International Journal of Latest Research In Engineering and Computing (IJLREC)
Volume 1, Issue 1 : Page No.56-63, September-October 2013
www.ijlrec.com

Detection and Mitigation DDoS Defence Techniques to Strengthen Intrusion Prevention Systems

V.Suresh[1], Dr.A.Rajiv Kannan[2], K.Sudhakar[3]
[1]Assistant Professor, IT, Sengunthar College of Engineering, Tiruchengode, India
[2]Professor & Head, CSE, K S R College of Engineering, Tiruchengode, India
[3]Asst Prof & Head, CSE, Sengunthar College of Engineering, Tiruchengode, India

Abstract: Nowadays, guarantee of secure communication is as important as the traditional computer and information security assurance. Presently Distributed Denial of Service (DDoS) Attacks are causing billions of dollars losses by affecting the normal functioning of organizations. DDoS attackers are infiltrating large numbers of computers by exploiting software vulnerabilities. By the time specific countermeasures are developed to prevent DDoS attacks, attackers enhance existing DDoS attack tools, developing new and derivative DDoS attack tools and techniques. Organizations are trying their best to minimize their losses from these systems. However, most of the organizations widely use the Intrusion Prevention Systems (IPS) to observe and manage their networks. In this paper the Preventive, Detective and Mitigation DDoS Defence techniques and Mechanisms have been discussed to strengthen existing IPS concepts, which can help to develop a new and intelligent Network Intrusion Prevention System. A new technique for an intelligent and smart Intrusion Prevention system has been introduced on the basis of Captcha, IP addresses, MAC Addresses and Application_Id.

Keywords: Intrusion Prevention System, Preventive, Detective & Mitigation Techniques, Application_Id.

INTRODUCTION

Prevention of illegitimate traffic is one of the goals of communication security and seeks to prevent an eavesdropper from gaining any meaningful information about network users' behavior or objectives by observing the legitimate traffic on the network. Denial of service attacks have become a growing problem over the last few years resulting in large losses for the victims [2]. One good example of this loss is the attacks of Yahoo, CNN, and Amazon in February of 2000 which had an estimated loss of several million to over a billion dollars [8]. This paper will discuss the concepts of denial of service attacks, how they can be detected, and some of the most common ways of mitigating the damage they can inflict upon their victims.

Distributed Denial of Service (DDoS) attacks are a virulent, frequent type of attack on the availability of Internet services and resources. DDoS attackers infiltrate large numbers of computers by exploiting software vulnerabilities, to set up DDoS attack networks. These unwitting computers are then invoked to wage a coordinated, large-scale attack against one or more victim systems. As specific countermeasures are developed, attackers enhance existing DDoS attack tools, developing new and derivative DDoS techniques and attack tools. Rather than react to new attacks with specific countermeasures, it would be desirable to develop comprehensive DDoS solutions that defend against known and future DDoS attack variants. However, this requires a comprehensive understanding of the scope and techniques used in different DDoS attacks.

After this introduction part rest of the paper is organized as follows: Investigation of DDoS attack problem is given in Section 2; DDoS Attack Defence Mechanisms have been proposed in Section 3; Proposed Intrusion Prevention System has been given in Section 4; Related work has been discussed in Section 5 and paper is finally concluded in Section 6.

MATERIALS AND METHODS

A. DDoS Attacks

A DDoS attack can be characterized by an explicit attempt of attackers to prevent legitimate users of a service from using that service. E.g. :

- 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

Distributed denial of service attacks are basically denial of service attacks perpetrated by many systems at the same time on a single victim. Such an attack occurs in two phases, the recruiting stage where the attacker recruits machines infecting them with an attack code and the actual attack phase when the recruited machines run the attack code [14]. Some tools used by attackers in the past have included Trinoo (Trojan horse first discovered on December 30th 1999) [5], Tribe Flood Network (capable of UDP, ICMP, SYN Flood attacks as well as Smurf attacks) [3] and stacheldraht (based on Tribe Flood Network's Code) [4].

Denial-of-service attacks come in a variety of forms and aim at a variety of services. There are three basic types of attack:

- Consumption of scarce, limited, or non-renewable resources
- Destruction or alteration of configuration information
- Physical destruction or alteration of network components

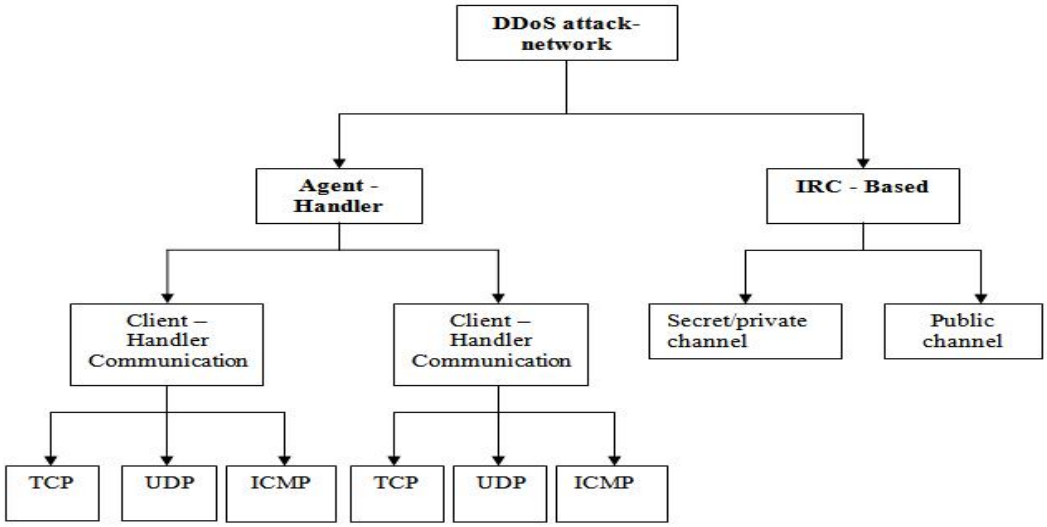

Fig 1: DDoS Attack Network [6]

Distributed denial of service attacks can be deeply analyzed and broken into a variety of components [1]. Figure 1 shows two main types of DDoS attack networks: the Agent-Handler model and the Internet Relay Chat (IRC-Based) model.

B. Agent-Handler Model

An Agent-Handler DDoS attack network consists of clients, handlers, and agents (Figure 2). The client platform is where the attacker communicates with the rest of the DDoS attack network. The handlers are software packages located on computing systems throughout the Internet that the attacker uses to communicate indirectly with the agents. The agent software exists in compromised systems that will eventually carry out the attack on the victim system.

The attacker communicates with any number of handlers to identify which agents are up and running, when to schedule attacks, or when to upgrade agents. Depending on how the attacker configures the DDoS attack network, agents can be instructed to communicate with a single handler or multiple handlers. The communication between attacker and handler and between the handler and agents can be via TCP, UDP, or ICMP protocols. Sometimes handler and agents are known as master and daemons. The systems that have been violated to run the agent software are referred to as the secondary victims, while the target of the DDoS attack is called the (primary) victim.

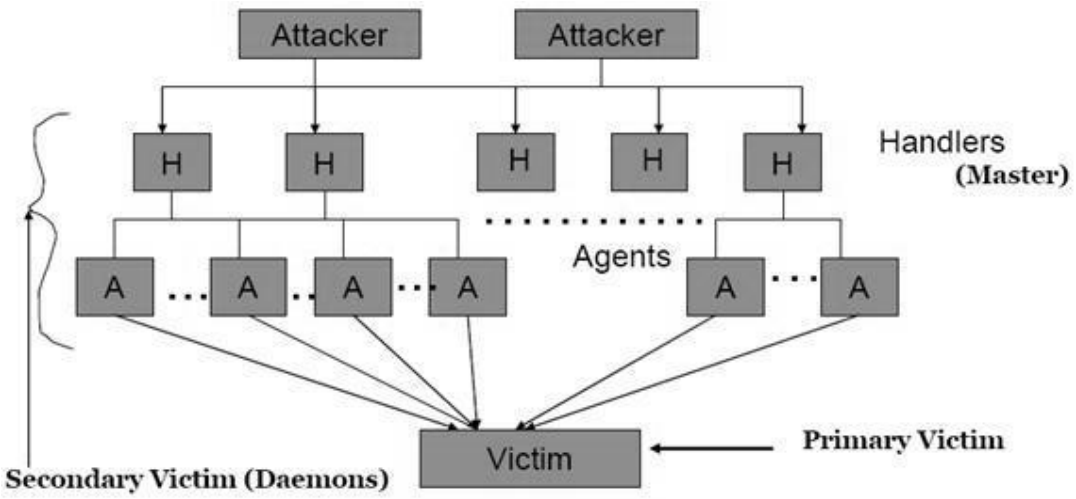

Fig 2: Agent-Handler Model

C. IRC Based Attack Models

Internet Relay Chat (IRC) is a multi-user, on-line chatting system. It allows computer users to create two-party or multi-party interconnections and type messages in real time to each other [9]. IRC chat networks allow their users to create public, private and secret channels. Public channels are channels where multiple users can chat and share messages and files. [10]. Private and secret channels are set up by users to communicate with only other designated users. Both private and secret channels protect the names and messages of users that are logged on from users who do not have access to the channel [11].

An IRC-Based DDoS attack network is similar to the Agent-Handler DDoS attack model except that instead of using a handler program installed on a network server, an IRC communication channel is used to connect the client to the agents. By making use of an IRC channel, attackers using this type of DDoS attack architecture have additional benefits. For example, attackers can use "legitimate" IRC ports for sending commands to the agents [12]. The agent software installed in the IRC network usually communicates to the IRC channel and notifies the attacker when the agent is up and running.

In an IRC-based DDoS attack architecture, the agents are often referred to as "Zombie Bots" or "Bots". In both IRC-based and Agent-Handler DDoS attack models, we will refer to the agents as "secondary victims" or "zombies."

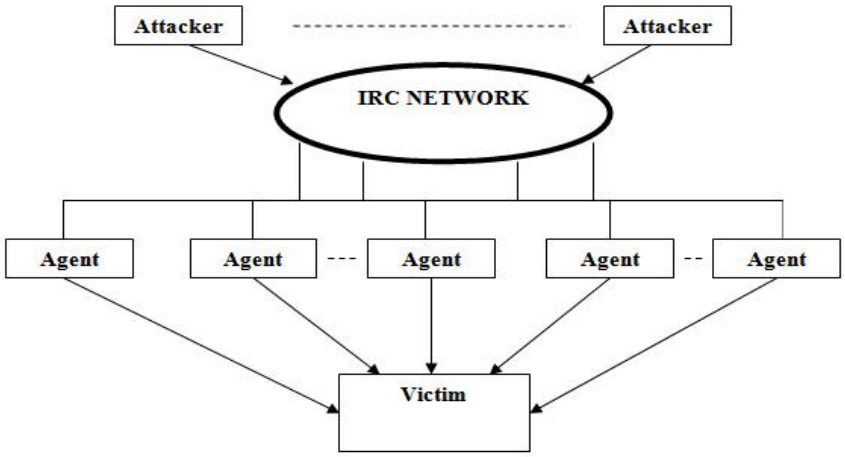

Fig 3: IRC Based Attack Model

D. Common Facilitation Characteristics:

The hackers are using following common programs in order to facilitate DDoS attacks:

- Trinoo

  Communication between clients, handlers and agents use ports, which are default ports for this tool:

  1524 tcp
  27665 tcp
  27444 udp

31335 udp

- TFN
  Communication between clients, handlers and agents use :
  ICMP ECHO and
  ICMP ECHO REPLY packets.

- Stacheldraht
  Communication between clients, handlers and agents use these ports:
  16660 tcp
  65000 tcp
  ICMP ECHO
  ICMP ECHO REPLY

- TFN2K
  Communication between clients, handlers and agents does not use any specific port, for example, it may be supplied on run time or it is chosen randomly by a program, but is a combination of
  UDP,
  ICMP and
  TCP packets.

DDOS ATTACK DEFENCE MECHANISMS

The seriousness of the DDoS problem and the increased frequency of DDoS attacks have led to the advent of numerous DDoS defence mechanisms. Some of these mechanisms address a specific kind of DDoS attack such as attacks on Web servers or authentication servers.

Other approaches attempt to solve the entire generic DDoS problem. Based on the activity level of DDoS defence mechanisms, we differentiate between preventive and reactive mechanisms

A. *Preventive Mechanisms*

The goal of preventive mechanisms is either to eliminate the possibility of DDoS attacks altogether or to enable potential victims to endure the attack without denying services to legitimate clients. According to these goals we further divide preventive mechanisms into attack prevention and denial-of-service prevention mechanisms

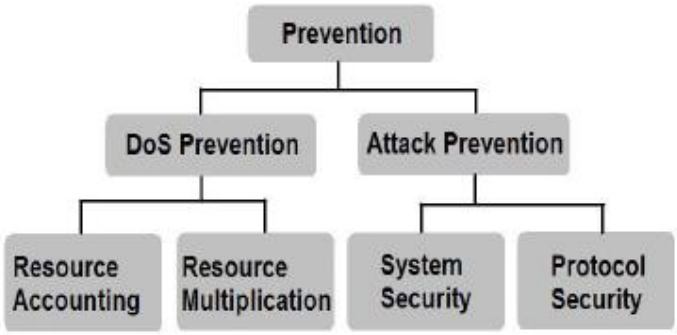

Fig 4: DDoS Prevention Defence Mechanisms.

We encourage you to consider the following options with respect to your needs:

- Implement router filters as described in [15]. This will lessen your exposure to certain denial-of-service attacks. Additionally, it will aid in preventing users on your network from effectively launching certain denial-of-service attacks.
- If they are available for your system, install patches to guard against TCP SYN flooding as described in [15]. This will substantially reduce your exposure to these attacks but may not eliminate the risk entirely.
- Disable any unused or unneeded network services. This can limit the ability of an intruder to take advantage of those services to execute a denial-of-service attack.
- Enable quota systems on your operating system if they are available. For example, if your operating system supports disk quotas, enable them for all accounts, especially accounts that operate network services. In addition, if your operating system supports partitions or volumes (i.e., separately mounted file systems with independent attributes) consider partitioning your file system so as to separate critical functions from other activity.
- Observe your system performance and establish baselines for ordinary activity. Use the baseline to gauge unusual levels of disk activity, CPU usage, or network traffic.

- Routinely examine your physical security with respect to your current needs. Consider servers, routers, unattended terminals, network access points, wiring closets, environmental systems such as air and power, and other components of your system.
- Use Tripwire or a similar tool to detect changes in configuration information or other files.

- Invest in and maintain "hot spares" - machines that can be placed into service quickly in the event that a similar machine is disabled.
- Invest in redundant and fault-tolerant network configurations.
- Establish and maintain regular backup schedules and policies, particularly for important configuration information.
- Establish and maintain appropriate password policies, especially access to highly privileged accounts such as UNIX root or Microsoft Windows NT Administrator. [7]

B. *Detective Mechanisms*

Reactive mechanisms strive to alleviate the impact of an attack on the victim. In order to attain this goal they need to detect the attack and respond to it. The goal of attack detection is to detect every attempted DDoS attack as early as possible and to have a low degree of false positives. Upon attack detection, steps can be taken to characterize the packets belonging to the attack stream and provide this characterization to the response mechanism.

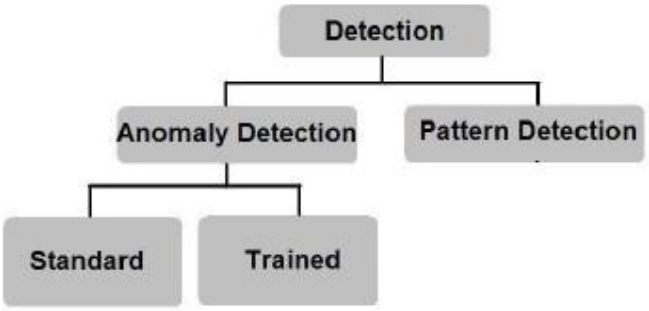

Fig 5: DDoS Detection Defence Mechanisms.

C. *Mitigation Mechanisms*

When a customer or the network infrastructure is under attack, monitoring is important for quick identification of the attack characteristics and entry points but the next question that immediately follows is, "What are you going to do to stop it?" Good mitigation techniques are a required part of a service provider's security architecture.

1. *ACLs/Rate Limiting*

Access control lists (ACL) or firewall filters are the first line of defence for a service provider. For a simple DDoS attack directed at a single customer, deployment of an egress ACL on the customer's edge router is an easy way to stop the attack. The problem with this technique is scaling both from a router performance perspective and as the number of attacks managed increases.

Operation personnel deploying the ACLs must know the performance limitation of the routers they are using. ASIC based ACLs will perform better than ACLs processed in software. Different ASICs can and do have different performance characteristics based on the packet size, interface speed and other features turned on in the router and interface cards. Most service providers have home grown scripts for their router configuration and ACL management.

Traffic loads must be monitored as the ACLs are removed to ensure that worm traffic from unpatched customers does not have a significant impact on other customers or the provider's backbone. Legitimate customer traffic may also be blocked by the ACLs and support organizations must be notified and prepared to answer customer's questions and complaints.

2. *Destination based Black Hole Filtering*

Black hole filtering is an effective, quick and simple technique for dropping attack traffic destined toward a victim. Using iBGP as a trigger mechanism, black hole filtering can be remotely triggered across the entire perimeter of a provider's network. This technique is used when more harm is done by the attack filling up a customer's circuit than by the loss of an individual site. Many times, traffic can be redirected to a different IP address through DNS.

Several variations of remotely triggered black hole filtering can be setup. By using different community strings, remote triggers can be setup for different types of routers such as edge and border. Community strings can be setup for different geographic regions or POPs in a provider's network. This flexibility allows the provider to identify the ingress points of the attack and only block traffic at those locations.

3. *Attack Distribution and/or Isolation – Anycast*

IPv4 anycast implementations have been in use on the Internet for at least the past 10 years. Particularly suited for single response UDP queries, DNS anycast architectures are in use in most tier 1 Internet providers' backbones. Anycast implementations can be used for both DNS authoritative and recursive implementations. Several root name servers are implementing anycast architectures to mitigate DDoS attacks [16]. Black hole filtering is a specialized form of anycast. Sinkholes can use anycast to distribute the load of an attack across many locations [17].

Many DNS anycast implementations are done using eBGP announcements. Anycast networks can be contained in a single AS or spam multiple AS's across the globe. Anycast provides two distinct advantages in regard to DoS / DDoS attacks. In a DoS attack, anycast localizes the effect of the attack. In a DDoS attack, the attack is distributed over a much larger number of servers, distributing the load of the attack and allowing the service to better withstand it.

PROPOSED INTRUSION PREVENTION SYSTEM

Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS), are network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about said activity, attempt to block/stop activity, and report activity. The Intrusion Prevention Systems are placed in-line and are able to actively prevent/block intrusions that are detected. More specifically, IPS can take such actions as sending an alarm, dropping the malicious packets, resetting the connection and/or blocking the traffic from the offending IP address. An IPS can also correct Cyclic Redundancy Check (CRC) errors, unfragment packet streams, prevent TCP sequencing issues, and clean up unwanted transport and network layer options.
Intrusion prevention systems can be classified into four different types:

- Network-based intrusion prevention system (NIPS): monitors the entire network for suspicious traffic by analyzing protocol activity.
- Wireless intrusion prevention systems (WIPS): monitors a wireless network for suspicious traffic by analyzing wireless networking protocols.
- Network behavior analysis (NBA): examines network traffic to identify threats that generate DDoS attacks, certain forms of malware, and policy violations.
- Host-based intrusion prevention system (HIPS): an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host.

A. *Requirements for Proposed Intrusion Prevention System:*

The major Functional Requirements for an Intrusion Prevention System need to be discussed before the mechanisms of security architecture. The Functional requirements of an IPS are outlined below:

- **Online operations:** In order to perform real time protection, an IPS must operate in online mode at crucial points of the network. IPS can take the required action immediately only when they operate online, discarding any suspicious packets before they reach their target and blocking the remainder flow from that source.
- **High performance:** Packet processing must be at the real time traffic speed. Poor performance of IPS will result in slow network speed and lost of packets. Thus, an IPS should perform analysis at very high data rates; degradation in network performance is not at all acceptable.
- **Scalability:** An IPS deployment should be scalable in performance and management. IPS could be deployed to medium and large networks without significant performance degradation. NIPS deployment should also provide scalable management for multiple Sensors deployed at choke points of the network.
- **Reliability and availability:** Fail of an online device will directly affect the network up-time. Since IPS's are installed on crucial points where any failure can cause the lost of a vital network path and again, can lead to a DDoS condition. Thus, an extremely low failure rate is very important in order to maximize the network up-time and as an assurance, the device should support fail-over to another IPS operating in a fail-over group or provide fail-open option [68]. It is also important that rebooting of online devices will turn into network downtime for the duration of reboot.
- **Detection accuracy:** An IPS must detect attacks and should not block the valid traffic flow. Since IPS's operate online, false positives can lead to a DDoS condition and become a new tool for attackers. The user must be able to trust that the IPS is blocking only the malicious traffic [68]. NIPS should not block the valid traffic and prevent employees doing their jobs.
- **Ability to perform various types of detection analysis:** IPS's are only as valuable as their detection engines. Success or failure of an IPS depends mainly on its detection engine. There are various detection methods that are used in existing IDS's; each has success at detecting different types of intrusions. Mixing these various methods to use their superior parts and eliminating their weak points can form out a system that is more reliable than any of these methods alone.
- **Low latency:** Since IPS is operating online and all traffic has to flow through them, the latency on these devices affects the network performance. Packets should be processed quickly enough that end nodes can not sense the performance degradation. The over all latency of IPS must be as minimal as the latency of other online devices such as firewalls, router, and load balancers.

- **Easier management:** An IPS allow the security managers to choose the response they want among various response mechanisms. Since IPSs are not only detecting attacks, but also preventing them by limiting or blocking which directly affects the network performance. Thus, configuring an IPS is a complex job. It is important to make the security managers' job of configuration as easy and simple as possible by providing them a user friendly interface to set and change configuration and eliminate the dreadful results of configuration errors [69].
- **Safety of historic data:** Beyond detecting and preventing attacks, IPS should save the evidence of an intrusion for historical analysis. In order to do this, historic data could be copied for safe and offline observation. Mechanisms for the safety of these data should be in place.
- **Data analysis capability:** IPS should be having a mechanism to allow security managers access individual packets from summary reports, to minimize administration efforts.
- **Patch Update:** IPS needs to be updated time to time with patches in order to update with new DDoS attacks, detection and mitigation policies.
- **Modular Design:** IPS needs to be made using modular design in order to easily upgrade new functionalities and mechanisms.

B. *Major strengths of proposed intrusion prevention system are:*

- Automatically Identifies and Blocks Threats
- Reduces Time Spent Reviewing Log Files to Identify Threats
- Reduces Need for Manpower to Monitor Threats
- Enhances Network Security Architecture

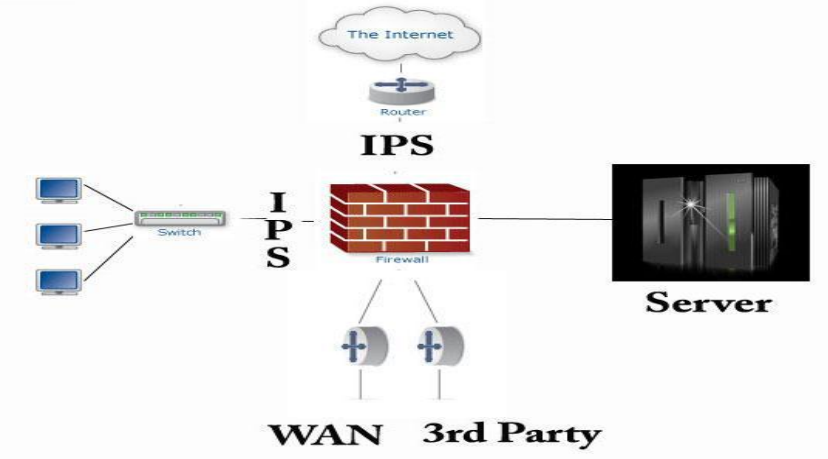

Fig 6: Proposed Intrusion Prevention System

C. *Procedure of Proposed Intrusion Prevention System [13]*

Step 1: Client sends a Http Request to IPS
Step 2: IPS registers the Application Id of Client App
Step 3: Then a Random Captcha mechanism starts.
Step 4: If Client enters wrong Captcha, the App_Id is recorded and in response a tougher captcha is generated, sensing a DDoS attack.
Step 5: At the maximum 3 try has to be given to the Client Application.
Step 6: On failure the App Id, Mac Add and IP Add will be blocked.

RESULT AND CONCLUSION

Denial of service attacks are a huge threat to the internet as a whole. In order to thwart these attacks over all internet security must be promoted and potential targets must be prepared for the potential attacks. It is critical that security methods evolve with the evolving denial of service attacks to be truly secure. Formal Classification by some Community related organization is necessary in the field of Distributed Denial of Service [1].

REFERENCES

1. Manish Saxena, Jameel Hashmi, Dr. D.B.Singh, "Classification of DDoS Attacks and their Defence Techniques using Intrusion Prevention System", IJCSCN Volume 2, Issue 5, October-November 2012. http://www.ijcscn.com/Documents/Volumes/vol2issue5/ijcscn2012020508.pdf

2. Howard J., "An Analysis of security incidents on the Internet 1989 – 1995," Carnegie Mellon University, Carnegie Institute of Technology, <http://www.cert.org/research/JHThesis/Start.html>, Apr. 1997.

3. Mirkovic J., Martin J. and Reiher P., "A Taxonomy of DDoS Attacks and DDoS defence Mechanisms," UCLA Computer Science Department, Technical report no. 020018. http://www.lasr.cs.ucla.edu/ddos/ucla_tech_report_020018.pdf

4. Spech S. and Lee R., "Taxonomies of Distributed Denial of Service Attacks, Tools and Countermeasures," Princeton University Department of Electrical Engineering, Technical report CE-L2003-004, May 2003.

5. CERT Coordination Center, "Denial of Service Attacks," http://www.cert.org/tech_tips/denial_of_ service.html.

6. http://forum.athena.edu.vn/mang-co-ban-acbn/1521-tim-hieu-ky-thuat-tan-cong-ddos.html

7. http://www.cert.org/tech_tips/denial_of_service.html

8. Distributed DNS Flooder v0.1b (ddnsf), <http://www.packetstormsecurity.org/distributed/ddnsf.tar.gz>, 2001.

9. Flitz, <http://www.packetstormsecurity.org/distributed/flitz-0.1.tgz>.

10. Kaiten, <http://www.packetstormsecurity.org/irc/ kaiten.c>

