Truth of D-DoS Attacks in MANET

Gaurav Kumar Gupt[1], Mr. Jitendra Singh[2]

GJCST Classification
I.2.3, C.2.0

***Abstract*-Network security is a weak link in wired and wireless network systems. Malicious attacks have caused tremendous loss by impairing the functionalities of the computer networks. Denial of Service (DoS) and Distributed DoS (DDoS) attacks are two of the most harmful threats to the network functionality. Mobile Ad Hoc Networks (MANET) are even more vulnerable to such attacks.. Denial of Service (DoS) is the degradation or prevention of legitimate use of network resources. The wireless ad hoc network is particularly vulnerable to DoS attacks due to its features of open medium, dynamic changing topology,cooperative algorithms, decentralization of the protocols, and lack of a clear line of defense is a growing problem in networks today. Many of the defense techniques developed on a fixed wired network are not applicable to this new mobile environment. How to thwart the DoS attacks differently and effectively and keep the vital security-sensitive ad hoc networks available for its intended use is essential.**

Background -This research work concentrates on developing defense mechanism against certain types of DoS attacks in the Ad Hoc network environment

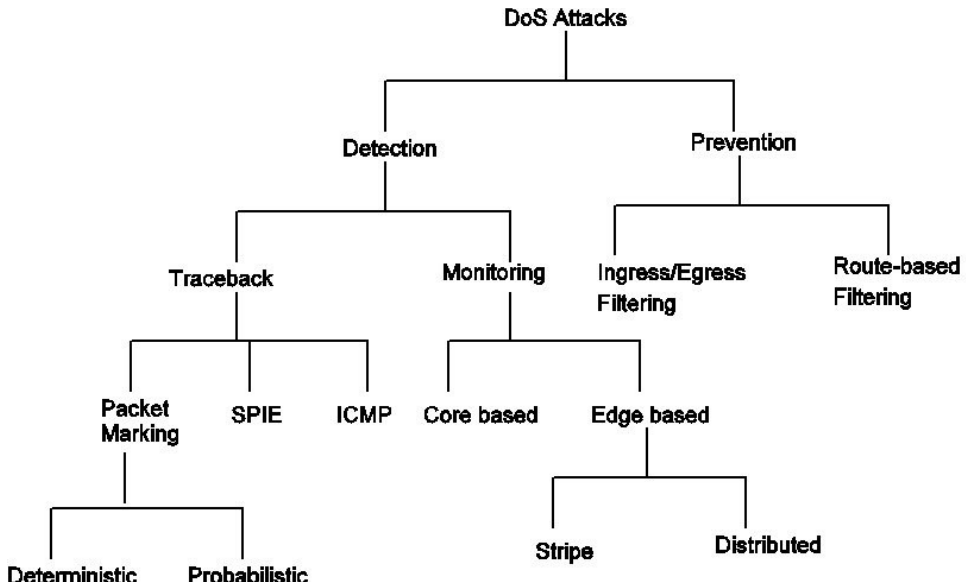
HOW THEY WORK

To give a very simple example, let us assume that there is already a small ad-hoc network in place. When a new node in this example it can be the PDA of Tom joins the ad-hoc network, there are a number of things to do: The device needs to set up contact to other nodes in range, telling them: I am here. By this, the new node learns who the neighbour nodes are, and vice versa. Another point is that the new node, in this example the PDA, needs a unique identifier to make it addressable an IP address in IP networks. For all this, the new node is on its own, as there is neither a central controlling entity nor a pre-existing fixed infrastructure in adhoc networks. When Tom wants to send a message from his PDA to that of Maria, other nodes serve as a relay station in a process called multi-hop routing, if the PDA of Maria is not in direct reach, using one of the routing protocols designed for ad-hoc networks. This small example shows a few imminent advantages of ad-hoc networks: They can extend the range of the wireless technology in use, e.g. WLAN or Bluetooth, they can reduce the nodes power consumption due to a lower transmission power required, and they increase the nodes mobility. To make this work, though, ad-hoc networks require a critical mass of well-behaving nodes, willing to forward others traffic.

About[1] -Department:Computer science Srm university (Mtech (cse) student) E-mail-gauravkumarblack@yahoo.coml.com
About[2]-Department:Computer science Srm university E-mail:jitendra.jit@gmail.com

I. INTRODUCTION

An ad hoc network is a collection of wireless mobile nodes that forms a temporary network without any centralized administration. In such an environment, it may be necessary for one mobile node to enlist other hosts in forwarding a packet to its destination due to the limited transmission range of wireless network interfaces. Each mobile node operates not only as a host but also as a router forwarding packets for other mobile nodes in the network that may not be within the direct transmission range of each other. Each node participates in an ad hoc routing protocol that allows it to discover multihop paths through the network to any other node. This idea of Mobile ad hoc network is also called infrastructureless networking, since the mobile nodes in the network dynamically establish routing among themselves to form their own network on the fly. So, Mobile Ad Hoc Network (MANET) is a collection of communication devices or nodes that wish to communicate without any fixed infrastructure and pre-determined organization of available links. The nodes in MANET themselves are responsible for dynamically discovering other nodes to communicate.Now-a-days, Mobile ad hoc network (MANET) is one of the recent active fields and has received marvelous attention because of their self-configuration and selfmaintenance capabilities. 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.



SECURITY GOALS:For analyzing the security of wireless mobile adhoc networks, we need certain parameters. The basic parameters for a secure system are:

- Availability
- Confidentiality
- Authentication
- Integrity
- Non-repudiation
- Scalability

II. SECURITY ATTACKS IN MANETS

The security attacks in MANETs can be categorized as active attacks and passive attacks. Active attack is an attack when misbehaving node has to bear some energy costs in order to perform the threat. On the other hand, passive attacks are mainly due to lack of cooperation with the purpose of saving energy selfishly. Nodes that perform active attacks with the aim of damaging other nodes by causing network outage are considered as malicious while nodes that make passive attacks with the aim of saving battery life for their own communications are considered to be selfish. 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. Network Protocol Stack Based Attack Classification

Stack Layer	Attacks
Application	Backdoor, Virus, Data corruption or deletion, Repudiation
Transport	Desynchronization, Session hijacking, SYN flooding
Network	Blackhole, Byzantine, Flooding, Location disclosure, Misdirection, packet dropping, Resource consumption (Sleep deprivation), Rushing, Selfish, Spoofing, Wormhole
Link	Collision, Disruption MAC (802.11), Exhausting, Monitoring (Traffic analysis), Unfairness, WEP weakness
Physical	Eavesdropping, Interceptions, Jamming, Tampering
Multi-layer attacks	DoS, impersonation, replay, man-in-the-middle

Attacks could also be classified according to the target layer in the protocol stack

III. DENIAL OF SERVICE (DOS)

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. 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.

IV. DISTRIBUTED DENIAL OF SERVICE ATTACK(DDOS)

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. 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 distributed format adds the "many to one" dimension that makes these attacks more difficult to prevent. A distributed denial of service attack is composed of four elements, as shown in Figure 1.First, it involves a victim, i.e., the target host that has been chosen to receive the brunt of the attack. Second, it involves the presence of the attack daemon agents. These are agent programs that actually conduct the attack on the target victim. Attack daemons are usually deployed in host computers. These daemons affect both the target and the host computers.

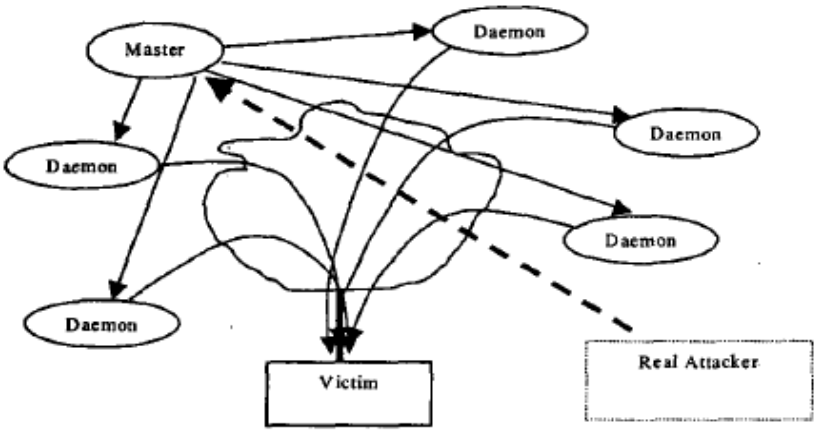


Figure 1: The four components of a distributed denial of service attack: a real attacker, a control master program, attack daemons and the victim

The task of deploying these attack daemons requires the attacker to gain access and infiltrate the host computers. The third component of a distributed denial of service attack is the control master program. Its task is to coordinate the attack. Finally, there is the real attacker, the mastermind behind the attack. By using a control master program, the real attacker can stay behind the scenes of the attack. 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.

V. DEFENSE MECHANISMS

We classify defense mechanisms to DDoS attacks 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.

VI. 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*

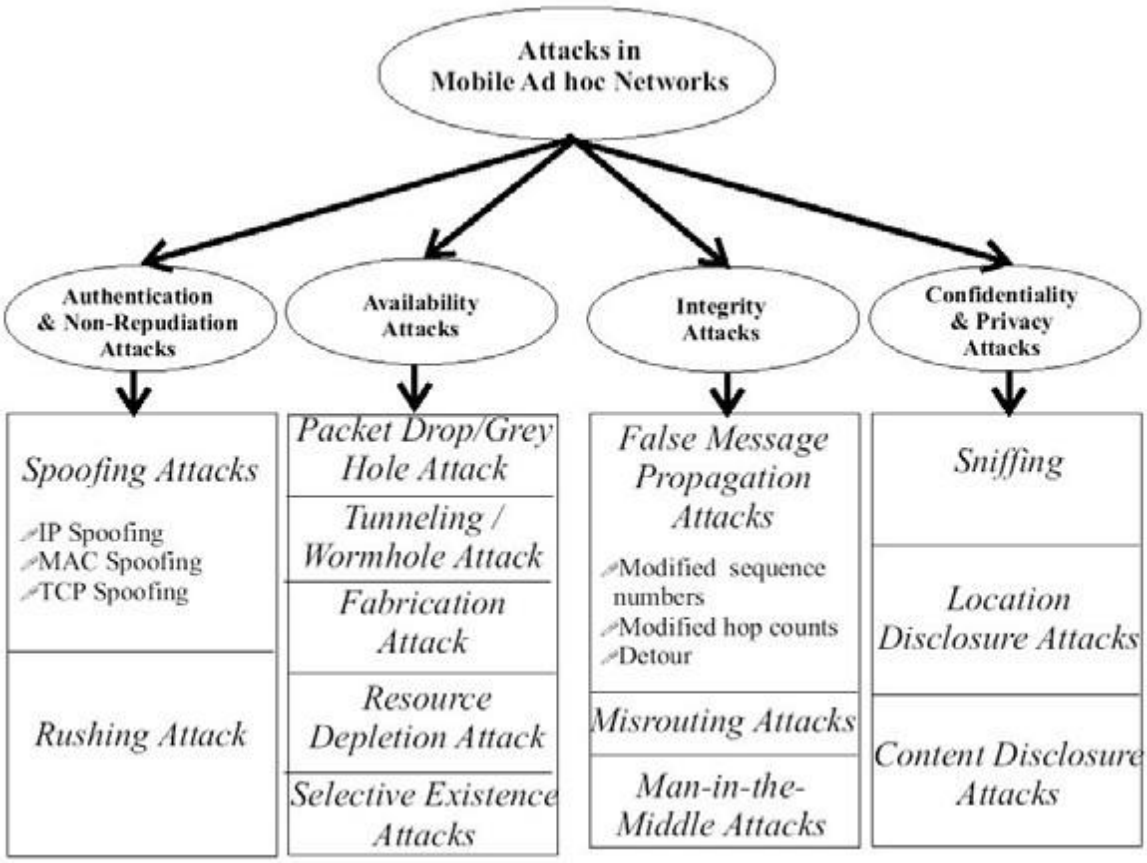
A Band-Aid solution to a DDoS attack is to change the victim computer's IP address, thereby invalidating the old address. This action still leaves the computer vulnerable because the attacker can launch the attack at the new IP address. This option is practical because the current type of DDoS attack 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/c lientpuzzles.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?"

Attacks in MANET



VII. 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

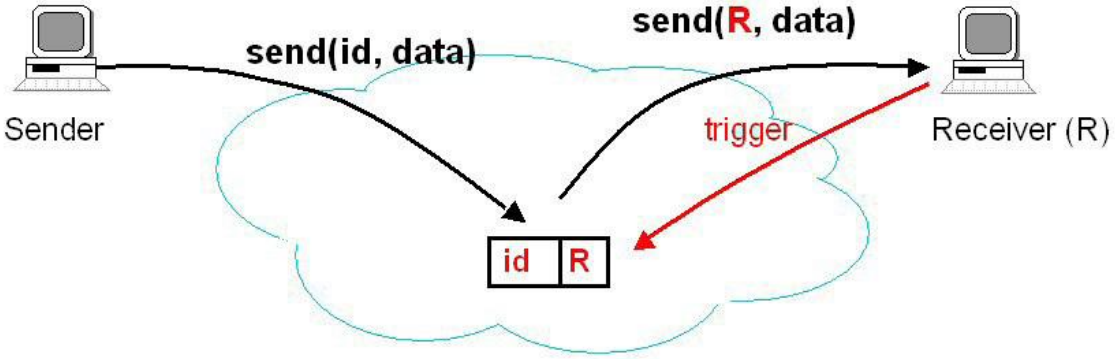
- The hierarchical attacking structure that detaches the control traffic from the attacking traffic, effectively hiding attackers even if the zombie computers are identified.

VIII. REVIEW

This section gives a brief overview of the. The contents of this are all about the various related to mobile ad hoc network, distributed denial of service attack and defense against this attack.

1) *Wireless Ad hoc Networks*

Lu Han describes [1] that the wireless ad hoc networks were first deployed in 1990's, Mobile Ad-hoc networks have been widely researched for many years. Mobile Ad-hoc Networks are collection of two or more devices equipped with wireless communications and networking capability. These devices can communicate with other nodes that immediately within their radio range or one that is outside their radio range. For the later, the nodes should deploy an intermediate node to be the router to route the packet from source toward destination. The Wireless Ad-hoc Networks do not have gateway, every node can act as the gateway. As per this paper, although, lots of research has been done on this particular field, it has often been questioned as to whether the architecture of Mobile Ad-hoc Networks is a fundamental flawed architecture. The main reason for the argument is that Mobile Ad-hoc Networks are not much used in practice, almost every wireless network nodes communicate to base station and access points instead of cooperating to forward packets hop-by-hop. As per the contents of this paper the key technologies to Wireless Adhoc Networks were not implemented as we expect. That is to say, many problems are inherently unsolvable.



2) *Security Threats In Mobile ad-hoc Networks*

Kamanshis Biswas and Md. Liakat Ali describes [2] that Mobile Ad Hoc Network (MANET) is a collection of communication devices or nodes that wish to communicate without any fixed infrastructure and pre-determined organization of available links. The nodes in MANET themselves are responsible for dynamically discovering other nodes to communicate. Although the ongoing trend is to adopt ad hoc networks for commercial uses due to their certain unique properties, the main challenge is the vulnerability to security attacks. A number of challenges like open peer-to-peer network architecture, stringent resource constraints, shared wireless medium, dynamic network topology etc. are posed in MANET. As MANET is quickly spreading for the property of its capability in forming temporary network without the aid of any established infrastructure or centralized administration, security challenges has become a primary concern to provide secure communication. This paper gives information about various security threats an ad-hoc network faces, the security services required to be achieved and the countermeasures for attacks in each layer. As per the contents of this paper, secure routing protocol is still a burning question. There is no general algorithm that suits well against the most commonly known attacks such as wormhole, rushing attack etc. In short, we can say that the complete security solution requires the prevention, detection and reaction mechanisms applied in MANET.

3) *Security In Ad-hoc Networks*

Vesa Kärpijoki describes [3] that in ad hoc networks the communicating nodes do not necessarily rely on a fixed infrastructure, which sets new challenges for the necessary security architecture they apply. In addition, as ad hoc networks are often designed for specific environments and may have to operate with full availability even in difficult conditions, security solutions applied in more traditionalnetworks may not directly be suitable for protecting them. A short literature study over papers on ad hoc networking shows that many of the new generation ad hoc networking proposals are not yet able to address the security problems and they face. Environment-specific implications on the required approaches in implementing security in such dynamically changing networks have not yet fully realized.

4) *Distributed Denial of Service:*

Taxonomies of Attacks, Tools and Countermeasures Stephen M. Specht and Ruby B. Lee describe [4] 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. This paper gives us information about DDoS attack models and proposed taxonomies to characterize the scope of DDoS attacks, the characteristics of the software attack tools used, and the countermeasures available. These taxonomies illustrate similarities and patterns in different DDoS attacks and tools, to assist in the development of more generalized solutions to countering DDoS attacks, including new derivative attacks. It is essential, that as the Internet and Internet usage expand, more comprehensive solutions and countermeasures to DDoS attacks be developed, verified, and implemented.

5) *Distributed Denial of Service Attacks*

Felix Lau, Stuart H. Rubin, Michael H. Smith and Ljiljana TrajkoviC describe [5] 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 an attacker 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. In this paper, distributed denial of service attack is simulated using ns-2 network simulator. This paper gives information about how various queuing algorithms implemented in a network router perform during an attack, and whether legitimate users can obtain desired bandwidth. In short, simulation results indicate that implementing queuing algorithms in network routers may provide the desired solution in protecting users in cases of distributed denial of service attacks.

6) *Denial of Service and Distributed Denial of Service Attacks*

Andrim Piskozub describes [6] main types of DoS attacks which flood victim's communication channel bandwidth, is carried out their analysis and are offered methods of protection from these attacks.

7) *A Survey of DDoS Defense Mechanisms*

Antonio Challita, Mona El Hassan, Sabine Maalouf and Adel Zouheiry describe [7] different types of DDoS attacks, present recent DDoS defense methods as published in technical papers, and propose a novel approach to counter DDoS. Based on common defense principles and taking into account the different types of DDoS attacks, this paper survey defense methods and classify them according to several criteria. This paper propose a simple-to-integrate DDoS victim based defense method, Packet Funneling, which aims at mitigating an attack's effect on the victim. In this approach, heavy traffic is "funneled" before being passed to its destination node, thus preventing congestion at the node's access link and keeping the node on-line. This method is simple to integrate, requires no collaboration between nodes, introduces no overhead, and adds slight delays only in case of heavy network loads. The proposed packet funneling approach promises to be a suitable means of coping with DDoS traffic, with easy integration at minimal cost

8) *Framework for Statistical Filtering Against*

DDoS Attacks in MANETs Hwee-Xian Tan and Winston K. G. Seah describes [8] that 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. 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. There are many proposed methods in the literature which aim to alleviate this problem; such as hop-count filtering, rate-limiting and statistical filtering. However, most of these solutions are meant for the wired Internet, and there is little research efforts on mechanisms against DDoS attacks in wireless networks such as MANETs. This paper gives information about the vulnerability of MANETs to DDoS attacks and provide an overview of statistical filtering, which is commonly used as a security mechanism against DDoS attacks in wired networks and then propose a framework for statistical filtering in MANETs to combat DDoS attacks. This paper also simulates some DDoS attacks in MANETs without any filtering mechanisms to explore and understand the effects of such attacks on the performance of the network.

9) *Defeating Distributed Denial of Service Attacks*

Xianjun Geng and Andrew B. Whinston describes [9] 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.

10) *On the Effectiveness of DDoS Attacks on Statistical Filtering*

Qiming Li, Ee-Chien Chang and Mun Choon Chan describes [10] that Distributed Denial of Service (DDoS) attacks pose a serious threat to service availability of the victim networkby severely degrading its performance. There has been significant interest in the use of statistical-based filtering to defend against and mitigate the effect of DDoS

attacks. Under this approach, packet statistics are monitored to classify normal and abnormal behaviour. Under attack, packets that are classified as abnormal are dropped by the filter that guards the victim network. This paper gives the effectiveness of DDoS attacks on such statistical-based filtering in a general context where the attackers are "smart". We first give an optimal policy for the filter when the statistical behaviours of both the attackers and the filter are static. Next, this paper considers cases where both the attacker and the filter can dynamically change their behavior, possibly depending on the perceived behavior of the other party. This paper observes that while an adaptive filter can effectively defend against a static attacker, the filter can perform much worse if the attacker is more dynamic than perceived.

IX. CHALLENGES IN MANETS

- MANETs face challenges in secure communication. For example the resource constraints on nodes in ad hoc networks limit the cryptographic measures that are used for secure messages. Thus it is susceptible to link attacks ranging from passive eavesdropping to active impersonation, message replay and message distortion.
- Mobile nodes without adequate protection are easy to compromise. An attacker can listen, modify and attempt to masquerade all the traffic on the wireless communication channel as one of the legitimate node in the network.
- Static configuration may not be adequate for the dynamically changing topology in terms of security solution. Various attacks like DoS (Denial of Service) can easily be launched and flood the network with spurious routing messages through a malicious node that gives incorrect updating information by pretending to be a legitimate change of routing information.
- Lack of cooperation and constrained capability is common in wireless MANET which makes anomalies hard to distinguish from normalcy.
- In general, the wireless MANET is particularly vulnerable due to its fundamental characteristics of open medium, dynamic topology, and absence of central authorities, distribution cooperation and constrained capability.

X. PROBLEMS DUE TO DOS/DDOS ATTACKS

- A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users.
- The bandwidth of a router between the Internet and a LAN may be consumed by DoS, compromising not only the intended computer, but also the entire network.
- Slow network performance (opening files or accessing web sites) due to Distributed Denial of Service attacks.
- Unavailability of a particular web site due to Distributed Denial of Service attacks.
- Inability to access any web site due to Distributed Denial of Service attacks.
- Dramatic increase in the number of spam emails received due to Distributed Denial of Service attacks.

Lot of work has to be done to solve these problems as given in literature survey. But there is no exact solution to these problems and I will try to detect and prevent DDoS attack.

XI. OBJECTIVES

To measure network performance which include parameters like first packet received at [s], last packet received at [s], average end-to-end delay [s], total number of bytes received, total number of packets received etc.

- Study the effect of Distributed Denial of Service (DDoS) attacks under different attack intensities, different number of attackers and different node mobilities.
- 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.
- Analysis of the effectiveness of the prevention techniques.

XII. CONCLUSION

Introductory of future plan,

- Used to improve Network Performance.
- Used to improve wireless network efficiency.
- Provide better security to the intended user.
- Solve the problems of bandwidth depletion and resource depletion.
- Helps in providing network resource such as a website, web service, or computer system to the legitimate users.

XIII. 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) 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.
9) Xianjun Geng and Andrew B. Whinston; Defeating Distributed Denial of Service Attacks; February 2000.
10) Q. Li, E-C. Chang and M. C. Chan; On the Effectiveness of DDoS Attacks on Statistical Filtering; Proceedings of the 24th Annual Conference of the IEEE Communications Society (INFOCOM 2005), Miami; Mar 13-17, 2005.
11) Y. Kim, W. Lau, M. Chuah and J. Chao, PacketScore: Statistical-based Overload Control against Distributed Denial-of-Service Attacks, Proceedings of the 23rd Conference of the IEEE Communications Society (INFOCOM 2004), Hong Kong, Mar 7-11, 2004.
12) Bechler M, Hof H J, Kraft D, Pahlke F, Wolf L; A Cluster Based Security Architecture for Ad hoc Networks; 0-7803-8356-7/2004 IEEE.
13) P. Michiardi and R. Molva; Ad hoc Networks Security; IEEE Press Wiley; New York; 2003.
14) L. Zhou and Z.J. Haas, Cornell Univ.; Securing Ad hoc Networks; IEEE Network; Nov/Dec 1999; Volume: 13; pp. 24-30, ISSN: 0890-8044.
15) 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.
16) Y. Kim, W. Lau, M. Chuah and J. Chao; PacketScore: Statistical-based Overload Control against Distributed Denial-of-Service Attacks; Proceedings of the 23rd Conference of the IEEE Communications Society (INFOCOM 2004); Hong Kong; Mar 7-11, 2004.
17) S. Bellovin; Distributed denial of service attacks; Feb. 2000; http://www.research.att.com/-smbhalks.
18) H. Wang, D. Zhang, and K. Shin; Detecting SYN flooding Attacks; IEEE INFOCOM 2002, Jun. 2002, pp. 1530-1539.
19) http://www.merl.com/projects/DenialServiceAttacks/