosts as well as packet-forwarding routers. The nodes in MANET themselves are responsible for dynamically discovering other nodes to communicate. While such networks have potential commercial viability, the main deployment of MANETs is still mainly for disaster-relief emergencies and military expeditions in hostile terrains. Such applications involving information-retrieval and data sensitive transactions require some level of cyber security to be provided to users. One of the most common forms of security breaches is the Distributed Denial-Of-Service (DDoS) attack. A Distributed Denial of Service (DDoS) attack [4, 5, 6] 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.

- Nodes in MANETs do not have any central base station to coordinate the transmission and authentication of packets. Thus, the delivery of data packets from source to destination nodes in the network is dependent on the cooperation of the (intermediate) nodes in the network.
- The wireless channel in MANETs is a shared broadcast medium, where as in wired scenarios channel can be configured to provide dedicated access to any particular user group. Therefore, nodes in wireless networks are often subject to interference (whether deliberate or not) from neighbouring nodes within the transmission and interference ranges.
- The wireless links that are being used offers little protection towards authentication and confidentiality of data packets. Each transmitted packet can easily be overheard and/or intercepted by all neighbouring nodes, and each node will also inevitably hear all packets that are sent from its neighbours.
- The mobility of the nodes in the network also increases the challenge of node authentication, because nodes can easily venture into and out of the network.

In the literature, there are many proposed mechanisms and protocols that aim to provide security in wired networks, such as via cryptography techniques, data encryption and decryption, shared private/public infrastructures, etc. Compared to wired networks, there are relatively fewer viable solutions for security in wireless networks, particularly MANETs.

Existing work relating to security measures in MANETs typically address the issue of selfish or malicious nodes in the network. A selfish node is one that attempts to make use of its neighbours to forward packets without offering the same services – which could be a measure to conserve its limited battery supply. In contrast, a malicious node is one which may attempt to modify packet information, provide false routing information, impersonate other nodes or even do passive eavesdropping. Some of the proposed methods in the literature include replication and threshold cryptography schemes [8], intrusion detection and response mechanisms [9], use of a fair MAC protocol [10] and secure routing protocols with in-built authentication procedures. However, none of these protocols are very effective against DDoS attacks in MANETs. In the next section, we describe the effects DDoS attacks in MANETs. We will then discuss the various defense mechanisms, in subsequent sections.

### III DDoS ATTACKS IN MANETS

As DDoS attacks are both distributed and denial-of-service attacks [11], they are often large-scale in nature and can greatly deteriorate the performance of the victim network. In a typical DDoS attack, the malicious users first build a network of vulnerable hosts which are used to launch the attack. The vulnerable nodes, known as zombies, are then installed with attack tools, which allow them to carry out attacks under the control of the attacker.

J. Mirkovic and P. Reiher in [12] provide a comprehensive overview of the DDoS problem and design space by proposing taxonomies of DDoS attack and defense mechanisms. There are many proposed methods in the literature which aim to handle DDoS attacks and mitigate their level of damage. Some of these include reactive attack response strategies such as filtering, which allows a certain class of datagrams to pass through while blocking all other datagrams.

In the case of DDoS attacks, its effects are more severe in shared wireless channels because attacks are no longer directed to a single node. Each illegitimate packet that is generated by the attacker may cause collisions at multiple neighbouring nodes as well as nodes within the interference range (which can often be twice as large as the transmission range), resulting in increased retransmissions and contention for channel access.

### IV EFFECT OF DDoS ATTACKS ON NETWORK PERFORMANCE

In this section, we study the performance of the network when it is subject to DDoS attacks. Hwee-Xian Tan and Winston K. G. Seah in [13] consider the case whereby the attackers are compromised hosts in the network, i.e., they will still continue to forward packets for other neighbouring nodes in the network and they do not modify packet contents deliberately. The following performance measures are compared:

- Packet Delivery Ratio (PDR) – number of successfully delivered legitimate packets as a ratio of the number of generated legitimate packets; and
- Average end-to-end delay – average time taken to deliver a legitimate packet successfully from its source to destination.

In paper [13] the effect of DDoS attacks under the following conditions is considered. They are:

- Different attack intensities, which is the rate at which attack packets are being sent as a ratio of the nominal traffic rate. The attack intensity is varied by shortening the interval time which the attacker sends the attack packets.
- Different number of attackers; and
- Different node mobilities.

The network performance does not deteriorate significantly as traffic has not reached saturation point. However, as the attack intensity increases, there are more packets (both legitimate and illegitimate) which compete for channel access in the shared wireless medium. This leads to a drop in the packet delivery ratio and also causes an increase in the delay of the network. Thus, we can predict that as the intensity of the attacks increases, the performance of the network will deteriorate even further.

As the number of attackers varies PDR of the network decreases rapidly when it is subject to attacks. This degradation of the network performance is more significant when the intensity of the attack is increased, and seems to suggest that high attack intensity is more effective than distributed attacks (with greater numbers of attackers).

As node mobility increases, link breakages occur more frequently and lead to route repairs and maintenance. This increases the overhead in the network, thus causing the network performance to deteriorate. However, it is interesting to note that at low or no mobility, the performance of the network does not seem to deteriorate significantly even when under DDoS attacks with an intensity of 5. Therefore, static nodes or nodes with low mobilities may not be very much affected by DDoS attacks (especially if traffic rate is low).

Thus, DDoS attacks can deteriorate the performance of MANETs significantly. Depending on the different attack intensity, number of attacking nodes and node mobility, the impact of these effects can be quite different. And all these shows that higher attack intensity seems to have a greater impact than the increased number of attackers. This could be

attributed to the fact that in wireless medium, there is often spatial reuse of the channel. Therefore, a distributed attacker may be less effective than an aggressive attacker, especially in cases where traffic is not saturated. In addition, attackers are more effective in highly mobile scenarios. This can be attributed to the fact that as node mobility increases, more nodes move into the vicinity of the attacker nodes during packet transmission and/or reception. Hence, effects of DDoS attacks are more pronounced in highly mobile scenarios.

## V DEFENSE MECHANISMS

According to paper [7,14] 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.

### *A Local Solutions*

Protection for individual computers falls into three areas.

1. **Local Filtering:** 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 his 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.

2. **Changing IPs:** A Band-Aid solution to a DDoS attack is to change the victim computer's IP address, thereby invalidating the old address. This action still leaves the computer vulnerable because the attacker can launch the attack at the new IP address. This option is practical because the current type of DDoS attack is based on IP addresses. System administrators must make a series of changes— to domain name service entries, routing table entries, and so on - to lead traffic to the new IP address. Once the IP change—which takes some time—is completed, all Internet routers will have been informed, and edge routers will drop the attacking packets.

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

- ❖ *RSA Security Corp. Client Puzzles:* RSA's Client Puzzles algorithm (see <http://www.rsasecurity.com/rsalabs/staff/ajuels/papers/clientpuzzles.pdf>) requires the attacking computer to correctly solve a small puzzle before establishing a connection. Solving the puzzle consumes some computational power, limiting the attacker in the number of connection requests it can make at the same time.
- ❖ *Turing test:* Software implementing this approach requires the attacking computer to answer a random question before establishing the connection. The question

should be easy for humans to answer but not computers—for example, "Which film won the Oscar for best picture in 2000?"

### *B Global Solutions*

Clearly, as DDoS attacks target the deficiencies of the 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.

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.

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 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.

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, and
- ❖ The hierarchical attacking structure that detaches the control traffic from the attacking traffic, effectively hiding attackers even if the zombie computers are identified.

## CONCLUSIONS

DDoS attacks make a networked system or service unavailable to legitimate users. These attacks are an annoyance at a minimum, or can be seriously damaging if a critical system is the primary victim. Loss of network resources causes economic loss, work delays, and loss of communication between network users. Solutions must be developed to prevent these DDoS attacks.

In this paper, we discussed distributed denial of service attacks on the Internet. We reviewed various security issues in MANET and discussed the effects of distributed denial of service attacks on MANET or network performance. We also discussed various defense mechanisms that could be employed by networks and hosts. It is essential, that as the Internet and Internet usage expand, more comprehensive

solutions and countermeasures to DDoS attacks be developed, verified, and implemented.

#### REFERENCES

- [1] Han L; Wireless Ad hoc Network; October 8, 2004.
- [2] Kamanshis Biswas and Md. Liakat Ali; Security Threats in Mobile Ad Hoc Network; Master Thesis; Thesis no: MCS-2007:07; March 22, 2007.
- [3] Vesa Kärpijoki; Security in Ad Hoc Networks; Helsinki University of Technology; HUT TML 2000.
- [4] 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.
- [5] Felix Lau, Stuart H. Rubin, Michael H. Smith and Ljiljana TrajkoviC; Distributed Denial of Service Attacks; 2275-2280/2004 IEEE.
- [6] Andrim Piskozub; Denial of Service and Distributed Denial of Service Attacks; TCSET 2002; February 18-23, 2002; Lviv – Shavsko, Ukraine.
- [7] Antonio Challita, Mona El Hassan, Sabine Maalouf and Adel Zouheiry; A Survey of DDoS Defense Mechanisms; Department of Electrical and Computer Engineering American University of Beirut; asc04,mhe03,sem05,atz00}@aub.edu.lb.
- [8] L. Zhou and Z. J. Haas, Securing Ad Hoc Networks, IEEE Network Magazine, Special Issue on Network Security, Vol. 13, No. 6, 1999.
- [9] Y. Zhang and W. Lee, Intrusion Detection in Wireless Ad Hoc Networks, Proceedings of the 6th International Conference on Mobile Computing and Networking, Boston, Massachusetts, United States, 2000.
- [10] V. Gupta, S. Krishnamurthy and M. Faloutsos, Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks, Proceedings of the Military Communications Conference (MICOM 2002), California, Oct 2002.
- [11] C. Patrikakis, M. Masikos and O. Zouraraki, Distributed Denial of Service Attacks, The Internet Protocol Journal, Vol. 7, No. 4, Dec 2004.
- [12] 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.
- [13] Hwee-Xian Tan and Winston K. G. Seah; Framework for Statistical Filtering Against DDOS Attacks in MANETs; Proceedings of the Second International Conference on Embedded Software and Systems; 2005 IEEE.
- [14] Xianjun Geng and Andrew B. Whinston; Defeating Distributed Denial of Service Attacks; February 2000.