International Journal of Research in Science And Technology http://www.ijrst.com
(IJRST) 2012, Vol. No. 2, Issue No. II, Apr-Jun **ISSN: 2249-0604**

"DDoS PREVENTION TECHNIQUE"

Madhu Malik

ABSTRACT

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. Routing protocols of MANET should 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. Security has become a primary concern in order to provide protected communication between nodes in a potentially hostile environment. Distributed Denial of Service (DDoS) attacks has also become a major problem in MANET. 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 Mobile Ad hoc Networks (MANET), various types of Denial of Service Attacks (DoS) are possible because of the inherent limitations of its routing protocols.

INTRODUCTION

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 and quality of service, limited bandwidth and limited power supply. These challenges set new demands on MANET routing protocols.

Ad hoc networks have a wide array of military and commercial applications. They are ideal in situations where installing an infrastructure network is not possible or when the purpose of the network is too transient or even for the reason that the previous infrastructure network was destroyed.

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. Existing solutions that are applied in wired networks can be used to obtain a certain level of security. Nonetheless, these solutions are not always being suitable to wireless networks. Therefore ad hoc networks have their own vulnerabilities that cannot be always tackled by these wired network security solutions.

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. 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.

WIRELESS NETWORKING INTRODUCTION

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.

There are two distinct approaches for enabling wireless communications between mobile hosts. The first approach is to use a fixed network infrastructure that provides wireless access points. In this network, a mobile host communicates with the network through an access point within its communication radius. When it goes out of range of one access point, it connects with a new access point within its range and starts communicating through it. An example of this type of network is the cellular network infrastructure. A major problem of this approach is handoff, which tries to handle the situation when a connection should be smoothly handed over from one access point to another access point without noticeable delay or packet loss. Another issue is that networks based on a fixed infrastructure are limited to places where there exist such network infrastructures. Figure 2.1 shows a simple infrastructure network with three nodes.

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. Nodes in the ad-hoc network are often mobile, but can also consist of stationary nodes. Each of the nodes has a wireless interface and communicates with others over either radio or infrared channels.

MOBILE AD HOC NETWORKS

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 [1]. 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. An ad hoc network uses no centralized administration. This ensures that the network will not cease functioning just because one of the mobile nodes moves out of the range of the others. Nodes should be able to enter and leave the network as they wish. Because of the limited

transmitter range of the nodes, multiple hops are generally needed to reach other nodes. Every node in an ad hoc network must be willing to forward packets for other nodes. Thus, every node acts both as a host and as a router. The topology of ad hoc networks varies with time as nodes move, join or leave the network. This topological instability requires a routing protocol to run on each node to create and maintain routes among the nodes [3].

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. 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.

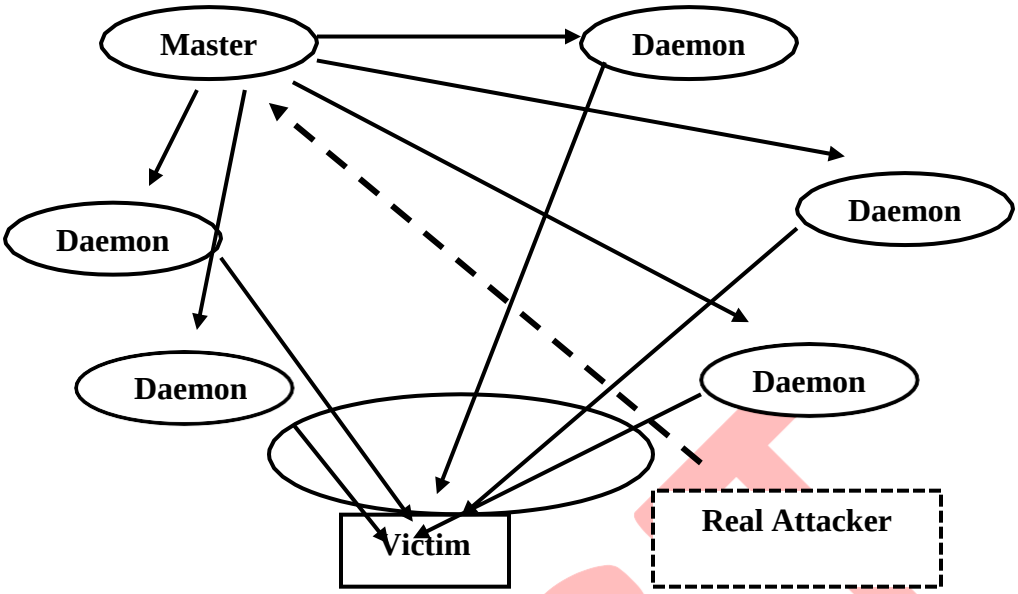
DDoS Attack

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 [2]. 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

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.

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.

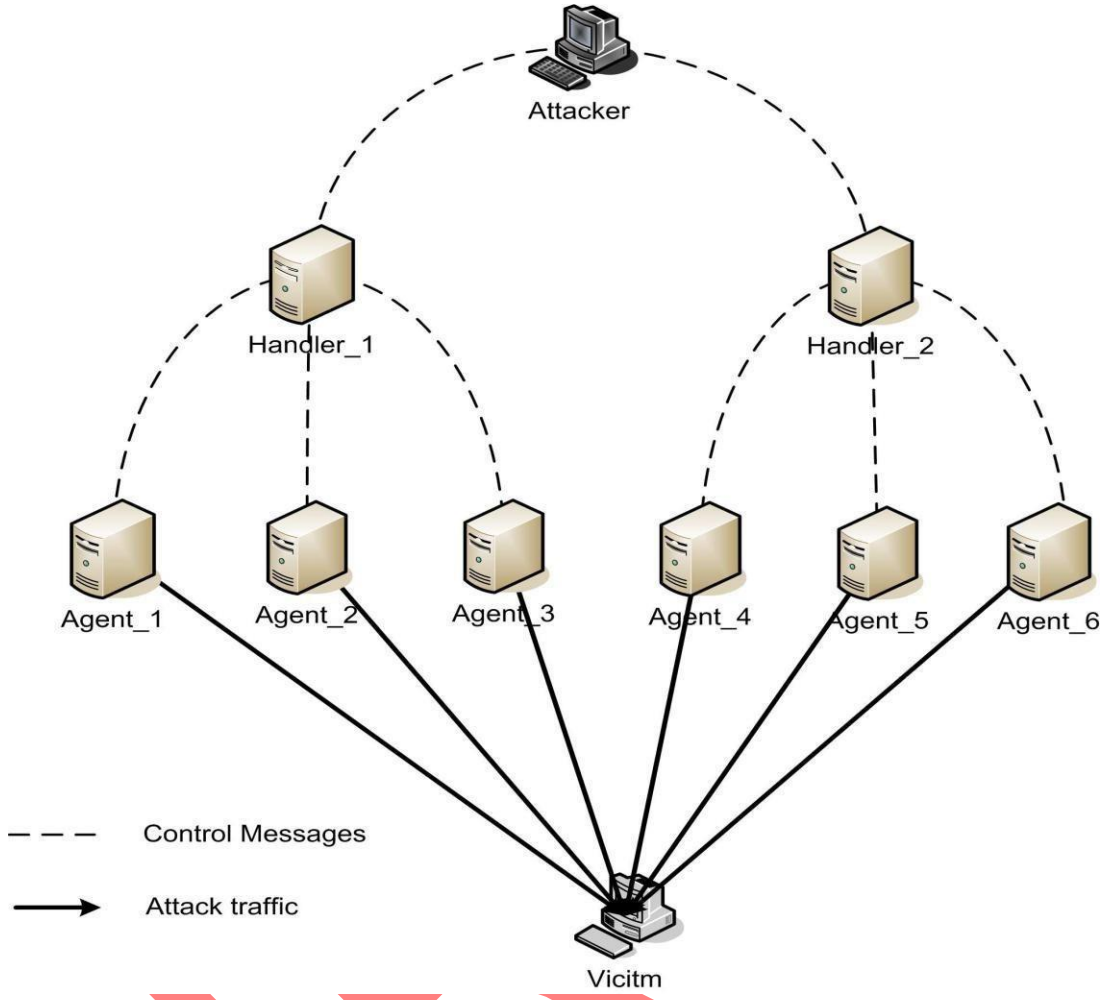


The four Components of DDoS Attacks.

Distributed Cooperative Architecture of DDoS Attacks

Before real attack traffic reaches the victim, the attacker must cooperate with all its DDoS agents. Therefore, there must be control channels between the agents and the attacker [7]. This cooperation requires all agents send traffic based on commands received from the attacker. The network which consists of the attacker, agents, and control channels is called the attack networks. In [2], attack networks are divided into three types: the agent-handle model, the Internet Relay Chat (IRC)-based model, and the reflector model.

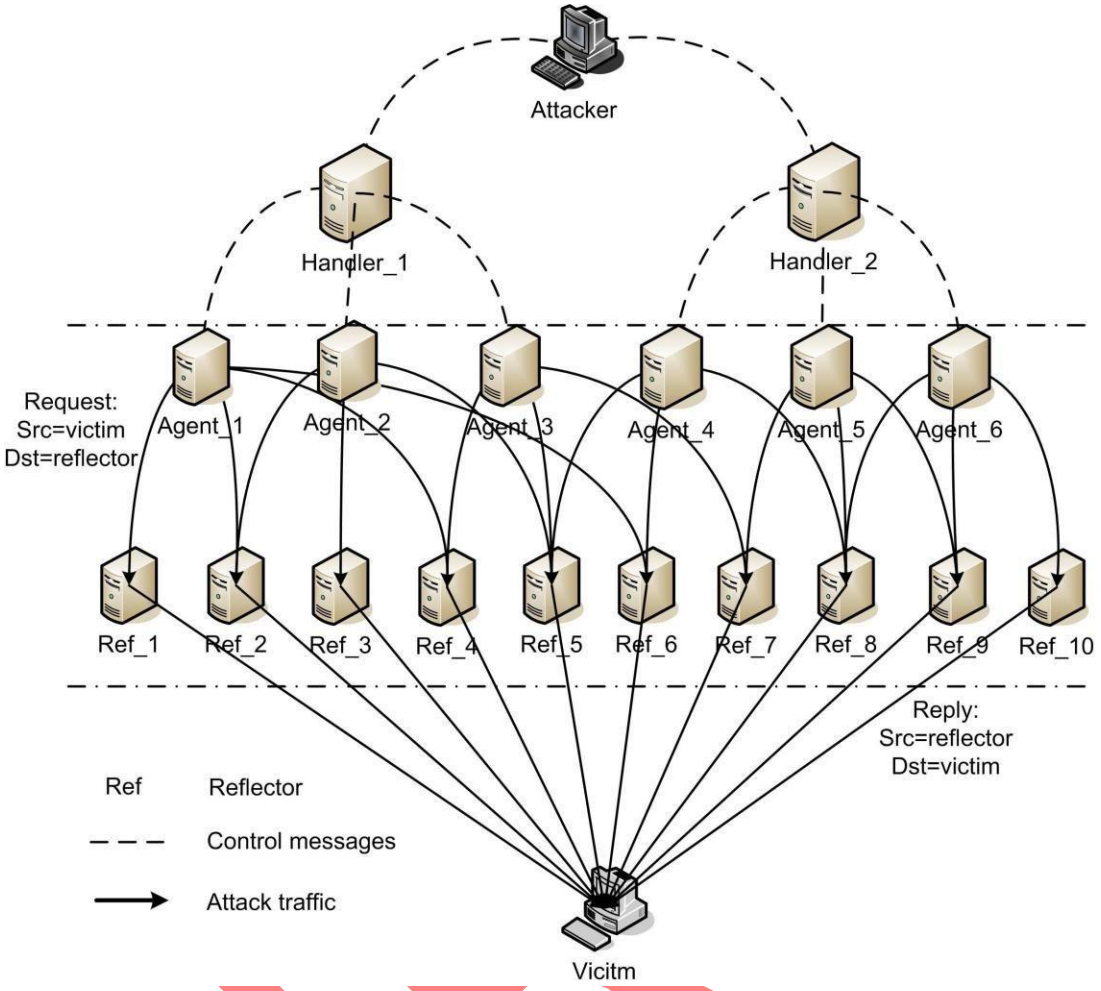
The agent-handler model consists of three components: attacker, handlers, and agents [9]. Figure 2.4 illustrates the typical architecture of the model. One attacker sends control messages to the previously compromised agents through a number of handlers, instructing them to produce unwanted traffic and send it to the victim.



Typical architecture of a DDoS attack.

The architecture of IRC-based model is not that much different than that of the agent-handler model except that instead of communication between an attacker and agents based on handlers, an IRC communication channel is used to connect the attacker to agents [2].

Figure 2.5 illustrates the architecture of an attack network in the reflector model. The reflector layer makes a major difference from the typical DDoS attack architecture. In the request messages, the agents modify the source address field in the IP header using the victim's address to replace the real agents' addresses. Then, the reflectors will in turn generate response messages to the victim. As a result, the flooding traffic which reaches the victim is not from a few hundred agents, but from a million reflectors [8]. An exceedingly diffused reflector-based DDoS attack raises the bar for tracing out the real attacker by hiding the attacker behind a large number of reflectors.



Architecture of a DDoS attack using reflectors.

Unlike some types of DDoS attacks, "the reflector does not need to serve as an amplifier" [8]. This means that reflectors still can serve other legitimate requests properly even when they are generating attack traffic. The attacker does not need to compromise reflectors to control their behaviors in the way that agents need to be compromised. Therefore, any host which will return a response if it receives a request can be a reflector. These features facilitate the attacker's task of launching an attack because it just needs to compromise a small number of agents and find a sufficient number of reflectors.

DDoS Attack Taxonomy

There are a wide variety of DDoS attacks. Two types of DDoS attacks are: Active and passive attack. Packet dropping is a type of passive attack in which node drops some or all of data packets sent to it for further forwarding even when no congestion occurs. There are two main classes of DDoS attacks: bandwidth depletion and resource depletion attacks shown in Figure 2.6.

Bandwidth Depletion Attacks

A **B**andwidth **D**epletion **A**ttack is designed to flood the victim network with unwanted traffic that prevents legitimate traffic from reaching the primary victim. Bandwidth depletion attacks can be characterized as flood attacks and amplification attacks.

(i) Flood Attacks: A *flood attack* involves zombies sending large volumes of traffic to a victim system, to congest the victim system's network bandwidth with IP traffic. The victim system slows down, crashes, or suffers from saturated network bandwidth, preventing access by legitimate users. Flood attacks have been launched using both UDP (User Datagram Protocol) and ICMP (Internet Control Message Protocol) packets.

In a *UDP Flood attack*, a large number of UDP packets are sent to either random or specified ports on the victim system. The victim system tries to process the incoming data to determine which applications have requested data. If the victim system is not running any applications on the targeted port, it will send out an ICMP packet to the sending system indicating a "destination port unreachable" message.

Often, the attacking DDoS tool will also spoof the source IP address of the attacking packets. This helps hide the identity of the secondary victims since return packets from the victim system are not sent back to the zombies, but to the spoofed addresses. UDP flood attacks may also fill the bandwidth of connections located around the victim system. This often impacts systems located near the victim.

An *ICMP flood attack* occurs when the zombies send large volumes of ICMP_ECHO_REPLY packets ("ping") to the victim system. These packets signal the victim system to reply and the combination of traffic saturates the bandwidth of the victim's network connection. During this attack, the source IP address of the ICMP packet may also be spoofed.

(i) Amplification Attacks: An amplification attack involves the attacker or the zombies sending messages to a broadcast IP address, using this to cause all systems in the subnet reached by the broadcast address to send a reply to the victim system. The broadcast IP address feature is found on most routers; when a sending system specifies a broadcast IP address as the destination address, the routers replicate the packet and send it to all the IP addresses within the broadcast address range. In this attack, the broadcast IP address is used to amplify and reflect the attack traffic, and thus reduce the victim system's bandwidth.

The attacker can send the broadcast message directly, or use the agents to send the broadcast message to increase the volume of attacking traffic. If the attacker decides to send the broadcast message directly, this attack provides the attacker with the ability to use the systems within the broadcast network as zombies without needing to infiltrate them or install any agent software.

A DDoS *Smurf attack* is an example of an amplification attack where the attacker sends packets to a network amplifier (a system supporting broadcast addressing), with the return address spoofed to the victim's IP address. The attacking packets are typically ICMP ECHO REQUESTs, which are packets (similar to a "ping") that request the receiver to generate an

ICMP ECHO REPLY packet [4]. The amplifier sends the ICMP ECHO REQUEST packets to all of the systems within the broadcast address range, and each of these systems will return an ICMP ECHO REPLY to the target victim's IP address [5]. This type of attack amplifies the original packet tens or hundreds of times.

Another example is the DDoS *Fraggle attack*, where the attacker sends packets to a network amplifier, using UDP ECHO packets [6]. There is a variation of the Fraggle attack where the UDP ECHO packets are sent to the port that supports character generation, with the return address spoofed to the victim's echo service creating an infinite loop. The UDP Fraggle packet will target the character generator in the systems reached by the broadcast address. These systems each generate a character to send to the echo service in the victim system, which will send an echo packet back to the character generator, and the process repeats. This attack can generate more bad traffic and cause more damage than a Smurf attack.

Resource Depletion Attacks

A **R**esource **D**epletion **A**ttack is an attack that is designed to tie up the resources of a victim system making the victim unable to process legitimate requests for service. DDoS resource depletion attacks involve the attacker sending packets that misuse network protocol communications or are malformed. Network resources are tied up so that none are left for legitimate users.

(i) Protocol Exploit Attacks: We give two examples, one misusing the TCP SYN (Transfer Control Protocol Synchronize) protocol, and the other misusing the PUSH+ACK protocol.

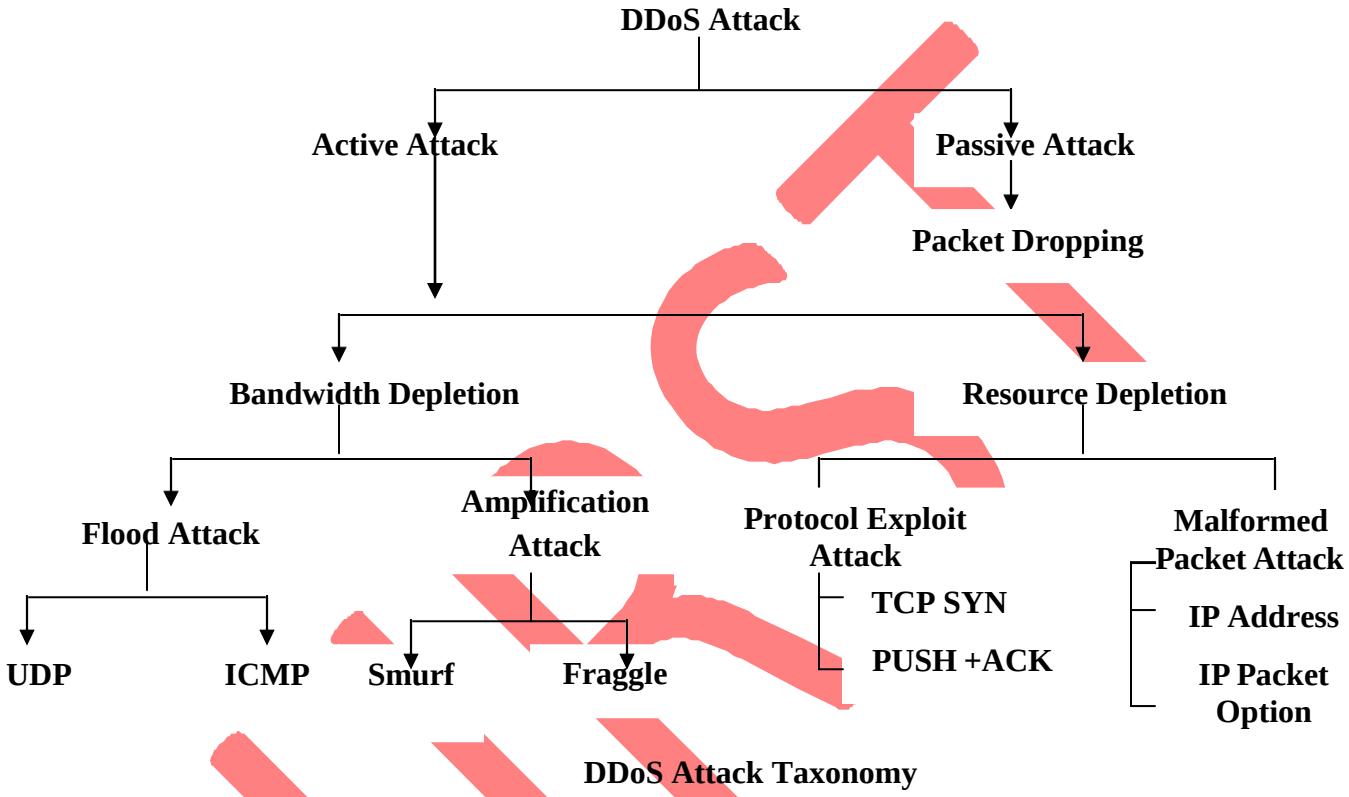
In a DDoS *TCP SYN attack*, the attacker instructs the zombies to send bogus TCP SYN requests to a victim server in order to tie up the server's processor resources, and hence prevent the server from responding to legitimate requests. The TCP SYN attack exploits the three-way handshake between the sending system and the receiving system by sending large volumes of TCP SYN packets to the victim system with spoofed source IP addresses, so the victim system responds to a nonrequesting system with the ACK+SYN. When a large volume of SYN requests are being processed by a server and none of the ACK+SYN responses are returned, the server eventually runs out of processor and memory resources, and is unable to respond to legitimate users.

In a *PUSH + ACK attack*, the attacking agents send TCP packets with the PUSH and ACK bits set to one. These triggers in the TCP packet header instruct the victim system to unload all data in the TCP buffer (regardless of whether or not the buffer is full) and send an acknowledgement when complete. If this process is repeated with multiple agents, the receiving system cannot process the large volume of incoming packets and the victim system will crash.

(ii) Malformed Packet attacks: A *malformed packet attack* is an attack where the attacker instructs the zombies to send incorrectly formed IP packets to the victim system in order to crash it. There are at least two types of malformed packet attacks.

In an *IP address attack*, the packet contains the same source and destination IP addresses. This can confuse the operating system of the victim system and can cause the victim system to crash.

In an *IP packet options* attack, a malformed packet may randomize the optional fields within an IP packet and set all quality of service bits to one so that the victim system must use additional processing time to analyze the traffic. If this attack is multiplied, it can exhaust the processing ability of the victim system.



DDoS Attack Taxonomy

PROPOSED PREVENTION SCHEME

With Different Number of Attackers

Table 3.1 and Figure 3.1 show the effect of proposed prevention technique on PDR with different number of attackers and it also shows comparison with the existing prevention scheme. This figure shows that proposed prevention technique (By disabling IP Broadcast) mitigate the effect of flooding based DDoS attack with larger extent. By using this technique PDR increases up to 31% as compared to the PDR of existing prevention scheme and 69% as compared to flood attack.

Table 3.2 and Figure 3.2 show the effect of proposed prevention technique on Number of Collisions with different number of attackers and it also shows comparison with the existing prevention scheme. This figure shows that proposed prevention technique (By disabling IP Broadcast) mitigate the effect of flooding based DDoS attack with larger extent. By using this

technique number of collisions decreases up to 41% as compared to the collisions of existing prevention scheme and 51.5% as compared to flood based DDoS attack.

Table 3.1: Effect of Proposed Prevention Technique on PDR with varying number of attackers.

NUMBER OF ATTACKERS PER NETWORK	PACKET DELIVERY RATIO (PDR)			
	WITHOUT ATTACK	FLOODING BASED DDoS ATTACK	EXISTING PREVENTION TECHNIQUE	PROPOSED PREVENTION TECHNIQUE
3	.926	.32	.57	.83
4	.926	.31	.55	.82
5	.926	.22	.47	.72
6	.926	.20	.45	.69
7	.926	.175	.44	.58
8	.926	.15	.42	.57
9	.926	.12	.39	.56

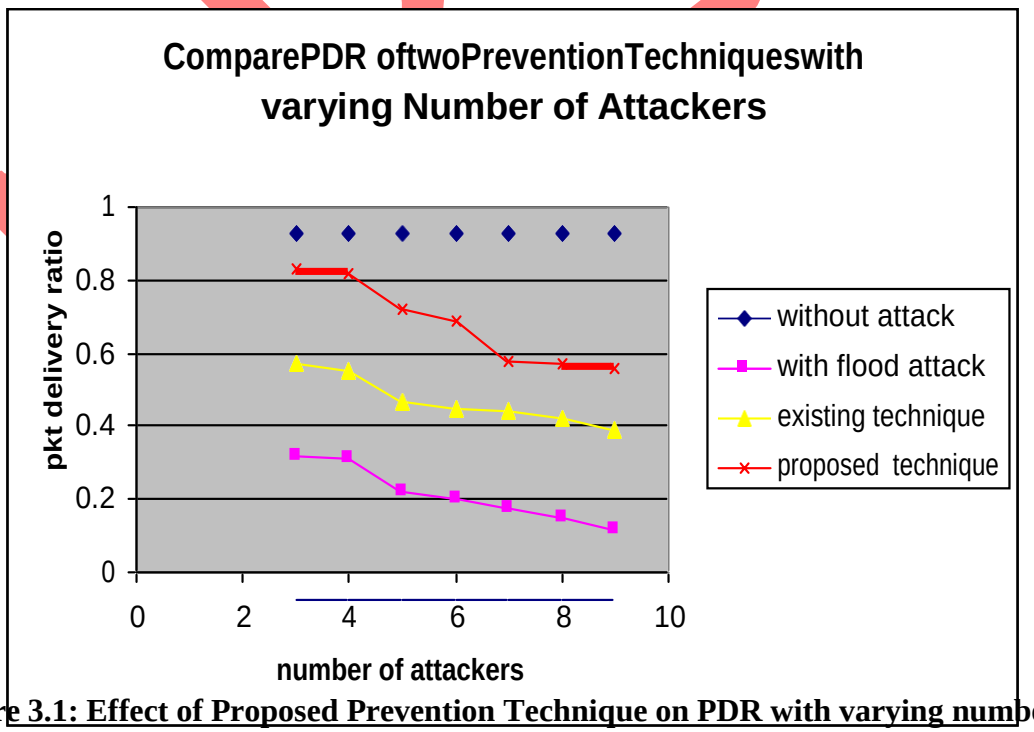


Figure 3.1: Effect of Proposed Prevention Technique on PDR with varying number of attackers.

Table 3.2: Effect of Proposed Prevention Technique on Number of Collisions with varying number of attackers.

NUMBER OF ATTACKERS PER NETWORK	NUMBER OF COLLISIONS PER NETWORK			
	WITHOUT ATTACK	FLOODING BASED DDoS ATTACK	EXISTING PREVENTION TECHNIQUE	PROPOSED PREVENTION TECHNIQUE
3	11	8543	7055	3955
4	11	8571	7091	4018
5	11	8685	7175	4175
6	11	8741	7233	4210
7	11	8756	7315	4315
8	11	8897	7400	4400
9	11	8918	7535	4535

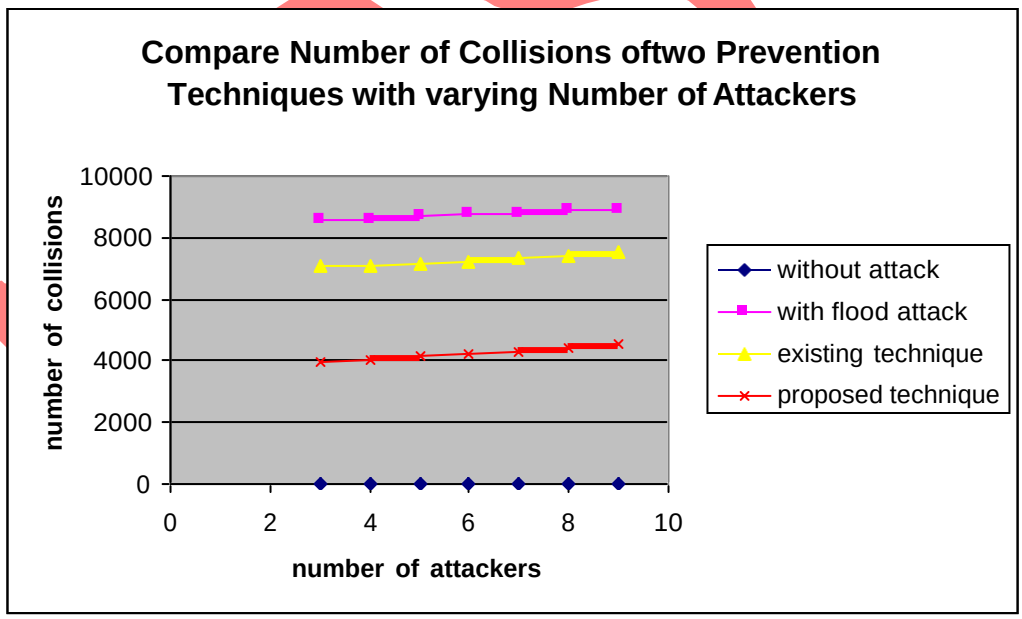


Figure 3.2: Effect of Proposed Prevention Technique on Number of Collisions with varying number of attackers.

Table 3.3 and Figure 3.3 show the effect of proposed prevention technique on Energy Consumption with different number of attackers and it also shows comparison with the existing prevention scheme. This figure shows that proposed prevention technique (By disabling IP Broadcast) mitigate the effect of flooding based DDoS attack with larger extent.

Table 3.4: Effect of Proposed Prevention Technique on Energy Consumption with varying number of attackers.

NUMBER OF ATTACKERS PER NETWORK	ENERGY CONSUMPTION (MWHR)			
	WITHOUT ATTACK	FLOODING BASED DDoS ATTACK	EXISTING PREVENTION TECHNIQUE	PROPOSED PREVENTION TECHNIQUE
3	5.010	5.16	5.15	5.080
4	5.010	5.187	5.162	5.090
5	5.010	5.200	5.179	5.114
6	5.010	5.215	5.188	5.119
7	5.010	5.22	5.197	5.139
8	5.010	5.235	5.205	5.146
9	5.010	5.257	5.210	5.180

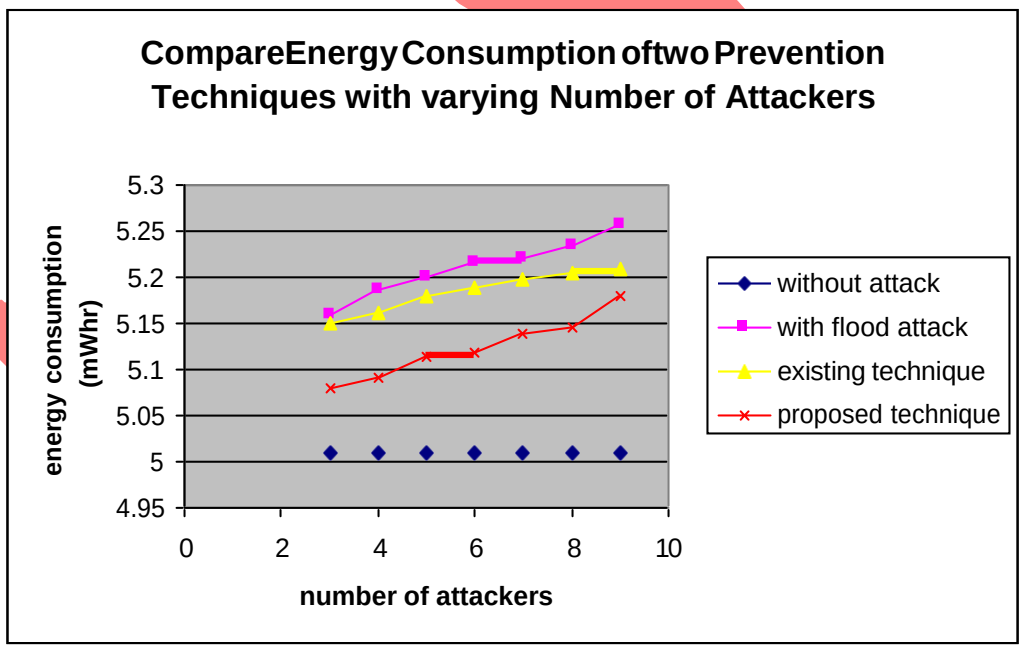


Figure 3.3: Effect of Proposed Prevention Technique on Energy Consumption with varying number of attackers.

With Varying Node Mobility

Table 3.5 and Figure 3.4 show the effect of proposed prevention technique on PDR with varying node mobility and number of attackers are 8. It also shows comparison with the existing

prevention scheme. This figure shows that proposed prevention technique (By disabling IP Broadcast) mitigate the effect of flooding based DDoS attack with larger extent. By using this technique PDR increases up to 47% as compared to the PDR of existing prevention scheme.

Table 3.5: Effect of Proposed Prevention Technique on PDR with varying node mobility.

MOBILITY	PACKET DELIVERY RATIO (PDR)			
	WITHOUT ATTACK	FLOODING BASED DDoS ATTACK	EXISTING PREVENTION TECHNIQUE	PROPOSED PREVENTION TECHNIQUE
0-5	.926	.15	.42	.57
5-10	.916	.135	.38	.53
10-15	.905	.110	.36	.49
15-20	.898	.083	.24	.47

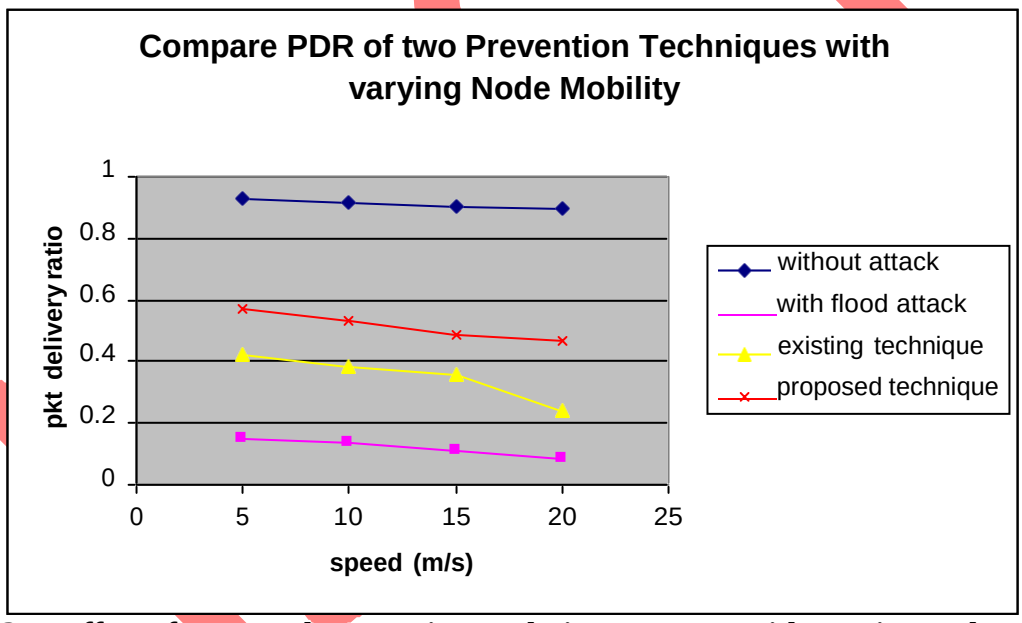


Figure 3.4: Effect of Proposed Prevention Technique on PDR with varying node mobility.

Table 3.6 and Figure 3.5 show the effect of proposed prevention technique on Number of Collisions with varying node mobility and number of attackers are 8. It also shows comparison with the existing prevention scheme. This figure shows that proposed prevention technique (By disabling IP Broadcast) mitigate the effect of flooding based DDoS attack with larger extent. By using this technique number of collisions decreases up to 39.5% as compared to collisions of existing prevention scheme.

Table 3.6: Effect of Proposed Prevention Technique on Number of Collisions with varying node mobility.

MOBILITY	NUMBER OF COLLISIONS PER NETWORK			
	WITHOUT ATTACK	FLOODING BASED DDoS ATTACK	EXISTING PREVENTION TECHNIQUE	PROPOSED PREVENTION TECHNIQUE
0-5	11	8897	7400	4400
5-10	12	9013	7535	4515
10-15	15	9117	7615	4675
15-20	19	9273	7725	4718

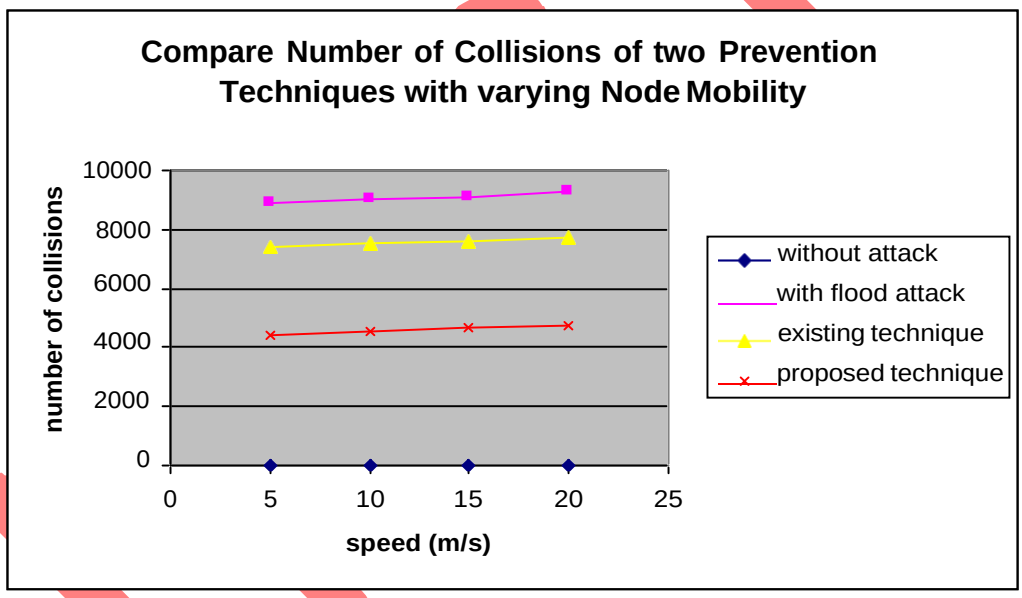


Figure 3.5: Effect of Proposed Prevention Technique on Number of Collisions with varying node mobility.

Table 3.7 and Figure 3.6 show the effect of proposed prevention technique on Energy Consumption with varying node mobility and number of attackers are 8. It also shows comparison with the existing prevention scheme. This figure shows that proposed prevention technique (By disabling IP Broadcast) mitigate the effect of flooding based DDoS attack with larger extent.

Table 3.7: Effect of Proposed Prevention Technique on Energy Consumption with varying node mobility.

MOBILITY	ENERGY CONSUMPTION (MWHR)			
	WITHOUT ATTACK	FLOODING BASED DDoS ATTACK	EXISTING PREVENTION TECHNIQUE	PROPOSED PREVENTION TECHNIQUE
0-5	5.010	5.230	5.205	5.146
5-10	5.012	5.235	5.210	5.160
10-15	5.019	5.240	5.222	5.170
15-20	5.021	5.250	5.230	5.185

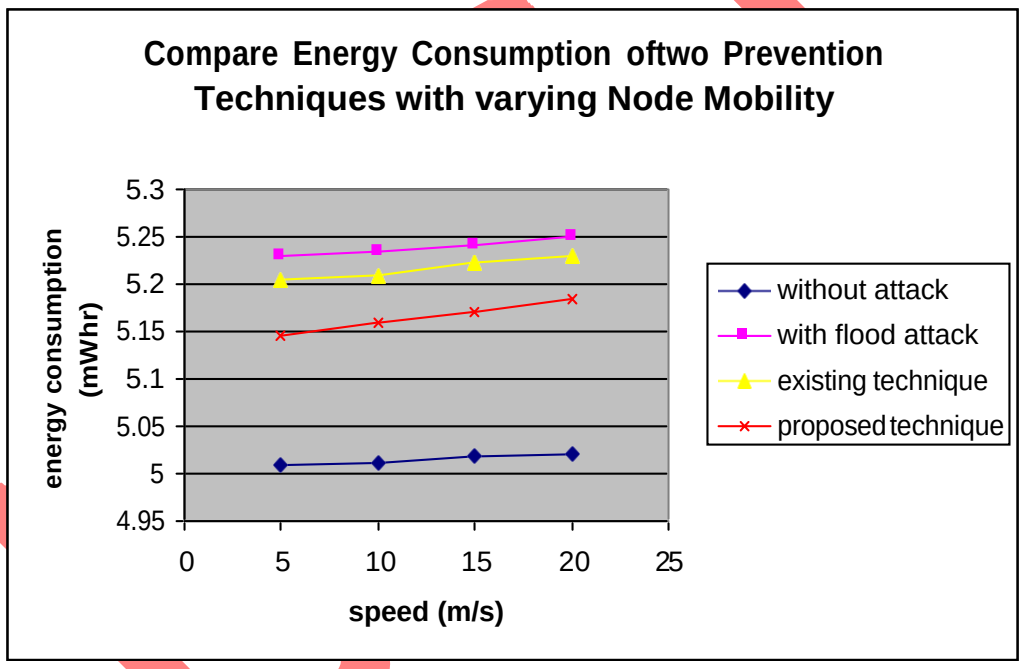


Figure 3.6: Effect of Proposed Prevention Technique on Energy Consumption with varying node mobility.

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. The risk from DDoS attacks should not thus be underestimated, but not overestimated, either.

In the future the problem from DDoS attacks will most probably increase because the number of hosts connected in the Internet increases, access lines get faster, software products get more complex, and security continues to be difficult for an ordinary home user and even many organizations. The more there are hosts in the Internet, the more of them can potentially be used for DDoS purposes. The intensity of DDoS attacks can also increase, as a higher number of hosts can produce more traffic over faster Internet access lines. As software gets more complex, more vulnerability will reside in them to be used for compromising hosts. The fast pace of new revisions does not make the situation easier. Finally, it will continue to be difficult to evaluate security risks in existing computer systems, especially by ordinary people.

REFERENCES

[1] Han L; Wireless Ad hoc Network; October 8, 2004.

[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] A. Sun; The design and implementation of fisheye routing protocol for mobile ad hoc networks; M.S. Thesis, Department of Electrical and Computer Science, MIT; May 2002.

[4] TFreak; smurf.c; www.phreak.org/archives/exploits/denial/smurf.c; May 6, 2003.

[5] Federal Computer Incident Response Center (FedCIRC); Defense Tactics for Distributed Denial of Service Attacks; Washington, DC; 2000.

[6] TFreak; fraggle.c; www.phreak.org/archives/exploits/denial/fraggle.c; May 6, 2003.

[7] J. MÄolsÄa; Mitigating denial of service attacks in computer networks; PhD thesis; Helsinki University of Technology, Espoo, Finland; June 2006.

[8] V. Paxson; An analysis of using reflectors for distributed denial-of-service attacks; ACM SIGCOMM Computer Communication Review, vol. 31, no. 3; July 2001.

[9] Yonghua You; A defense framework for flooding-based DDoS attacks; Master of Sc. Thesis; Queen's University Kingston, Ontario, Canada; August 2007.