International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 - 5161
©2014 INPRESSCO®, All Rights Reserved
Available at http://inpressco.com/category/ijcet

General Article

Prevention Policy of DDoS

Kanchan[Ȧ*], Jagmohan Singh[Ȧ] and Pavneet Kaur[Ȧ]

[Ȧ]CGC, Landran, India

Accepted 10 May 2014, Available online 01 June 2014, **Vol.4, No.3 (June 2014)**

Abstract

In view of the increasing demand for wireless information and data services, providing faster and reliable mobile access is becoming an important concern. Nowadays, not only mobile phones, but also laptops and PDAs are used by people in their professional and private lives. A mobile ad hoc network (MANET) is a spontaneous network that can be established with no fixed infrastructure. Ad hoc networks have a wide array of military and commercial applications. Security in mobile ad hoc networks is a hard to achieve due to dynamically changing and fully decentralized topology as well as the vulnerabilities and limitations of wireless data transmissions. 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 has 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. In this paper we describe the mechanism for detecting and preventing DDoS in ad hoc network.

Keywords: *DDoS, MANET, AODV*

1. Introduction

1.1Wireless Networking

Wireless networking is an emerging technology that allows users to access information and services electronically, regardless of their geographic position. The use of wireless communication between mobile users has become increasingly popular due to recent performance advancements in computer and wireless technologies. This has led to lower prices and higher data rates, which are the two main reasons why mobile computing is expected to see increasingly widespread use and applications. (Han L, et al, 2004)

There are two distinct approaches for enabling wireless communications between mobile hosts (Vesa Karpijoki, et al, 2000). The first approach is to use a fixed network infrastructure that provides wireless access points. The second approach which is the focus of this thesis research is to form a wireless ad hoc network among users wanting to communicate with each other with no pre-established infrastructure. Laptops and personal digital assistants (PDAs) that communicate directly with each other are examples of nodes in an ad hoc network.

1.2 Mobile Adhoc Network

A Mobile Ad Hoc Network (MANET) consists of a set of mobile hosts that carry out basic networking functions like packet forwarding, routing, and service discovery without the help of an established infrastructure (Han L, et al, 2004). Nodes of an ad hoc network rely on one another in forwarding a packet to its destination, due to the limited range of each mobile host's wireless transmissions.

1.3 Mobile Ad hoc Networks' Usages

Wireless ad-hoc networks can be deployed in areas where a wired network infrastructure may be undesirable due to reasons such as cost or convenience. It can be rapidly deployed to support emergency requirements, short-term needs, and coverage in undeveloped areas. So there is a plethora of applications for wireless ad-hoc networks. As a matter of fact, any day-to-day application such as electronic email and file transfer can be considered to be easily deployable within an ad hoc network environment. Some well-known ad hoc network applications are:

- Collaborative Work: for some business environments, the need for collaborative computing might be more important outside office environments than inside.
- Crisis-management Applications: these arise, for example, as a result of natural disasters where the entire communications infrastructure is in disorder. Restoring communications quickly is essential. By using ad hoc networks, a communication channel could be set up in hours instead of days/weeks required for wire-line communications.

Personal Area Networking and Bluetooth: a personal area network (PAN) is a short- range, localized network where nodes are usually associated with a given person. These nodes could be attached to someone's pulse watch, belt, and so on. (Sugata Sanyal)

*Corresponding author: **Kanchan**

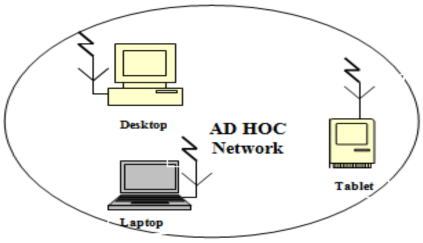

Figure 1: AdHoc Network

1.4 Security Goals for Manets

- Availability
- Confidentiality
- Integrity
- Authentication
- Non-repudiation Access and usage control

1.5Attacks in Manet

Various types of attacks in MANETs are: Modification, Impersonation, Fabrication, Eavesdropping, Replay, Denial of Service, Malicious Software and Lack of Cooperation. Denial of Service attack is described below.

Distributed Denial of Service (DDoS) Attack

- *DoS Attack*

A denial of service (DoS) attack is characterized by an explicit attempt by an attacker to prevent legitimate users of a service from using the desired resources (Sugata Sanyal). Examples of denial of service attacks include:

- Attempts to "flood" a network, thereby preventing legitimate network traffic
- Attempts to disrupt connections between two machines, thereby preventing access to a service
- Attempts to prevent a particular individual from accessing a service
- Attempts to disrupt service to a specific system or person.
- *DDoS Attack*

A DDoS (Distributed Denial-Of-Service) attack is a distributed, large-scale attempt by malicious users to flood the victim network with an enormous number of packets (Stephen M.Specht, et al, 2004). 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. The following steps take place during a distributed attack

- The real attacker sends an "execute" message to the control master program.
- The control master program receives the "execute" message and propagates the command to the attack daemons under its control.
- Upon receiving the attack command, the attack daemons begin the attack on the victim.

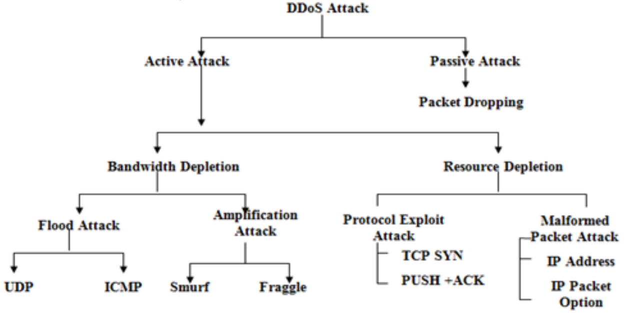

Figure 2: DDoS Attack Taxonomy

1.6 Routing Protocols in Manets

The routing protocols in adhoc networks may be categorized as proactive routing protocols, reactive routing protocols, and hybrid routing protocols.

- Proactive Routing Protocols are those protocols, in which the routes are maintained to all the nodes, including those nodes to which packets are not sent.
- Reactive Routing Protocols are those protocols in which the route between the two nodes is constructed only when the communication occurs between the two nodes.
- Hybrid Routing Protocols are those protocols in which the combined approach of proactive routing and reactive routing are used for the route generation between the nodes.

2. Review of Literature

2.1 Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures (Stephen M.Specht,et al, 2004)

Stephen M. Specht et al. describe that Distributed Denial of Service (DDoS) attacks have become a large problem for users of computer systems connected to the Internet. DDoS attackers hijack secondary victim systems using them to wage a coordinated large-scale attack against primary victim systems. As new countermeasures are developed to prevent or mitigate DDoS attacks, attackers are constantly developing new methods to circumvent these new countermeasures.

2.2 Distributed Denial of Service Attacks (Felix Lau, Straut H.Rubin, Michael H. Smith, et al, 2004)

Felix Lau *et al.* present Distributed Denial of Service attacks in the Internet. They were motivated by the widely known February 2000 distributed attacks on Yahoo!, Amazon.com, CNN.com, and other major Web sites. A denial of service is characterized by an explicit attempt by anattacker to prevent legitimate users from using resources. An attacker may attempt to: "flood" a network and thus reduce a legitimate user's bandwidth, prevent access to a service, or disrupt service to a specific system or a user. This paper gives information about methods and techniques used in denial of service attacks, and list possible defenses.

2.3 Defeating Distributed Denial of Service Attacks (XianjunGeng, Andrew B.Whinston, et al, 2000)

XianjunGeng et al. describe that the notorious, crippling attack on e-commerce’s top companies in February 2000 and the recurring evidence of active network scanning—a sign of attackers looking for network weaknesses all over the Internet—are harbingers of future Distributed Denial of Service (DDoS) attacks. They signify the continued dissemination of the evil daemon programs that are likely to lead to repeated DDoS attacks in the foreseeable future. This paper gives information about network weaknesses that DDoS attacks exploit the technological futility of addressing the problem solely at the local level, potential global solutions, and why global solutions require an economic incentive framework.

2.4Resisting Malicious Packet Dropping In Wireless Ad Hoc Networks (Mike Just, Evangelos Kranakis and Tao Wan, et al)

Mike Just et al. mention that most of the routing protocols in wireless ad hoc networks, such as DSR, assume nodes are trustworthy and cooperative. This assumption renders wireless ad hoc networks vulnerable to various types of Denial of Service (DoS) attacks. This paper presents a distributed probing technique to detect and mitigate one type of DoS attacks, namely malicious packet dropping, in wireless ad hoc networks. A malicious node can promise to forward packets but in fact fails to do so. In this distributed probing technique, every node in the network will probe the other nodes periodically to detect if any of them fail to perform the forwarding function.

3. **Problems and Goal**

3.1 Problem Statement

- Very little has been done to compare, contrast, and categorize the different ideas related to DDoS attacks and defenses. As a result it is difficult to understand what a computer network user needs to do and why to prevent the threat from DDoS attacks.
- There are no effective defense mechanisms against many important DDoS attack types.
- There is no guidance on how to select defense mechanisms.
- Existing defense mechanisms have been evaluated according to very limited criteria. Often relevant risks have been ignored or evaluations have been carried out under ideal conditions. No research publications exist for giving a systematic list of issues related to defense evaluation

3.2 Proposed Goal

The main goals of this paper are:

- To measure network performance which include parameters like first packet received at [s], last packet received at [s], total number of collisions, total number of bytes received, total number of packets received and total energy consumption etc.
- Study the effect of Distributed Denial of Service (DDoS) attacks under different number of attackers and different node mobility.
- To measure impact of Distributed Denial of Service (DDoS) attacks on network performance.
- Detection of Distributed Denial of Service attacks in Mobile Ad-hoc Network.
- Prevention of Distributed Denial of Service attacks in Mobile Ad-hoc Network using defense techniques.

4. Simulation Environment

Three well-known simulators are used for MANET simulations: NS-2, GloMoSim and OPNET. We chose GloMoSim, because it is a scalable simulator that was designed especially to large wireless networks. It supports thousands of nodes, using parallel and distributed environment.

4.1 Glomosim Overview

GloMoSim stands for Global Mobile information systems Simulation library, was designed as a set of library modules, each of which simulates a communication protocol in the protocol stack. The library uses the OSI layer approach and supports multiple protocols in each layer:

Table 1: GloMoSim OSI Library

Layer	**Model**
Physical	Free-space, Two-ray
Data Link	CSMA, MACA, 802.11, TSMA
Network	Bellman-Ford, FISHEYE, WRP, AODV ,DSR ,LAR1 ,ODMPR
Transport	TCP, UDP
Application	CBR, HTTP, TELNET, FTP

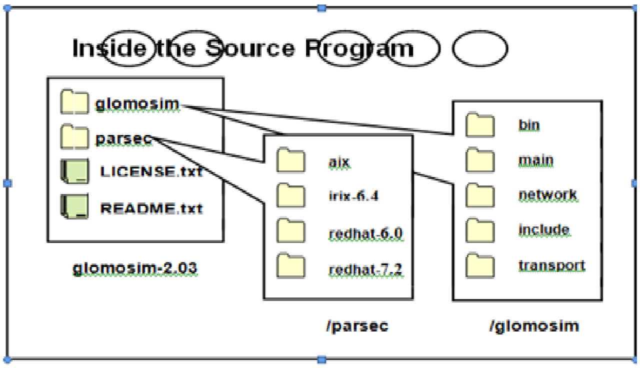

Figure 3: Basic structure of source directory

4.2 Detail of Input File

Application .Config (app .conf) File

Application (config) file is used to generate the traffic for the simulation i.e. to specify the number of packets, source, destination and the duration of transmission. The version of GloMoSim, which we are using now, provides the facility to use the following traffic generators:
FTP: FTP uses tcplib to simulate the file transfer protocol. In order to use FTP, the following format is needed:

FTP <src><dest><items to send><start time>
Where
<src> is the client node.
<dest> is the server node.
<items to send> is how many application layer items to send.
<start time> is when to start FTP during the simulation.
If <items to send> is set to 0, FTP will use tcplib to randomly determine the amount of application layer items to send. The size of each item will always be randomly determined by tcplib. Note that the term "item" in the application layer is equivalent to the term "packet" at the network layer and "frame" at the MAC layer.

Example

a) FTP 0 1 10 0S
Node 0 sends node 1 ten items at the start of the simulation, with the size of each item randomly determined by tcplib.

4.3 Config.in File

During the simulation, config.in is used as a input file, which specifies various parameters to be used.

5. Mechanism for DDoS

5.1 Malicious Packet Dropping Based DDoS Attack Mechanism

Malicious packet dropping attack presents a new threat to wireless ad hoc networks since they lack physical protection and strong access control mechanism.

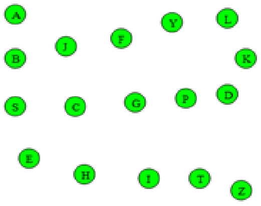

Figure 4: Nodes in the Network.

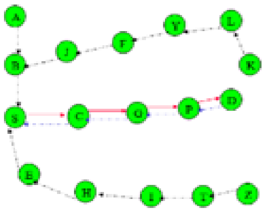

Figure 5: Route from node S to node D.

An adversary can easily join the network or capture a mobile node and then starts to disrupt network communication by silently dropping packets. It is also a threat to the Internet since the various software vulnerabilities would allow attackers to gain remote control of routers on the Internet. If malicious packet dropping attack is used along with other attacking techniques, such as shorter distance fraud, it can create more powerful attacks i.e. black hole which may completely disrupt network communication. Now let us illustrate malicious packet dropping with an example. Suppose we want to send packets from node S to node D in the network shown in Figure 4,5.
S → C → G → P → D

In case of malicious packet dropping based DDoS attack, suppose node G becomes malicious and because of attack on node G, it does not forward the packets to node P. There is a path from node S to node D, and there is no congestion in the network, still node D does not receives the packet because of malicious node G shown in Figure 6.

Current network protocols do not have the capability to detect the malicious packet dropping attack. Network congestion control mechanisms do not apply here since packets are not dropped due to congestion. Link layer acknowledgment, such as IEEE 802.11 MAC protocol, can detect link layer break, but cannot detect forwarding level break. Although upper layer acknowledgment, such as TCP ACK, allows for detecting end-to end communication break, it can be inefficient and it does not indicate the node at which the communication breaks. Moreover such mechanism is not available in connectionless transport layer protocols, such as UDP. Therefore, it is important to develop mechanisms to render networks the robustness for resisting the malicious packet dropping attack.

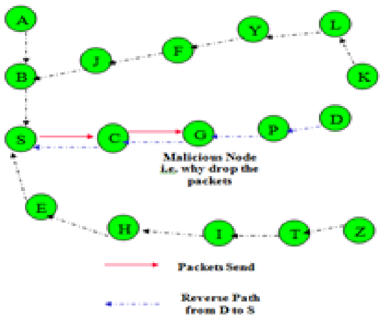

Figure 6: Malicious Packet Dropping Attacks.

5.2 Flooding Based Ddos Attack Mechanisms

Flooding-based DDoS attacks involve agents or reflectors sending a large volume of unwanted traffic to the victim (Bo-CangPeng , Chiu-Kuo Liang). The victim will be out of service for legitimate traffic because its connection resources are used up. Common connection resources include bandwidth and connection control in the victim system. Generally, flooding-based DDoS attacks consist of two types: direct and reflector attacks (Bo-CangPeng , Chiu-Kuo Liang). Figure 7 is another view of the process of a direct flooding-based DDoS attack.

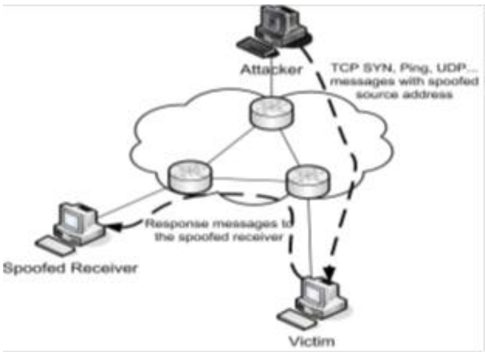
Attacker
TCP SYN, Ping, UDP... messages with spoofed source address
Response messages to the spoofed receiver
Spoofed Receiver
Victim

Figure 7: A direct flooding-based DDoS attack.

Direct attacks usually choose three mechanisms: TCP SYN flooding, ICMP echo flooding, and UDP data flooding (Yi-an Huang, Wenke Lee, et al). The TCP SYN flooding mechanism is different from the other two mechanisms. It causes the victim to run out of all available TCP connection control resources by sending a large number of TCP SYN packets. The victim cannot accept a new connection from a legitimate user without new available control resources. ICMP echo flooding-based attacks will consume all available bandwidth as a large number of ICMP ECHO REPLY packets arrive at the victim.

5.3 Detection Of Malicious Packet Dropping Based Ddos Attack

Unconditional Packet Dropping**:** Monitor the statistics FP (Forward Percentage) over a sufficiently long time period T.

$$FPm = \frac{PacketActuallyForward}{PacketToBeForwarded} = \frac{\#T(m,M) - \#T([m],M)}{\#T(M,m) - \#T(M,[m])}$$

FP determines the ratio of forwarded packets over the packets that are transmitted from M to m and that m should forward. If the denominator is not zero and $FP_i = 0$, the attack is detected as Unconditional Packet Dropping and m is identified as the attacker.

Malicious Flooding on specific target

Monitor the total number of $\#T_{([m],[d])}$ over a period of time T for every destination d. If it is larger than threshold MaxCount, the attack is a Malicious Flooding. Selective (Random) Packet Dropping**:** Monitor the statistics LFP (Local Forward Percentage) over a sufficiently long time period T for each sources.

$$LFPm = \frac{PacketFromSourceActuallyBeingForward}{PacketFromSourceToBeForwarded}$$
$$= \frac{\#T([s],m,M)}{\#T([s],M,m) - \#T([s],M,[m])}$$

5.4 Prevention of Flooding Based DDoS Attack

Existing Prevention Techniques

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.

5.5 Proposed Prevention Technique

Disabling IP Broadcasts: A broadcast is a data packet that is destined for multiple hosts. Broadcasts can occur at the data link layer and the network layer. Data-link broadcasts are sent to all hosts attached to a particular physical network. Network layer broadcasts are sent to all hosts attached to a particular logical network. The Transmission Control Protocol/Internet Protocol (TCP/IP) supports the following types of broadcast packets:

- All ones: By setting the broadcast address to all ones (255.255.255.255), all hosts on the network receive the broadcast.
- Network: By setting the broadcast address to a specific network number in the network portion of the IP address and setting all ones in the host portion of the broadcast address, all hosts on the specified network receive the broadcast. For example, when a broadcast packet is sent with the broadcast address of 131.108.255.255, all hosts on network number 131.108 receive the broadcast.
- Subnet: By setting the broadcast address to a specific network number and a specific subnet number, all hosts on the specified subnet receive the broadcast. For example, when a broadcast packet is set with the broadcast address of 131.108.4.255, all hosts on subnet 4 of network 131.108 receive the broadcast.

5.6 Advantages Of The Proposed Scheme

- The proposed scheme incurs no extra overhead, as it makes minimal modifications to the existing data structures and functions related to blacklisting a node in the existing version of pure AODV.
- Also the proposed scheme is more efficient in terms of its resultant routes established, resource reservations and its computational complexity.
- If more than one malicious node collaborate, they too will be restricted and isolated by their neighbors, since they monitor and exercise control over forwarding RREQs by nodes. Thus the scheme successfully prevents DDoS attacks.

Conclusion

Detection & Prevention of DDoS attacks is a part of an overall risk management strategy for an organization. Each organization must identify the most important DDoS risks, and implement a cost-effective set of defense mechanisms against those attack types causing the highest risk for business continuity. Studies and news about real-life DDoS attacks indicate that these attacks are not only among the most prevalent network security risks, but that these attacks can also block whole organizations out of the Internet for the duration of an attack. References

References

Han L (2004), Wireless Ad hoc Network.

Kamanshis Biswas and Md. Liakat Ali (2007), Security Threats in Mobile Ad Hoc Network, Master Thesis,Thesis no: MCS-2007:07.

VesaKärpijoki (2000), Security in Ad Hoc Networks, Helsinki University of Technology,HUT TML.

Stephen M. Specht and Ruby B. Lee (2004), 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.

Felix Lau, Stuart H. Rubin, Michael H. Smith and LjiljanaTrajkoviC (2004) Distributed Denial of Service Attacks, 2275-2280/2004 IEEE.

AndrimPiskozub; Denial of Service and Distributed Denial of Service Attacks (2002) TCSET 2002,Lviv – Shavsko, Ukraine.

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.

Hwee-Xian Tan and Winston K. G. Seah (2005) Framework for Statistical Filtering Against DDOS Attacks in MANETs, Proceedings of the Second International Conference on Embedded Software and System.

XianjunGeng and Andrew B. Whinston (2000) Defeating Distributed Denial of Service Attacks.

Q. Li, E-C. Chang and M. C. Chan (2005), On the Effectiveness of DDoS Attacks on Statistical Filtering; Proceedings of the 24th Annual Conference of the IEEE Communications Society (INFOCOM 2005), Miami.

Yi-an Huang and Wenke Lee, A Cooperative Intrusion Detection System for Ad Hoc Networks; www.cc.gatech.edu/~wenke/papers/sasn.pdf.

SugataSanyal, Ajith Abraham, DhavalGada, RajatGogri, PunitRathod, ZalakDedhia and NiraliMody, Security Scheme for Distributed DoS in Mobile Ad Hoc Networks; www.softcomputing.net/iwdc-manet.pdf.

Mike Just, EvangelosKranakis and Tao Wan; Resisting Malicious Packet Dropping in Wireless Ad-HocNetworks,www.scs.carleton.ca/~kranakis/Papers/adhocnow03.pdf.

Bo-CangPeng and Chiu-Kuo Liang, Prevention Techniques for Flooding Attacks in Ad Hoc Networks,explore.ieee.org/iel5/9755/30769/01425219.pdf.