International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:5, No:1, 2011

Distributed Denial of Service Attacks in Mobile Adhoc Networks

Gurjinder Kaur, Yogesh Chaba, V. K. Jain

***Abstract*—**The aim of this paper is to explore the security issues that significantly affect the performance of Mobile Adhoc Networks (MANET)and limit the services provided to their intended users. The MANETs are more vulnerable to Distributed Denial of Service attacks (DDoS) because of their properties like shared medium, dynamic topologies etc. A DDoS attack is a coordinated attempt made by malicious users to flood the victim network with the large amount of data such that the resources of the victim network are exhausted resulting in the deterioration of the network performance. This paper highlights the effects of different types of DDoS attacks in MANETs and categorizes them according to their behavior.

***Keywords*—**Distributed Denial, Mobile Adhoc Networks

I. Introduction

A mobile adhoc networks operate without any fixed infrastructure and centralized administration. It is an autonomous system of mobile nodes connected by wireless links having capability to operate as host and router as well. As routing functionality is incorporated in mobile nodes, they are capable to discover topology and deliver messages to other nodes themselves. They are fast and easy deployable networks in situations such as military battlefield, emergency rescue, vehicular communications and mining operations where it is not possible to have fixed infrastructure. The dynamic nature of network topology increases the challenges of design of adhoc networks. Mobile ad-hoc networks are defined with the characteristics such as purpose-specific, autonomous and dynamical.

Among all other issues, security is an important and essential requirement in MANET environments. MANETs are more vulnerable to security attacks as compared to wired networks, due to their characteristics such as lack of a centralized authority, easy eavesdropping because of shared wireless medium, dynamic network topology, low bandwidth and battery constraints of mobile devices [1]. Although several types of security attacks in MANETs have been studied in the literature, the most pioneered attack is denial of services attack because of their potential impact and automatic tools are available easily to attack the victim and it is very hard to locate an attacker. The main aim of DDoS is to restrict the system/network to provide the normal services to their intended users by consuming the bandwidth or overload the resources. It generally consists of the concerted efforts of a person or people to degrade legitimate user's service from functioning accurately. Perpetrators of DDoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root name servers. In a DDoS attack an attacker uses multiple source hosts to send attack traffic to one or more victims simultaneously.

In this paper we have explored the all possible types of DDoS attacks that may occur. The paper is organized as follows. Section 2 discusses major phases of attack. In Section 3 classification of DDoS attacks is explained. Finally Section 4 concludes the paper.

Gurjinder Kaur is Assistant Professor with Department Of CSE in SLIET, Longowal, India.
Yogesh Chaba is an Associate Professor with Department Of CSE in GJU, Hisar, India
V. K. Jain is professor in EIE department, SLIET, Longowal.

II. Phases of DDoS Attack

DDoS attacks consist of two major phases [8]:

A. Deployment phase

After finding the vulnerable machines, an attacker installs a DDoS attack tools in one or more vulnerable hosts that are called zombies.

B. Attack phase

An attacker coordinates a attack against a victim by flooding the unwanted data to capture the bandwidth and resources. Both of these phases take advantages of flaws in the design or implementation of applications, protocols, and the Internet architecture [9].

One common method of attack involves saturating the target machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable. In general terms, DDoS attacks are implemented by either forcing the targeted computer(s) to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

III. Types of DDoS Attack

There are two main classes of DDoS attacks: bandwidth depletion and resource depletion attacks.

A. Bandwidth depletion

Bandwidth depletion attack is designed to flood the victim

network with unwanted traffic by sending that prevents legitimate traffic from reaching the victim system. Bandwidth attacks can be divided to flood attacks and amplification attacks.

B. Resource depletion

Resource depletion attack is an attack that is designed to tie up the resources of a victim system. This is done by exploiting the TCP protocol and sending willfully incorrect semantic IP packets to crash the victim system. This type of attack can be divided to protocol exploit attacks and malformed packet attacks [3]. The DDoS attacks can also be classified as follow:

1) Network Device Level: DDOS attacks at the Network Device Level lay more stress to exhaust the hardware resources of network devices or try to take the advantage of loopholes in the software. For example a possible attack on a router can be buffer overrun error in password checking routines by typing extremely long passwords which can cause a router to crash.
2) OS Level: These types of attacks take advantage of the pitfalls left behind by the operating system while implementing the protocols. Common example is ICMP echo requests also called Ping of Death having total data size grater then the IP packet size which can cause certain operating systems to crash, freeze, or reboot due to buffer overflow [4].
3) Application level: The attacks at application level bring down either a service or sometimes the whole system by taking advantage of certain flaws of network applications that are running on the system or by using such applications to withdraw the resources from the system. Most common examples of such attacks are:
   - HTTP flood attacks
   - Mail bombs
   - DNS based attacks, in which attackers flood DNS servers with bogus but well formed requests.
4) Data Flooding: In these types of attacks the attacker transmits the large amount of data to exhaust the recourses of the system or the device. Three categories of this type of attack are:
   - amplification attacks: Smurf attack and Fraggle attack
   - oscillation attacks,
   - simple flooding.
5) Protocol level: DDOS may take advantage of certain standard protocol features, for example several attacks exploit the fact that IP source addresses can be spoofed. The different types of protocol level attacks are [3]:
   - TCP SYN flood where the attacker requests for multiple TCP session initiation, but does not finalize the TCP handshake after the responding by server to the request. Thus these half open TCP sessions consume more memory of victim.
   - PUSH + ACK flood the server with packets such as ACK or PSH/ACK.

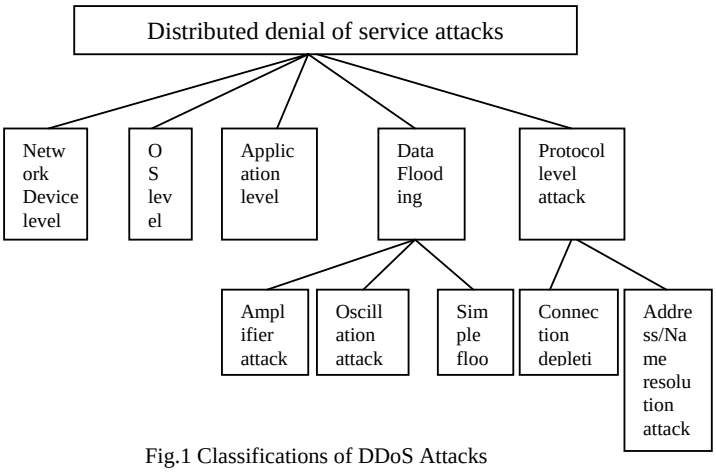

Fig.1 Classifications of DDoS Attacks

IV. Conclusion

The DDoS attacks in MANETs are implemented by taking advantages of the weaknesses of the routing protocols, operating systems and security schemes applied on systems. But the results of these types of attacks may lead to degrade the performance of systems/sites or break the services to legitimate users. To avoid such types of attacks there is need to develop more powerful security schemes and secure routing protocols. In this paper the categories and types of DDoS attacks are classified and the loopholes and weaknesses of which these attacks take advantage of have been elaborated. Still there remain many aspects which need to be explored like mechanism to prevent the DDoS attacks or to make a strategy to avoid them.

References

[1] Hoang Lan Nguyen, Uyen Trang Nguyen "A study of different types of attacks on multicast in mobile ad hoc networks" Ad Hoc Networks vol 6, page no. 32–46, 2008.
[2] Christos Douligeris and Aikaterini Mitrokotsa "DDOS ATTACKS AND DEFENSE MECHANISMS: A CLASSIFICATION
[3] Arun Raj Kumar, P. and S. Selvakumar"Distributed Denial-of-Service (DDoS) Threat in Collaborative Environment- A Survey on DDoS Attack Tools and Traceback Mechanisms" IEEE International Advance Computing Conference (IACC 2009)India, 6-7 March 2009.
[4] Sven Ehlert , Dimitris Geneiatakis , Thomas Magedanz "Survey of network security systems to counter SIP-baseddenial-of-service attacks", journal of computers &Security vol 29, page no. 2 2 5 – 2 4 3 Year 2010.
[5] TAO PENG, CHRISTOPHER LECKIE, and KOTAGIRI RAMAMOHANARAO, "Survey of Network-Based Defense Mechanisms Counteringthe DoS and DDoS Problems". ACM Computing Surveys, Vol. 39, No. 1, Article 3, Year 2007.
[6] Jarmo Mölsä, "Mitigating denial of service attacks: A tutorial" Journal of Computer Security Vol.13 Page no. 807–837 IOS Press , Year 2005.

[7] Charalampos Patrikakis, Michalis Masikos, and Olga Zouraraki, “Distributed Denial of Service Attacks” The Internet Protocol Journal- Vol. 7 no. 4 Dec. 2004.
[8] K.J. Houle, G.M. Weaver, N. Long and R. Thomas, Trends in Denial of Service Attack Technology. CERT Coordination Center, Oct. 2001. [Online] Available: http://www.cert.org/archive/pdf/ DoS_trends.pdf.
[9] J. Mirkovic and P. Reiher, A taxonomy of DDoS attack and DDoS defense mechanisms, ACM SIGCOMMComputer Communication Review 34, vol. 2page no. 39–53, year 2004.