

Arabic Academy For Banking And Finance  
Computer Information System Dept.

Damascus, 2005/2006.



## Defense against Distributed Denial of Service Attack

Presented by

Eng: Fadi BAGHDADLIAN

Supervisor

Dr .Assem Shekh

## **Abstract**

Have you ever tried to use the phone on a special occasion like New Year or mother day? Did you face some problem in making the call? If yes then you know the distributed denial of service, it happens when the number of users trying to use a service is bigger than the capacity of the service provider.

In the phone call example, let us assume that the telephone network can serve 1000 users in the same time, normally less than 1000 user will use the network at the same time, but in some special occasion more than 1000 users may use the network and that causes Denial of Service (DoS) for many users.

In computer network we have the same idea, if the number of clients that try to connect to a Server is bigger than the band width of the Server then we will face DoS.

Many attackers are using this technique to attack servers on the internet. This threat started with Morris worm 1988 and continued until our days without a solution (Code Red worm – 2001 , SQLSlammer worm – 2003 , MyDoom – 2004 ...)

We will study these types of attack and classify them and their Defense methods, then we will make a comparison between these methods to reach the best solutions and precautions.

# CONTENTS

	Page
<b>Chapter 1: Introduction</b>	
<b>1-1 Introduction of Internet .....</b>	<b>3</b>
<b>1-2 Security Principles .....</b>	<b>5</b>
<b>1-3 Background in Computer Threat .....</b>	<b>6</b>
<b>1-4 Background in Defense .....</b>	<b>7</b>
<b>1-5 Background in TCP/IP.....</b>	<b>7</b>
<b>1-6 Master's Thesis task.....</b>	<b>9</b>
<b>Chapter 2: Study Of DoS</b>	
<b>2-1 Classification of DoS.....</b>	<b>10</b>
<b>2-2 Example of DoS .....</b>	<b>12</b>
<b>Chapter 3: Study Of DDoS</b>	
<b>3-1 Definition of DDoS.....</b>	<b>14</b>
<b>3-2 Why DDoS is possible? .....</b>	<b>15</b>
<b>3-3 Classification of DDoS .....</b>	<b>15</b>
<b>3-4 Example of DDoS.....</b>	<b>23</b>
<b>3-5 DDoS attack tools.....</b>	<b>23</b>
<b>Chapter 4: Defense against DDoS</b>	
<b>4-1 Introduction.....</b>	<b>24</b>
<b>4-2 Defense Taxonomy.....</b>	<b>24</b>
<b>4-3 Defense Steps.....</b>	<b>27</b>
<b>4-4 Defense Method Comparison.....</b>	<b>33</b>
<b>Chapter 5: Conclusion and Recommendations .....</b>	<b>35</b>

# Chapter 1

## Introduction

### 1-1 Introduction of Internet

The first attack on the internet was on 1988 with a worm named Morris worm. And this worm changed people's way of thinking towards internet. In the beginning the main concern when connecting to the internet is the connection itself, but after 1988 there is more than the connection to think about... There is Security problems.

Mr. Dave Clark tells a story about an angry manager wondering how the problem of Morris worm could happen. And Dave Clark answers him that this is what the internet was designed to do: spread the worm as quickly and efficiently as possible.

In the beginning there were no problems with Internet since most users were scientists but now every one uses internet and we are facing more and more of cyber crimes. [9]

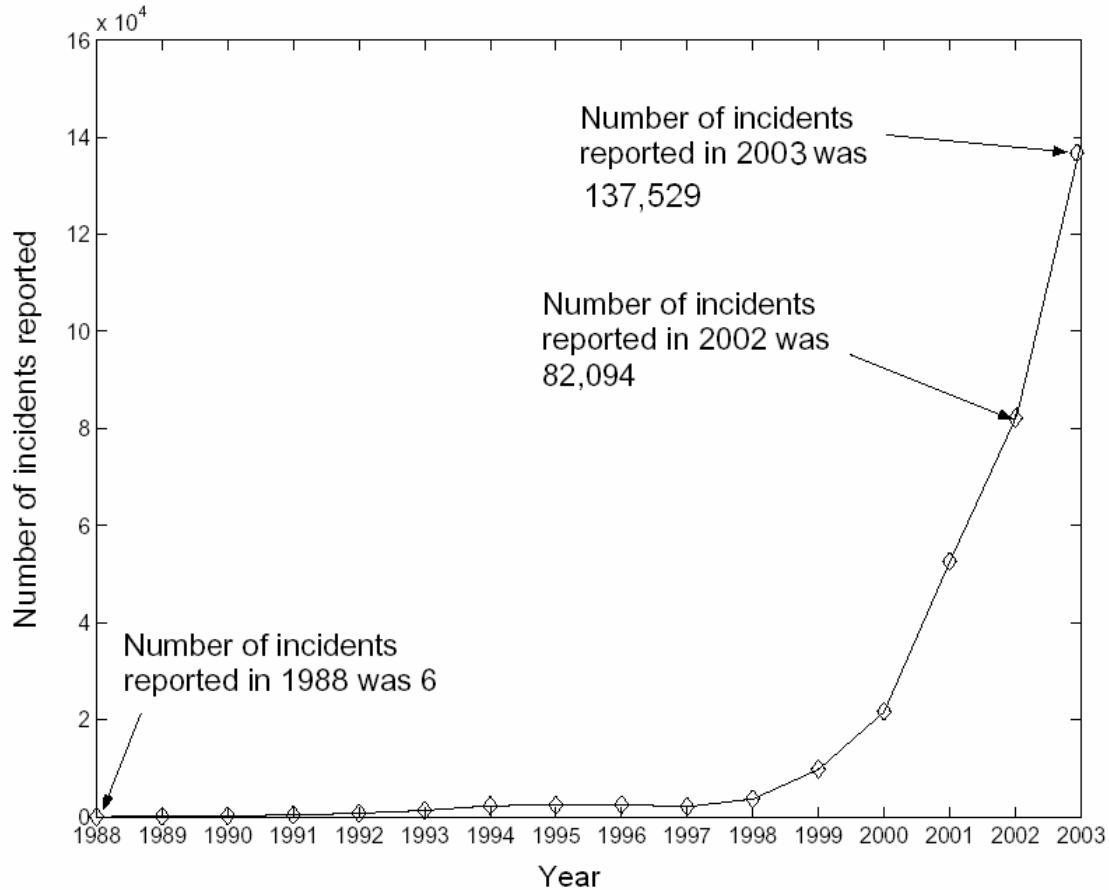
Now after 18 years we still face the same problems similar to Morris worm Some of the famous attacks were the Code Red and Nimda worms that infected hundred of thousands of computers in 2001. And these worms caused the loss of millions of dollars.

The SQL Slammer worm attack in 2003 was very fast and within 10 minutes more than 90% of vulnerable computers were infected. And it caused denial of service of many networks in Asia, Europe & America for several minutes. This worm was called the first "Warhol" because it was able to stop a big portion of the internet within 15 minutes

The dangerous effects of such worms, provoked many organizations such as " CERT, CAIDA, and SANS Institute" to monitor the internet and to

detect any suspicious packets. They analyze all packets to detect any abnormal network activities. These centers are the basis for a future nation worm monitoring and early warning system. [22]

The following chart represents the number of Internet security incidents reported from 1988 to 2003 [6]



Other problem with the internet is DoS, the most famous DDoS attacks in 2000 where some important dotcom sites like yahoo, eBay & Amazon were stopped for 2 days and costed the companies millions of dollars. [20]

We will study distributed denial of service attack in the next chapters since it is the main unsolved problem in the internet and there are many approaches to reduce its affect but none of them are a complete solution for this threat.

## 1-2 Security Principles

Information Security has 3 basic principles: *Confidentiality*, *Integrity*, and *Availability*.

***Confidentiality*** is concerned with keeping information secret and in allowing access for legitimated users only.

***Integrity*** means that the data must remain in known state, for example the number of a bank account that we transfer money to should not be changed! Otherwise the money will be transferred to an unknown account.

***Availability*** means that our Systems and Network should be available all the time for the company and its clients. And this is the case that we will study in our work (DDoS attack that makes our network unavailable).

Some other experts put other classifications and they add two other security principles, *Authentication* and *non repudiation*

***Authentication*** used when we need to be sure of the identity of the parties involved. Biometrics, tokens and smart cards are used to provide authentication.



***Non Repudiation*** used to be sure that a person made a transaction and could not deny it. It is similar to the verification of the hand signature. Asymmetric encryptions are used to provide digital signature (RSA algorithm is the famous asymmetric encryption used worldwide).

We can use encryption to address the Confidentiality and integrity but if we lose the encryption key we will lose the availability of the information.

[4][21]

### **1-3 Background in Computer Threat:**

Since the existence of computers, we faced many threats like: Viruses, Email Viruses, Worms, Trojan horse and Denial of service.

We will introduce these types of threats:

***Virus:*** Computer program that spreads by inserting copies of itself into other executable code or documents; it is similar to the biological virus which spreads in a live cell. Some types of the virus attack disk boot sectors. Some others just attack exe or com files. Usually they have a logical or timing bomb where the virus will attack its victim.

***E-mail viruses:*** it is a type of virus that uses an e-mail message as a mode of transport, and it automatically emails itself to all email addresses found in the victim's address book. One of the famed is "Mellisa"

***Trojan horses:*** it's a computer program pretends to do one thing such as compressing files while it is damaging them.

***Worms:*** it's a piece of software that uses computer networks and security flaws to create copies of itself. A copy of the worm will scan the network for any other machine that has a specific security flaw. It replicates itself to the new machine using the security flaw, and the replicating process continues. There are many famous worms like "Love Bug worm". Some times the worms cause DoS attack.

***DoS:*** Denial of Service is stopping a program or computer or network from working to deny the legitimate user from using the system. And this is the subject of our research... Some experts do not classify the DoS as threats, but as a consequence of other threats like worms.

All the previous threats are called malware (malicious software) that is software designed to make harm to your system. They use a bug in the systems or they flood the systems with traffics to make harm to your system.

## 1-4 Background in Defense [12]

There are many software and hardware that deal with the previous threats:

**Antivirus:** software that searches for viruses in all files that come to our system. And also searches for the suspicious action that may be caused by unknown virus (like writing on boot sector). The most famous are Semantic and MacAfee antivirus.

**Firewall:** it is a hardware or software that prevents any unauthorized access to our network; it helps in preventing some types of DoS attacks. Well known software firewall included with windows XP (internet connection firewall) and in Hardware firewall the most famous are Cisco Pix firewall.

**Intrusion detection or preventing systems:** it is like a monitor that waits for specific suspicious network traffic, and then it alarms about the incident and sometimes it takes action immediately. Some times the ISD or IPS are included with the firewall.

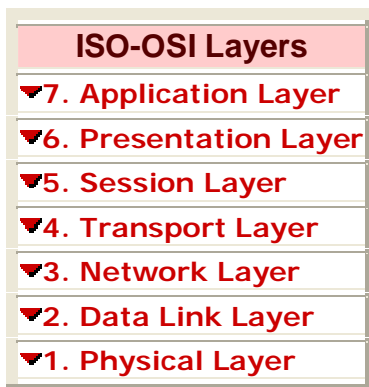
Many companies produce a single software product that have antivirus, antisпам, firewall and IDS in one package like Norton security center.

## 1-5 Background in TCP/IP [3][13]

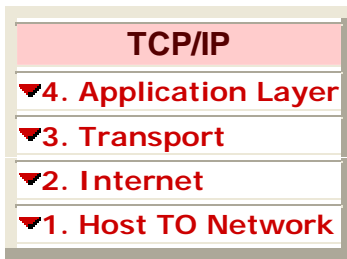
The most popular protocol in the entire world is IP, since it is used in Internet...

The ISO developed OSI model for providing a reference of complex aspects related to network communication.

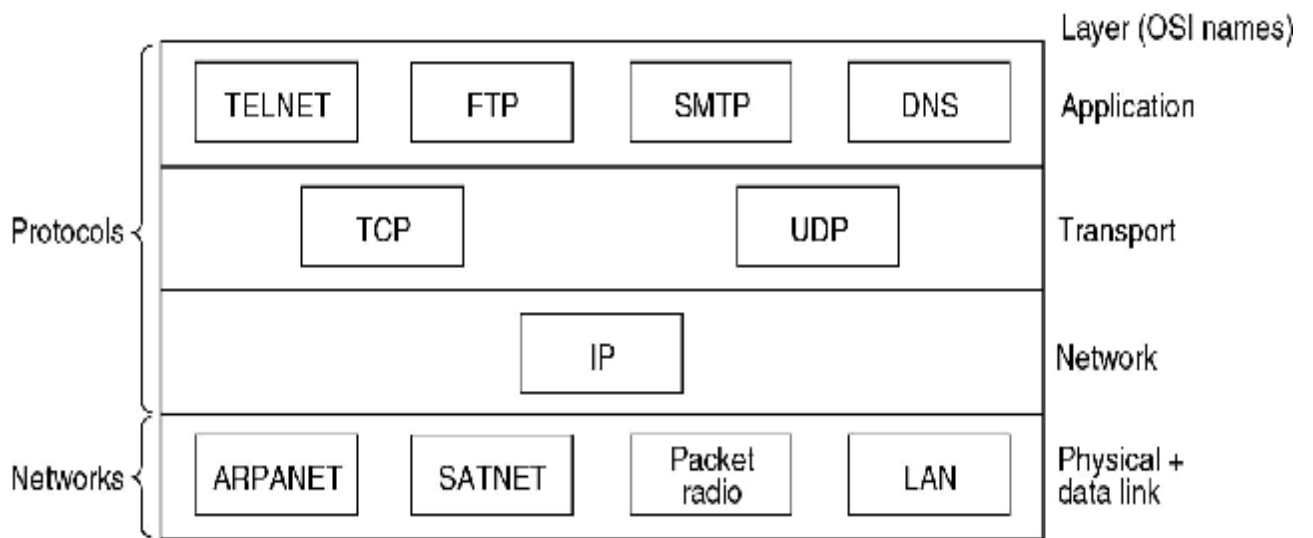
It divides the different functions and services provided by network hardware and software in 7 layers.



In the same time there is other model: ICP/IP, it was widely used more than the ISO – OSI model.



We can see in the next picture some of the protocols in the different layers.



The most attacks come to protocol TCP & IP.

We will introduce some of the main important aspect of TCP / UDP / IP protocol since we will need them in our next work:

**Socket:** the socket is the pair IP address + port number.

**TCP Flags:** the TCP header contains 6 flags

- **SYN** : Synchronize sequence numbers to initiate a connection
- **FIN** : The sender is finished sending data.
- **RST** : Reset the connection.
- **URG** : The *urgent pointer* is valid.
- **ACK** : The acknowledgment number is valid.
- **PSH** : The receiver should pass this data to the application as soon as possible.

**TCP Connection establishment:** TCP is a connection oriented protocol, it means that the two applications using TCP should establish a connection before exchange any data.

They use some flags with random numbers

- 1- SYN (XX)
- 2- SYN (YY) / ACK ( XX+1)
- 3- ACK (YY+1)

**Port scanning:** it is searching for the active ports on a specific IP address. For example Web server uses port 80, so Port scanner will found the port 80 opened on that system.

### **1-6 Master's Thesis task:**

I split my work into the following tasks in five chapters:

- General introduction about security (**chapter 1**)
- Study the different types of DoS (**chapter 2**)
- Study the different types of DDoS (**chapter 3**)
- Study and compare the different approaches to defend against DDoS (**chapter 4**)
- Conclusion and recommendation (**chapter 5**)

# Chapter 2

## Study Of DoS

Many network attacks try to gain access to systems and use variety of creative techniques to achieve this goal like sniffing, spoofing & session hijacking.

Other attacks don't care to obtain access; they want only to stop critical services or to prevent legitimate users from access into the system. We call this type of attack Denial of Service attack, and we refer to it as DoS not DOS to distinguish it from Disk operating system.

### 2-1 Classification of DoS [11]

	Stopping Services	Exhausting Resources
Locally	<ul style="list-style-type: none"><li>• Process killing</li><li>• System reconfiguration</li><li>• Process crashing</li></ul>	<ul style="list-style-type: none"><li>• Forking processes to fill the process table</li><li>• Filling up the whole file system</li><li>• Sending many traffic to the outside</li></ul>
Remotely	<ul style="list-style-type: none"><li>• Malformed packet attack</li></ul>	<ul style="list-style-type: none"><li>• Packet floods</li></ul>

#### *1- Locally Stopping Services:*

If a user has administration privileges, he can shut down any critical services offered by the system, in fact he can shut down all the system!

The hacker can kill important process or can change the system configuration that denies the service indirectly, for example the user can change NAT configuration and deny any external user from accessing a web server.

If the user doesn't have privilege to kill a critical process, he can crash the system using any existing vulnerability like overflow attack.

## ***2- Locally Exhausting Resource:***

There are many recourses that if exhausted will stop any user from accessing the system. If a user has privileges he can fill in the process table of the file system. If he has no privileges he can send traffics to the outside and that will flood the system and deny any external user from accessing the system.

## ***3- Remotely Stopping Services:***

Usually there are many bugs (vulnerabilities) in any system, some of them will cause the system to stop, and if the crackers find these bugs they will use them to make DoS.

## ***4- Remotely Exhausting Resource:***

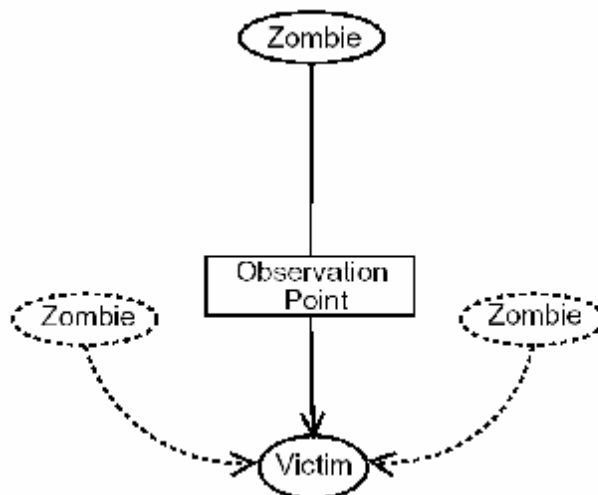
If the cracker doesn't find any vulnerability on the system he will try to exhaust the target resources, like CPU, Buffers & Communication link. For example he floods the server with many packets and the DoS attack will be successful if he has a band width bigger than the band width that the victim can support.

We can also distinguish between 3 types of the Remotely Exhausting Resource:

Based on the location of observation point: [1]

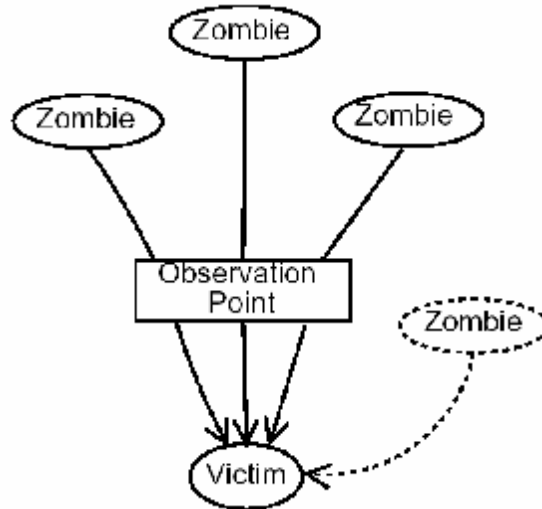
- Single-source:

When a single attacker (Zombie) is flooding the victim



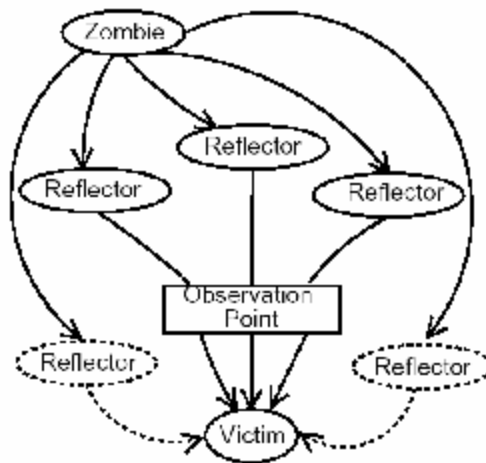
- Multi-source

When multi attackers (Zombie) are flooding the victim



- Reflector

It is a special case of Multi-sources, the attacker tries to hide his identity or to amplify the attack. An example of this attack is sending TCP SYN to a web server (Reflector) with spoofed source IP address (Victim IP), so the SYN-ACK will return to the victim, not to the attacker.



## 2-2 Example of DoS

**1- SYN Flood:** sending flood of TCP/SYN packets usually with a spoofed IP address, each packet is treated as a connection request, these requests cause the server to send TCP/SYN-ACK packet and wait for TCP/ACK that will

never come. If the number of packets is more than the resources available (Timers & memory) the server will stop responding to any real TCP connection.

## **2- ICMP flood**

**2-1 Smurf Attack:** the attacker sends a large number of ICMP echo traffic to the broadcast address and puts the victim address instead of the source address. Then all the machines on the broadcast network will reply to the victim and this consequently will cause DoS.

**2-2 Ping flood :** the sender floods the victim with many ICMP echo packets (ping). This attack will succeed if the attacker's band width is bigger than the victim's.

**3- Fraggle attack (UDP flood):** it is similar to Smurf attack, but the packet is UDP echo instead of ICMP echo.

**4- DNS attack:** this type is similar to Smurf attack; the attacker sends a DNS request to a nameserver with a spoofed source IP address with the Victim address. When the DNS server replies to the request, it replies to the victim instead of the attacker. This is a useful reflector attack, since the DNS reply has large size and can flood the victim.

**5- Buffer overflow:** programming error that may cause exception in memory and program termination or may cause security breach.

**5-1 Ping of Death:** sending a ping with size bigger than the usual size 64 bytes. Many old OS crashes when receiving a ping with the size 65,536.

**5-2 Morris worm:** a worm that exploits a buffer overflow bug in UNIX service called fingerd system (1988).

**5-3 Code Red worm:** a worm that exploits a buffer overflow bug in Microsoft Internet Information Service (IIS) 5.0 (2001).

**5-4 SQLSlammer worm:** a worm that exploits a buffer overflow bug in Microsoft SQL Server 2000 (in 2003).

**6- DDoS (Distributed denial of service attack):** more details on the DDoS in the next chapter.

# Chapter 3

## Study of DDoS

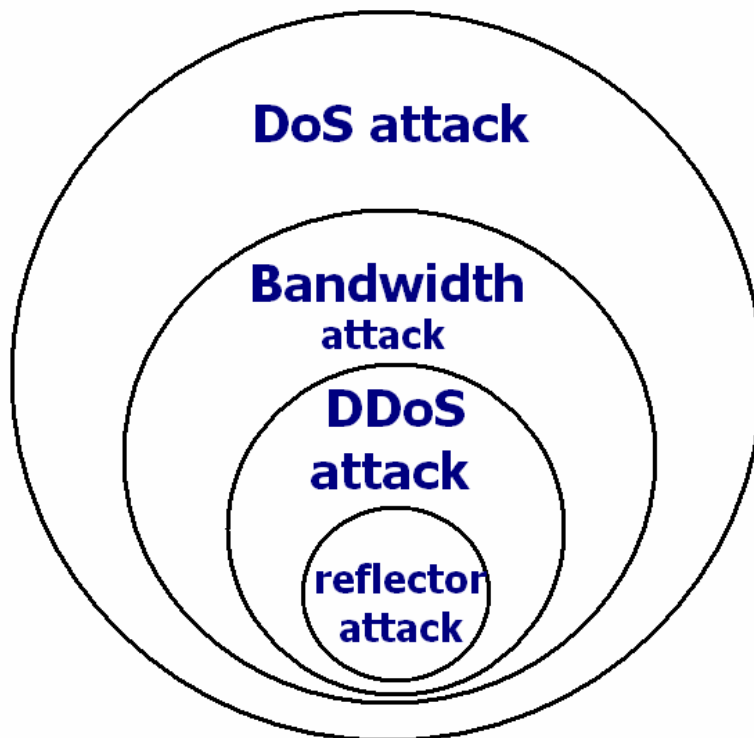
### 3-1 Definition of DDoS.

A DDoS attack directs hundreds or even thousands of compromised “zombie” hosts against a single target.

With enough zombies the victim won't be able to answer any legitimate users.

To start a DDoS attack we should have a big laboratory plain of computers that will attack together the victim, or we will use a single computer and a worm that will do the dirty job: spread from host to host and then attack in a specific time.

To understand the relation between DoS and DDoS please see the following picture



The relation of different types of attacks [18]

The bandwidth attack uses single node to attack the victim, and it makes use of some aspects in the protocols like the SYN-ACK problem.

DDoS attack is similar to bandwidth attack except that it uses many nodes to start the attack.

Reflector attack is similar to DDoS attack, except that it uses reflection in the last step near the victim to amplify the attack and to hide its source.

### **3-2 Why DDoS is possible?**

The designers of the internet haven't expected that it will be widely adopted and used; they thought that only the scientists will be using this network. That's why they haven't considered thoroughly security issues.

There are many features of internet that make it vulnerable to DDoS attack: [14]

- ***Internet security is highly interdependent:*** The DDoS attack uses some vulnerable hosts on the internet to launch the attack.
- ***Internet control is distributed:*** Each host runs according to its network configuration, there is no global configuration for the hosts connected to the internet.
- ***Internet resources are limited:*** any internet host (victim) has a limited resources (memory, band width, CPU) so there will be a number of hosts who have more resources and can attack the victim.
- ***Accountability is not enforced:*** there is no method of identifying the source of any packet, the packet contains its source address but it could be spoofed and this gives the attacker a possibility to escape from accountability for their actions.

### **3-3 Classification of DDoS.**

I will introduce two important categories for classification DDoS

***I Classification based on vulnerability type:***

#### **1- DDoS that uses technological vulnerabilities:**

In this type of attack, the attacker will use some bug in the system to copy the Zombies from host to host.

#### **2- DDoS that uses operational vulnerabilities:**

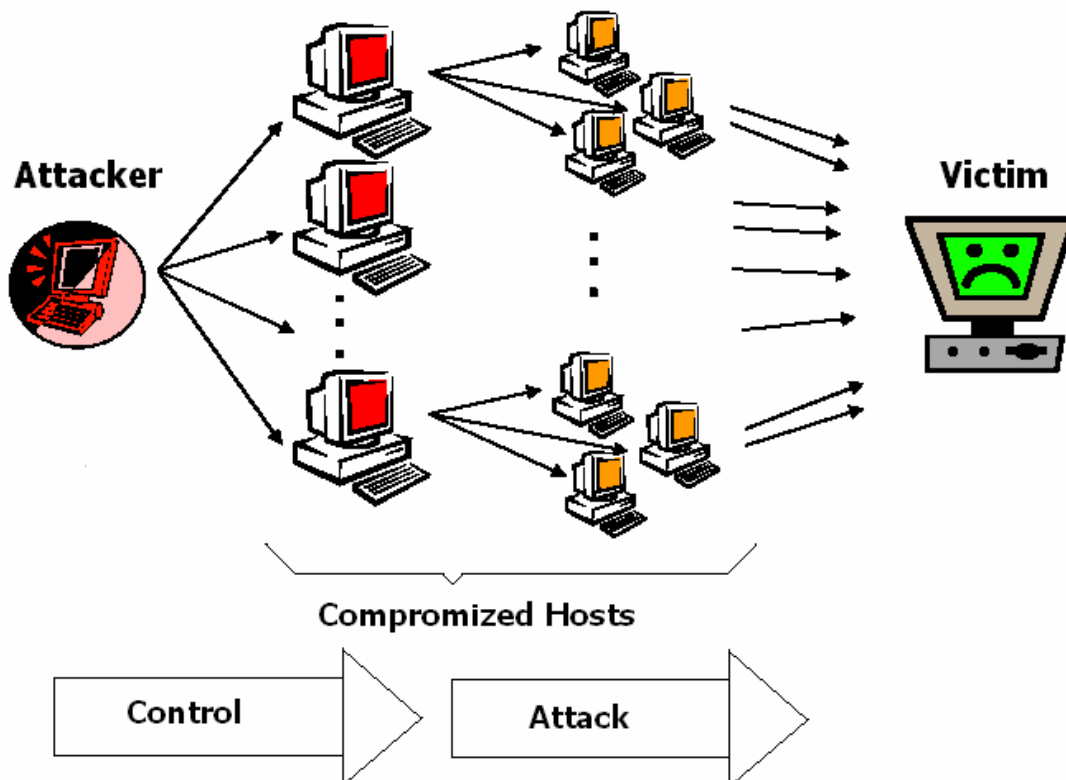
Sending Zombies via email attachment or as a file downloaded through Point-To-Point network connection.

## ***II Classification based on the control of commands:***

**1- Controlled DDoS:** the attacker gives the command of attack.

### **1-1 Spoofed DDoS**

The Attacker places a malware in some server on the internet called Zombie, with tree hierarchy. And he controls all the Zombies and let them start the attack in the same time. The Zombies send SYN packets to the victim and do not answer to the SYN\_ACK packet from the victim, this will force the victim to open many timers and if the number of Zombies is bigger than the capacity of the victim, then any legitimate user won't be able to connect to the victim.

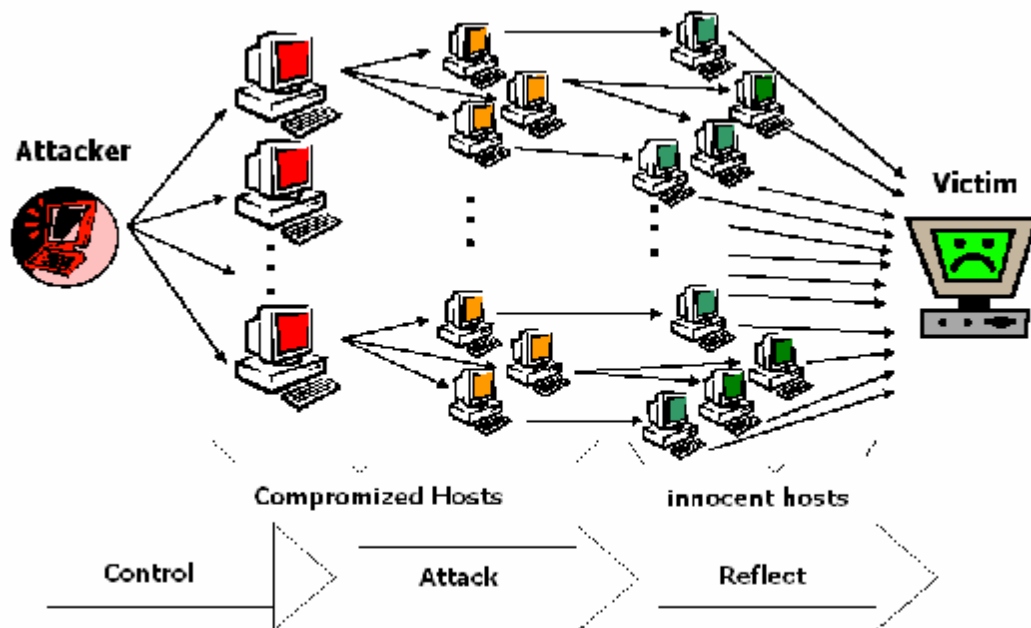


**1-2 Spoofed then reflector attack (DRDoS):** [19]

In the following picture we see the schema of DRDoS attack, that is similar to the spoofed DDoS attack except the final phase where there is new level of innocent hosts before the victim, the final level of compromised hosts will send packets to the innocent host with a spoofed source address set to victim address. All the innocent hosts will reply to the same Victim host.

Any Protocol which replies with a packet after it has received a request can be used in this attack. In this type we don't need a compromised end level servers, they are innocent hosts and do not contain any Zombies.

Some of the candidate servers are WEB Servers, FTP Servers, DNS, Gnutella Servers and Routers). These servers answer to a SYN packet with a SYN-ACK packet or RST packet or with ICMP packet.[23]



### 1-3-DDoS using Internet Relay Chat (IRC) network:

The DDoS attacker tries to find another way of communication with the Zombies since one of the defending way against them is finding the control and communication traffic. And a new generation of DDoS attack start using IRC network to communicate with the zombies and that eliminate the need for custom protocol.

#### *What is Internet Relay Chat?* [17]

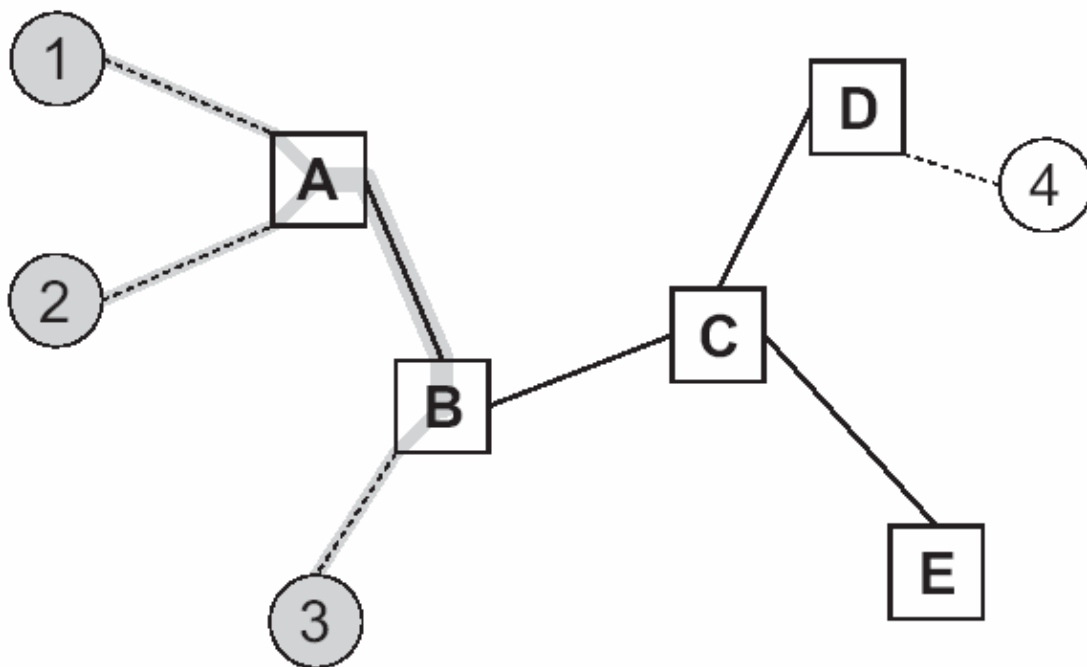
The birth of IRC was on 1988 when Jarkko Oikarinen Was trying to improve the software of Bulletin Board System (BBS) to make real time discussion in

the University of Oulu (Finland), then this protocol spread across the entire internet.

On 1989 there were only 40 IRC server worldwide, but now there is more than 5000 server.

The idea of this Network is so simple, it is just a chat program that can make conversation between 2 clients or more, and some of these conversations could be private protected with a password. Some users could use a "Channel" to talk about the same subject.

In the following picture we can see a IRC network with 5 server and 4 users and 1 channel, 3 users join the same channel.



Servers: A, B, C, D, E

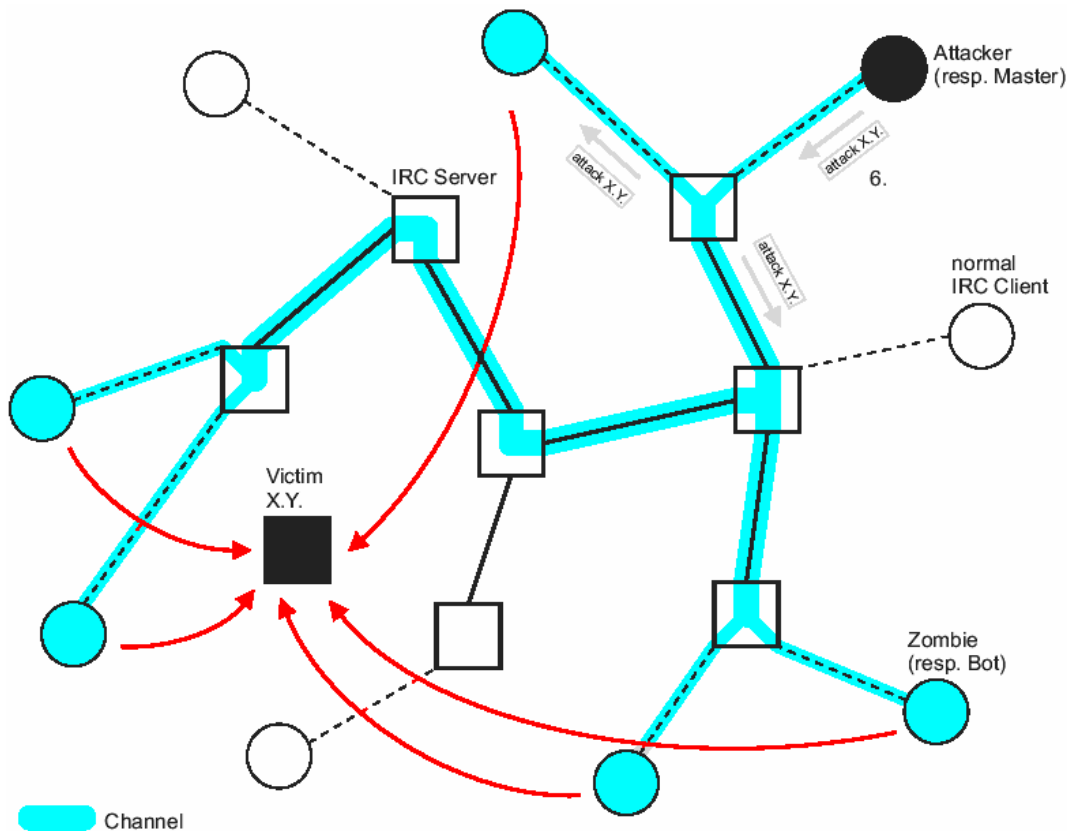
Clients: 1, 2, 3, 4

Channel

Some clients having joined the same channel [17]

This flexible network attract the attention of the attackers, they found it a good place to hide their communications.

The following picture demonstrates how the attacker can use the IRC network to connect with the Zombies.



IRC-based DDoS attack architecture [17]

#### 1-4-DDoS using Peer-to-Peer (P2P) file sharing network:

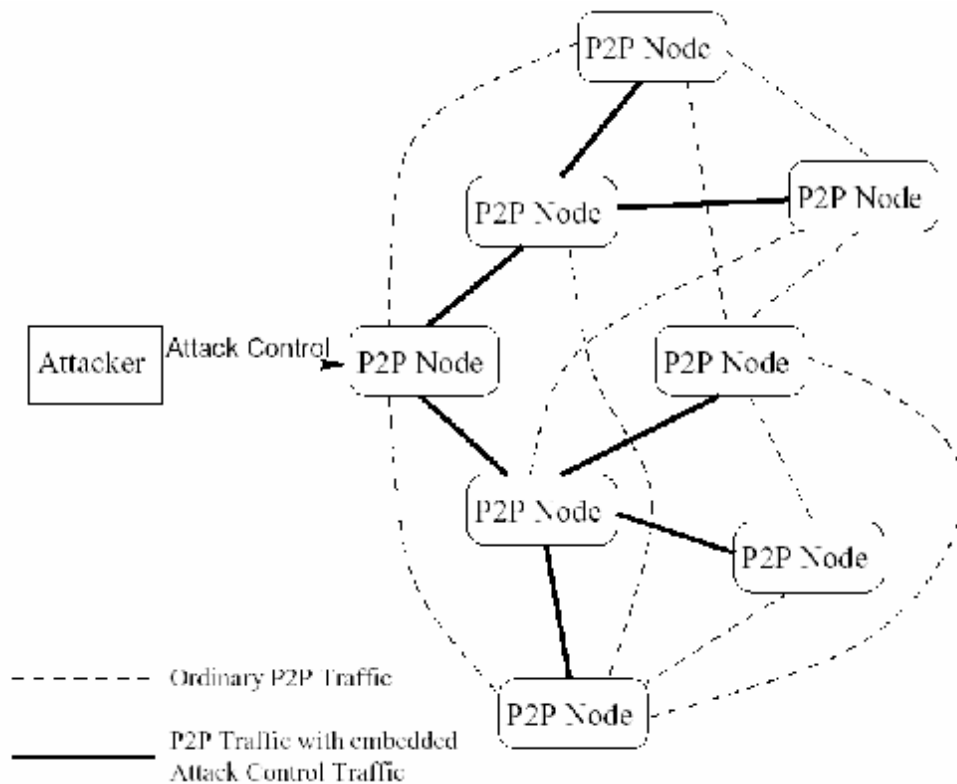
We saw in the previous paragraph a method of connection between the attacker and Zombies. In this paragraph we will study another method of communication based on P2P networks.

##### *What is a Peer to Peer network?* [5]

P2P systems are widely popular, it is method for sharing files between different nodes, and we can search about a file, download or upload a file. The important feature in this network that there is no servers; any computer of the internet can connect to P2P network.

One of the advantages in using P2P networks in DDoS attacks is that they work on application level, so the attacker has larger number of machine to infect and no need to know anything about the operating system,

Some of the famous P2P applications are: Napster, Gnutella, Freenet.



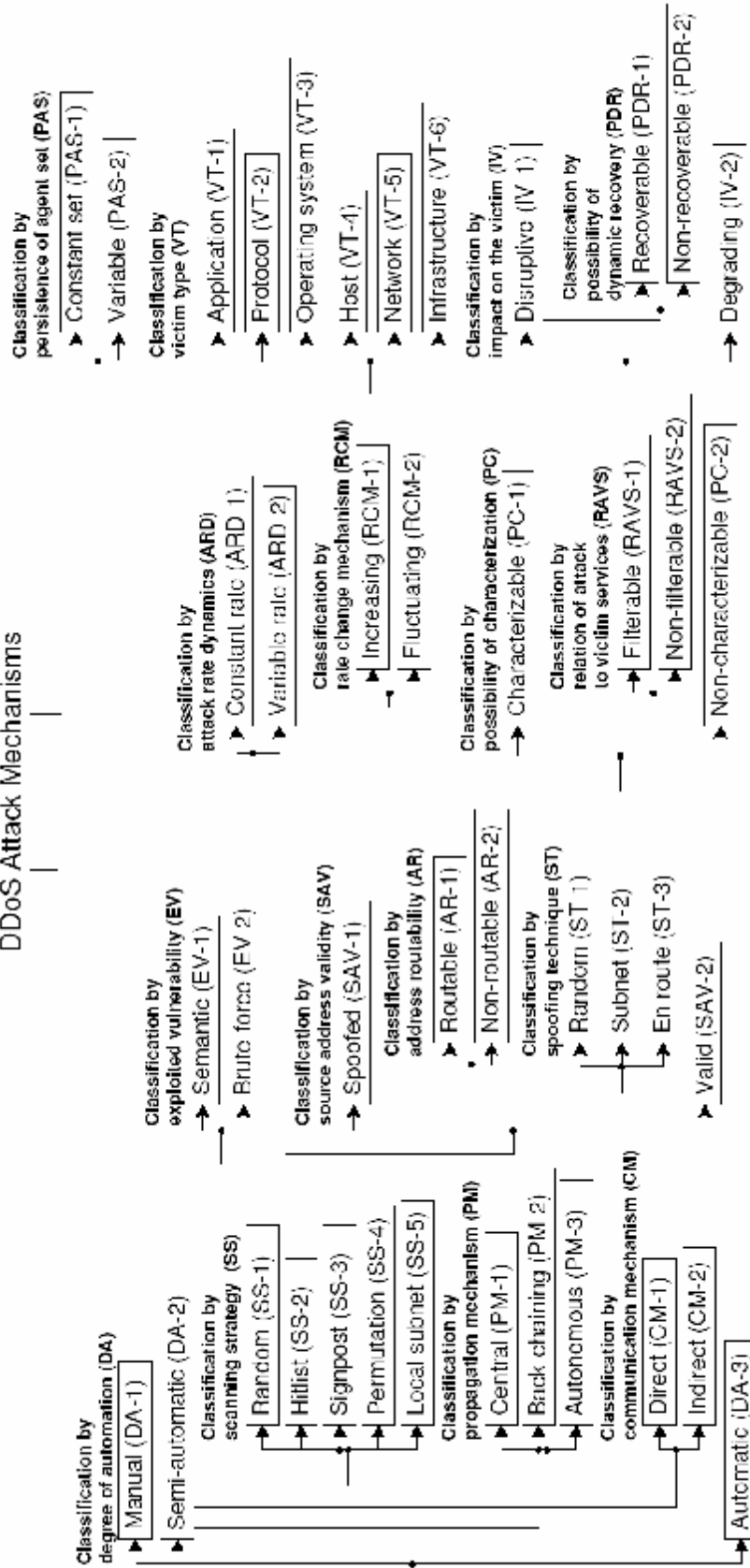
Possible Attack Control Scenario [5]

**2- Non Controlled DDoS:** There is no command of attack, all the program are pre configured to make the attack at a specific time like the worm MyDoom: the intruder designed it to automatically send significant amounts of traffic to [www.sco.com](http://www.sco.com) on February 1, 2004 and [www.microsoft.com](http://www.microsoft.com) on February 3, 2004.

***Classification of DDoS attack from [14]***

Jelena Mirkovic made a great classification in his PHD theses  
The following picture represents the Mirkovic taxonomy of DDoS attack.

## DDoS Attack Mechanisms



We will explain some of this category, please refer to [14] for more details. Mirkovic made eight main criteria for attack classification, some of these criteria have sub criteria.

The main eight criteria are:

- 1- ***Degree of automation:*** any phase of the attack could be Manual or Semi Manual or Automatic. (this is the category that I mentioned in my last paragraph: ***II Classification based on the control of commands***)
- 2- ***Exploited vulnerability:*** (semantic or Brute-Force) dose the attack use a bug in the system or it just flood the network with many packets. The difference between semantic and brute-force is that the defense of semantic attack can be done via upgrade the vulnerable software, but this solution did not affect Brute-Force attack.
- 3- ***Source address validity:*** Dose the address spoofed or valid.
- 4- ***Attack rate:*** Constant Rate or Variable (Increase or Fluctuating) Rate, the constant rate can be discovered rapidly, but the variable rate is difficult to discover rapidly.
- 5- ***Possibility of characterization:*** attacks can be characterizable or not for example UDP flood attack to a web server can be eliminate soon since web server do not use UDP. But TCP attack to a web server is not be characterizable
- 6- ***Persistence of agent set:*** all the agent attack in the same time or some agent attack in different time. The second case is difficult to defend since Zombies are not attacking in the same time.
- 7- ***Victim type:*** the victim can be application, protocol, operating system, host, network or infrastructure.
- 8- ***Impact on victim:*** The attack can be disruptive or degrading.

### 3-4 Examples of DDoS

Yankee Group predicts the cost of a 24-hour outage for a large ecommerce company would approach US\$30 million. A DDoS attacks against Amazon, Yahoo, eBay, and other major sites in February 2000 caused an estimated cumulative loss of US\$1.2 billion, according to the Yankee Group. And in January 2001, Microsoft lost approximately US\$500 million over the course of a few days from a DDoS attack on its site. [10]

### 3-5 DDoS attack tools [16]

The first attack tool was *Trinoo* or *Trino00* (1999) it uses SYN flood using master and zombies that communicate via especial ports.

Second tools were *Tribe Flood Network (TFN)*: it use SYN or ICMP or UDP flood or smurf attack. The communication between the agents is via ICMP echo and ICMP echo reply.

After *Trinoo* and *TFN* in the summer of 1999 new tools was introduces: *Stacheldraht*, it combines features of *trinoo* and *TFN* and contains some advanced features, such as encrypted communication and automated agent updates.

After this tools there is *Trinity* witch have the same capabilities of *Stacheldraht*, but it use the Internet Relay Chat to communicate between its agents.

*Shaft* DDoS tool was introduced in November 1999. It is similar to a *trinoo*; and it have interesting signature that the sequence number for all TCP packets is 0x28374839.

*Tribe Flood Network 2K (TFN2K)* was introduced in December 1999. It is similar to the original *TFN* and have many features that make *TFN2K* traffic difficult to recognize and filter, like hiding the true source of the attack using IP address spoofing.

# Chapter 4

## Defense against DDoS

### 4-1 Introduction:

A successful defense should meet the following requirements: [14]

- **Accurate detection:** The system must detect any attack.
- **Effective response:** The system must stop any attack regardless of its size and distribution.
- **Selective response:** The system must distinguish between the legitimate packets and the attacker packets, and provide the legitimate users good service.

There are two characteristic of DDoS that make it difficult to defend:

1- DDoS traffic is similar to normal traffic.

2- DDoS traffic is distributed: the attack comes from distributed nodes in the network.

### 4-2 Defense Taxonomy:

#### *Classification of Defense against DDoS attack from [14]*

Mirkovic made three main criteria for classification the defense against the attack, all of them have sub criteria.

#### *1- Activity Level*

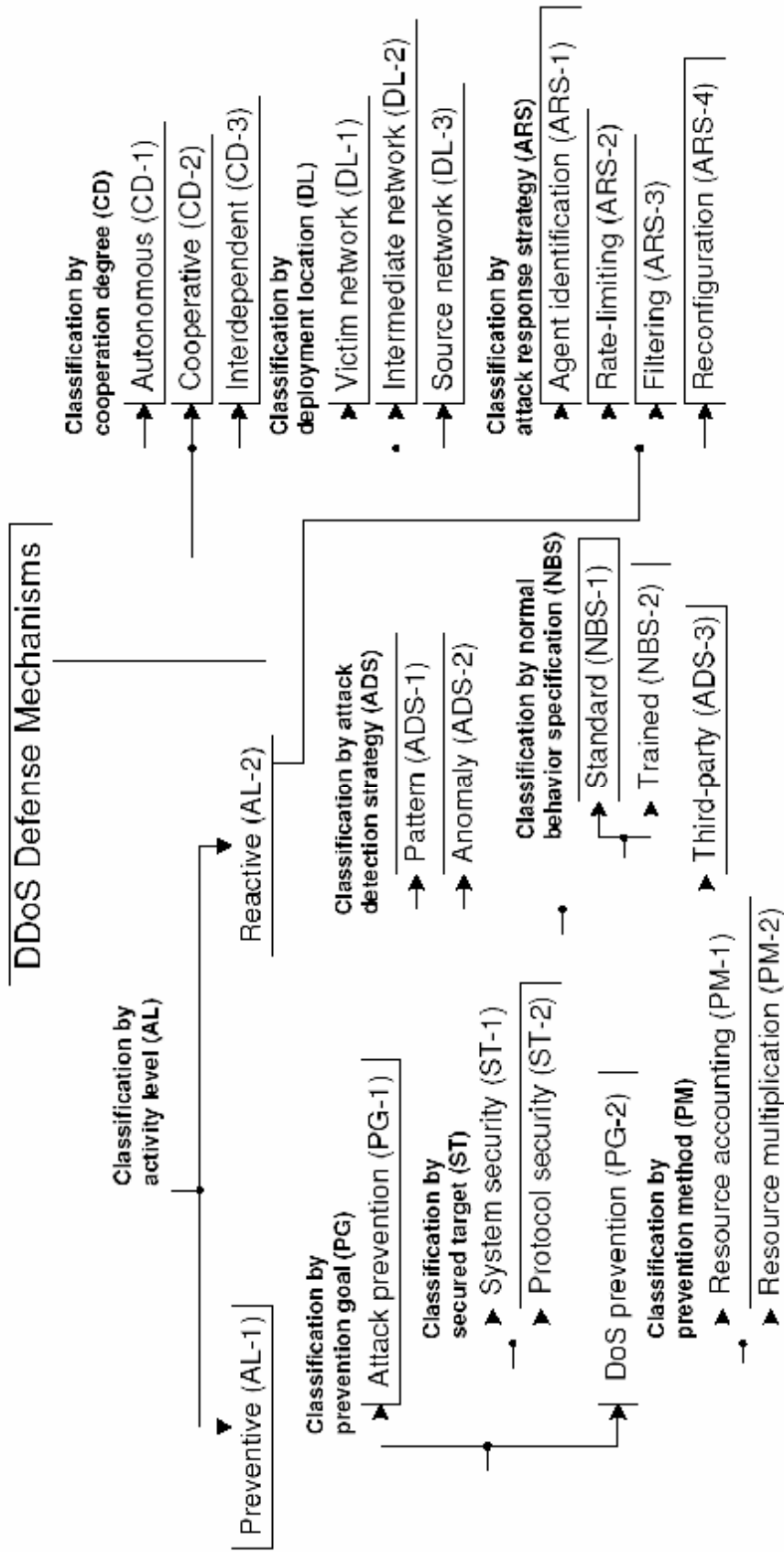
- a. **Preventive:** Prevent DDoS attack via changing the system or the protocols.
- b. **Reactive:** detect the attack then defense it. The detection can be *Pattern* (use signature detection), *Anomaly* (compare with normal) or *Third party*.

The response strategy can be one of the following:

- i. *Agent Identification*
- ii. *Rate Limiting*
- iii. *Filtering*
- iv. *reconfiguration*

- 2- **Cooperation Degree:** the victim can defense the attack alone or get help from other hosts.

- 3- ***Deployment Location:*** defense can be at:
- a. Victim Network:
  - b. Intermediate Network:
  - c. Source Network:



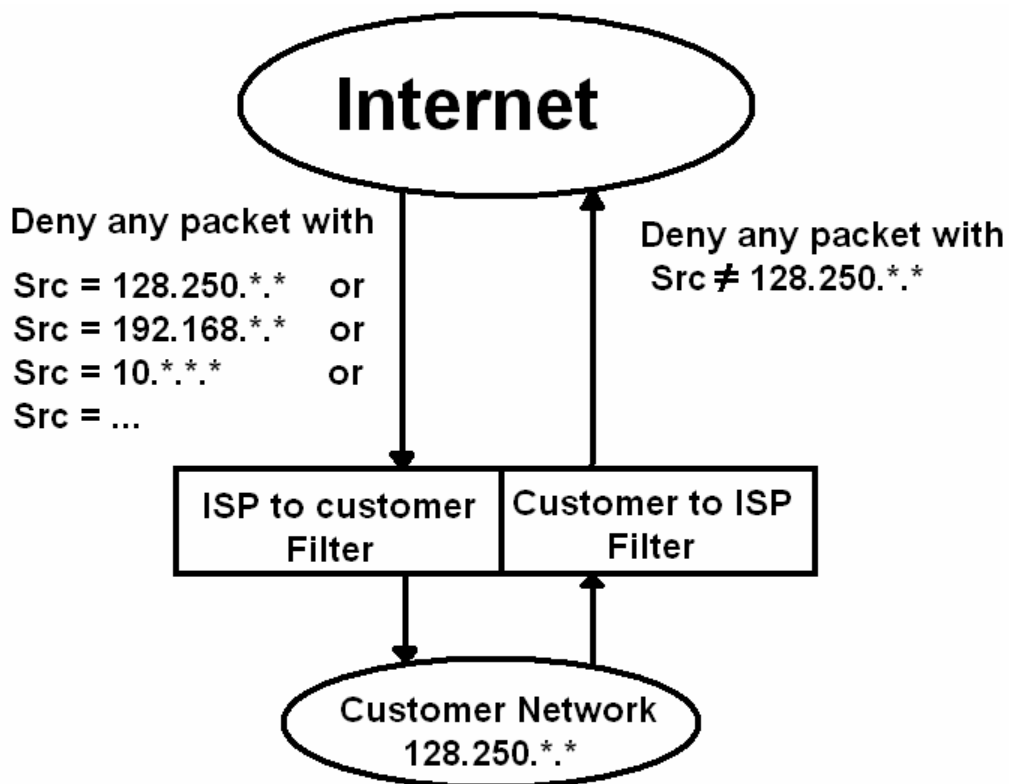
### 4-3 Defense Steps:

Tao Peng has made a good analysis concerning the defense against DDoS in his PHD theses, he divides the defense into four steps: [18] Best defense can use all the steps together.

1. **Attack prevention:** it is a mechanism for stopping the attack before it start and cause damage, it should fix security holes, such as insecure protocols, weak authentication and vulnerable computer systems. It needs Global cooperation.

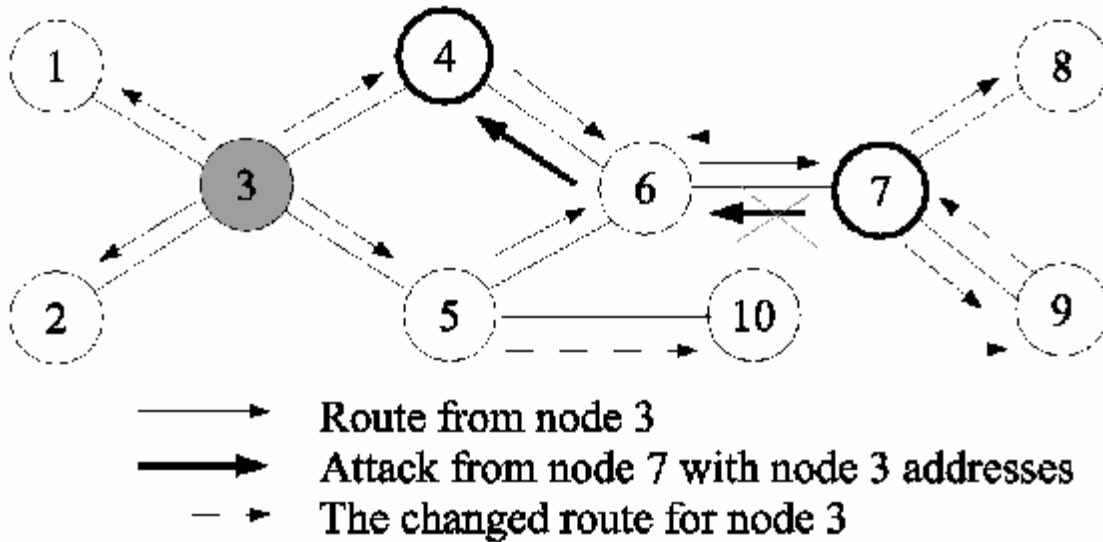
Since the most common attacks use spoofing to hide the attacker, preventing the attack can be done by eliminate or filtering any spoofed packet.

- a. **Ingress Filtering:** filter the incoming or outcoming traffic according to specific rules. The following picture show how it works:



Deny any incoming packet that has source IP address belong to customer network or private network. And deny any outcoming packet that has IP address not belong to internal network address.

**b. Router-based Packet Filtering:** this defense tries to filter spoofed traffic at routers instead of at victim side. The main rule used to filter the spoofed traffic is that generally the packets use the same path so if a router receives a packet with a new source address, that mean this address is spoofed. The main problem with this assumption is that in case of failure of some routers the path will be changed.



Router based packet filtering [18]

- c. **Source Address Validity Enforcement (SAVE) Protocol:** this protocol solve the problem of dynamic routing of the previous packet filtering, it send a SAVE message when there is a change in routing tables.
- d. **Hop count filter** [8]: This technique detect spoofed packet by inspecting each packet hop count and compare it with a table containing a mapping between IP address and hoop count. This defense can be done on the victim server or on routers, it is better to put it on routers to avoid bandwidth attack.

**Prevention analysis:** all preventing technique deal with spoofed DDoS, in fact with the availability of many vulnerable hosts, the attacker can use these host to start DDoS attack without the need of using spoofing. And the last two techniques need global implementation which is hard to do with more than 10000 routers.

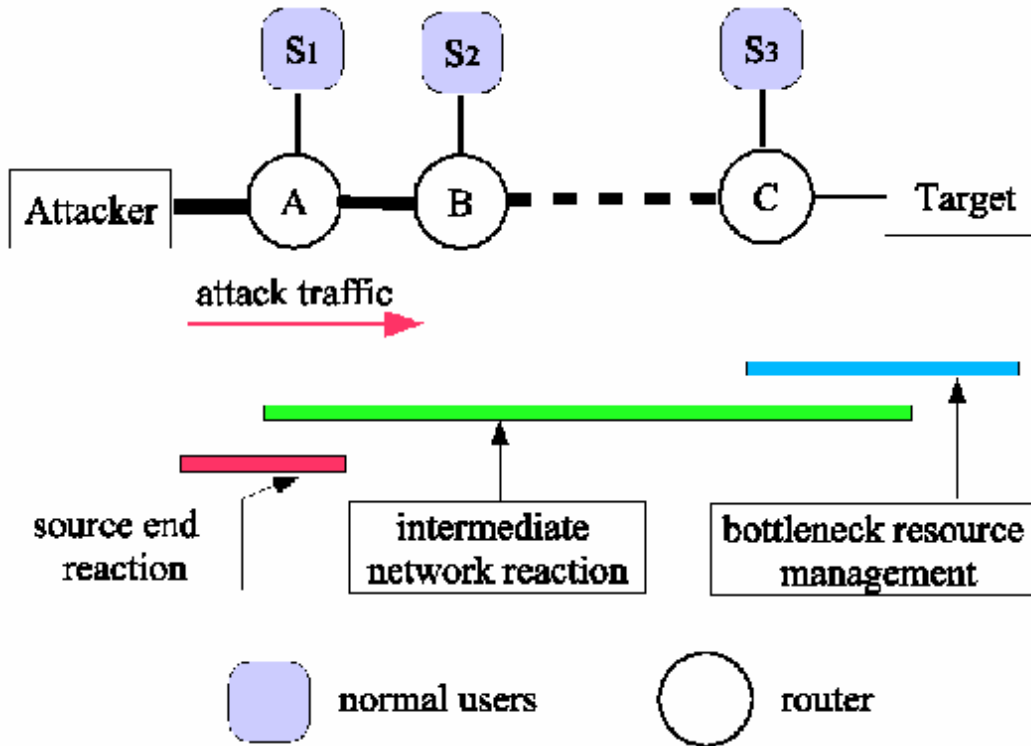
2. **Attack detection:** detect DoS in the beginning of the attack to reduce its effect, and to detect the source of the attack to filter it.
  - a. **DoS-attack-specific Detection:** based of specific feature of DDoS that make it different from normal traffics.
    - i. **MULTOPS:** packets rate between two hosts are proportional during normal operation, when this proportion changed, we have DDoS Attack.
    - ii. **SYN and Batch Detection:** use some statically information such as the ratio of SYN and FIN and RST. When this ratio changed we have DDoS.
    - iii. **Spectral Analysis:** in this approach the number of packet arrived in a fix interval is used as a signal, and a spectral analysis of the density of the signal is used to detect any DDoS attack.
    - iv. **Kolmogorov Test:** the DDoS traffic has many similar proprieties like destination address and protocol, but normal traffic dose not have this similarity. If we use the correlations between the traffics we can detect DDoS.
    - v. **Time Series Analysis:** this method is based on the strong correlation between the traffic behavior in the victim and attacker. There are three steps in this method: the first is selecting the criteria (in ICMP flood: the number of ICMP echo) second step is the check every suspicious machine, third step is to build a normal profile using the founder variables.
  - b. **Anomaly-based Detection:** model the normal traffic and compare any new traffic with this model to find abnormal traffics. The advantage of this method is that it can detect new type of attacks.
    - i. **Statistically-based Anomaly Detection:** build a normal model using statically measurement like packet length and rate. Then calculate the similarity distance between observed packets and normal model.
    - ii. **Artificial Immune System:** using artificial intelligence we can build a model of neural network help us to detect attacks, we represent the packet as a string, during training period we represent many packets as normal string, then we go to real packets and with a good threshold we can detect the abnormal packets.

**Detection analysis:** all *attack-specific* detection technique uses some assumptions. For example *SYN and Batch* use the assumption that in SYN flooding the number of SYN is more than FIN & RST, but the attacker can send FIN + RST to avoid detection. *Anomaly-based* have a problem of speed, when we increase the speed we will have the problem of false positive (legal packets that are detected as illegal).

3. **Attack source identification:** locate the attack sources regardless of the spoofed source IP addresses.
  - a. **IP Traceback by Active Interaction:** when a DDoS attack start, all routers will reject any packet to the victim and send ICMP host unreachable error message to the source IP address (it may be spoofed IP address) and all the router will detect any ICMP message with invalid IP address (since spoofed IP address usually contain no routable addresses) and they send all the messages to an analyzer that will detect the entry point of the attack.
  - b. **Probabilistic IP Traceback Schemes:** the router will select randomly one of the packets that pass throw it, then it stores its IP address in this packet for future tracking. The routers may use the sequence number or option in the IP header to store the router address. With a huge amount of packet in DDoS, the victim can collect packets with different path and reconstruct the path to the attacker.
  - c. **Hash-based IP Traceback:**[7] store some information in routers for trace any packets when needed, the information are stored hashed for privacy.

**Source identification analysis:** the first method can be easily avoided by using random routable addresses instead of non routable addresses. The second method needs a non distributed attack with a huge traffic. The third method is the best, but it needs space and time for storing the information on routers.

4. **Attack reaction:** eliminate the effects of an attack. We can divide this step into 3 levels as shown in the following picture:



DoS attack reaction schemes [18]

- a. **Bottleneck Resource Management:** reorganize the resource of the Host or the Network connected to the host to make it more robust and can pass around bandwidth attack.
  - i. **Host Resource Management:** modify the operating system and fix any vulnerability like the SYN-ACK problem.
  - ii. **Network Resource Management:** there is some algorithm like class based queuing (CBQ) that try to avoid the bottleneck in the connection between the router and the victim, this algorithm.
- b. **Intermediate Network Reaction:** in this approach, we try to filter the attack traffics near to attacker host. In this step we can decrease the damage of the attack, but we can not remove it completely.
  - i. **Pushback Scheme:** each router sends its adjacent routers the signature of the packets that should be filtered.
  - ii. **Controller-Agent Scheme:** the proposed solution work within one ISP domain, once we find a dirty packet, we mark it and send a command to all the agents in all routers to find the entry points of the attack.

*iii. Secure Overlay Service (SOS):* its main purpose to secure the communication between the confirm user and the victim. This protocol use a secret node called "Secret Servelt" and a known node called "Beacon" all the traffic are forwarded to Beacon, if it is legal it will be forwarded to Secret Servelt then the victim, since the last connection with the victim is unknown, the attacker will not find any method for attacking the victim.

This protocol use distributed secure overlay access points (SOAP) to authenticate the legal packets, so we should have many SOAP points to get a good performance.

*c. Source End Reaction:* Mirkovic proposed a solution called D-WARD [14], this solution monitor the source network and the internet, and store statistical information about the packets and traffics on the internet. Then he compares the statistic model with the current model, in case of difference it will alarm about DDoS and filter the origin of the suspicious packets.

#### ***Attack reaction analysis:***

The problem with *Bottleneck Resource Management* is that it need additional resources to be bigger than the attackers resources, but not all the company can afford the prices for increasing the bandwidth and the enlarge server capacity. Even when big company like Microsoft and Yahoo use this solution, they are still vulnerable for distributed attacks like the code red worm.

In the *Intermediate Network Reaction*, we could not stop the attack; we can only decrease its effect since we are still far from the attacker.

The *Source End Reaction* should be the best solution since it is near to the victim, and there will be no waste of resources. But this solution still has problems with distributed entry points.

## 4-4 Defense Method Comparison:

Attack prevention:

<b>Attack prevention</b>	<b>Effectiveness</b>	<b>Global Solution</b>	<b>Speed</b>	<b>Changing Hardware</b>	<b>Best of them</b>
<i>Ingress Filtering</i>	Problem with non spoofing attack	No	1: faster	No	4: filter near victim
<i>Router-based Packet Filtering</i>		Yes	2	Yes	3: Problem with dynamic routing
<i>SAVE Protocol</i>		Yes	3	Yes	1: The Best
<i>Hop count filter</i>		Yes if implemented on routers	4	If implemented on routers	2: need more storage and calculation

Attack detection:

<b>Attack detection</b>	<b>Effectiveness</b>	<b>Global Solution</b>	<b>Technical complexity</b>	<b>Speed</b>	<b>Best of them</b>
<i>MULTOPS</i>	Based on specific assumption that can be changed	Yes	Low	1: fastest	3
<i>SYN and Batch</i>			Low	1	5
<i>Spectral Analysis</i>			High	2	4
<i>Kolmogorov Test</i>			High	3	4
<i>Time Series Analysis</i>			Medium	2	4
<i>Statistically-based Anomaly</i>	A general solution that can detect new types		High	4	2
<i>Artificial Immune</i>			High	4	1 Best : complex problem need AI

Attack source identification:

<i>source identification</i>	Global Solution	Speed	Changing Hardware	Best of them
<i>IP Traceback by Active Interaction</i>	Yes	3: need extra communications	Yes: Routers	3: need bad spoofed address for detection
<i>Probabilistic IP Traceback Schemes</i>	Yes	2	Yes: Routers	2: Need huge amount of packets
<i>Hash-based IP Traceback</i>	Yes	1: faster	Yes :routers	1: Best can detect even one packet

Attack reaction:

<i>Attack reaction</i>	Effectiveness	Global Solution	Changing Hardware	Best of them
<i>Host Resource Management</i>	High price for increasing resources	No	Host	3
<i>Network Resource Management</i>		At Router close to Victim	1 Router	3
<i>Pushback Scheme</i>	Rely on detecting signature	Yes	Routers	2
<i>Controller-Agent Scheme</i>	One ISP!	Yes	Routers	2
<i>Secure Overlay Service</i>	Problem with SOAP	Yes	Routers	2
<i>Source End Reaction</i>	D-WARD	Yes	Routers	1

# Chapter 5

## Conclusion and Recommendations

We presented the several types of attacks. We presented also the different types of DDoS attacks and their taxonomy.

The main problem in DDoS is the distribution of the attack entry points and the difficulty to know the origin of the attack with the current infrastructure.

We studied two main types of DDoS: Controlled attack and non controlled attack. The Controlled attack use spoofing to hide the origin of the attacker, So we can defense this type if we could stop spoofing and this can be done with some technique that impose changes to the routers.

The second type is harder to defend since it may not use spoofing and since it may not use communication between the master and the zombies. This type of attack uses the vulnerable hosts on the internet, which are increasing day after day...

The dense against this type of attack can be done by impose new rules and policies on vulnerable hosts. But this solution is impossible to implement since most of this machine dose not have administrator and it is used by normal users.

Our study classifies all the defense method to the DDoS, and we make comparisons between them. There is no magic solution, this fields still good research subject since 10 years, and I it still waiting for a better solution.

## REFERENCES

- [1] Alefiya Hussain, John Heidemann, Christos Papadopoulos, A framework for classifying denial of service attacks, In Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications, August 2003.
- [2] Aleksandar Kuzmanovic, Edward W. Knightly, Denial-of-service: Low-rate TCP-targeted denial of service attacks, In Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications, August 2003.
- [3] Andrew S. TANENBAUM, 2003, PH PTR, Computer Networks fourth edition.
- [4] Anonymous, 2001, SAMS, Maximum Security Third edition.
- [5] Arno Wagner, Bernhard Plattner, Peer-to-Peer (P2P) systems, are good for DDoS, Swiss Federal Institute of Technology Zurich, Computer Engineering and Networks Laboratory, 2002.
- [6] CERT/CC Statistics, URL [http://www.cert.org/stats/cert\\_stats.html](http://www.cert.org/stats/cert_stats.html).
- [7] Chao Gong, Kamil Sarac, IP Traceback based on Packet Marking and Logging, Department of Computer Science University of Texas at Dallas, USA,2005.
- [8] Cheng Jin, Haining Wang, Kang G. Shin, Hop-count filtering: an effective defense against spoofed DDoS traffic, Proceedings of the 10th ACM conference on Computer and communications security, October 2003.
- [9] Cliff Changchun Zou, Lixin Gao, Weibo Gong, Don Towsley, Monitoring and early warning for internet worms, In Proceedings of the 10th ACM conference on Computer and communications security, October 2003.
- [10] DEFEATING DDOS ATTACKS, Whitepaper, Cisco Systems, 2004.
- [11] Ed Skoudis, 2002, Counter HACK, Printice Hall.
- [12] Lisa Yeo, 19-Dec-02, Printice Hall PTR, Personal Firewalls for Administrators and Remote Users.
- [13] Marco de Vivo, Eddy Carrasco, Germinal Isern, Gabriela O. de Vivo, A review of port scanning techniques, ACM SIGCOMM Computer Communication Review, Volume 29 Issue 2, April 1999.
- [14] Jelena Mirkovic, D-WARD: Source-End Defense against Distributed Denial-of-Service Attacks, Ph.D. Thesis in University of California Los Angeles, 2003.

- [15] Jelena Mirkovic, Peter Reiher, A taxonomy of DDoS attack and DDoS defense mechanisms, ACM SIGCOMM Computer Communication Review, Volume 34 Issue 2, April 2004.
- [16] Prateek Mittal, Defense against Distributed Denial of Service Attacks, A seminar report in Department of Computer Science and Engineering Indian Institute of Technology, April 19, 2005.
- [17] Stéphane Racine , Analysis of Internet Relay Chat Usage by DDoS Zombies, Master Thesis in Swiss Federal Institute of Technology Zurich, Apr 2004.
- [18] Tao Peng, Defending Against Distributed Denial of Service Attacks, Thesis in the University of Melbourne, April 2004.
- [19] Thomas Dübendorfer, Adaptive Distributed Traffic Control Service for DDoS Attack Mitigation, 1st International Workshop on Security in Systems and Networks (SSN 2005) hold in conjunction with IEEE IPDPS 2005 Conference, April 4-8, 2005 in Denver, Colorado.
- [20] Thomas W. Doepfner, Philip N. Klein, Andrew Koyfman, Using router stamping to identify the source of IP packets, In Proceedings of the 7th ACM conference on Computer and communications security, November 2000.
- [21] William Stallings, 2003, Printice Hall PTR, Cryptography and Network security principles & practice 3d edition.
- [22] Wu-chang Feng, The case for TCP/IP puzzles, In Proceedings of the ACM SIGCOMM workshop on Future directions in network architecture FDNA '03, Volume 33 Issue 4, August 2003.
- [23] [www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html](http://www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html) , 13/7/2006
- [24] [www.us-cert.gov/cas/techalerts/TA04-028A.html](http://www.us-cert.gov/cas/techalerts/TA04-028A.html), 13/7/2006.