International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 9 • Number 46 • 2016

An Efficient Technique for Detecting Distributed Denial of Service Attack

M. Dileep Kumar[a] and Smriti Agrawal[b]

[a]*Corresponding author, Department of Information Technology, Chaitanya Bharathi Institute of Technology Hyderabad, India. Email: dileep7551@gmail.com*
[b]*Department of Information Technology, Chaitanya Bharathi Institute of Technology Hyderabad, India*

Abstract: Distributed denial of service attack is a coordinated attack, generally performed on a massive scale on the availability of services of a target system or network resources. In this model, the server is responsible for answering service-requests sent by one or more clients. This design model was later utilized for executing threats such as Denial of Service (DoS) and Distributed Denial of Service (DDoS) which aim to disrupt the functionality of the serving entity. The model uses network monitor to inspect network traffic, apply traffic filters and trigger events in case a certain pattern of traffic occurred. This network monitor reads the incoming packets and analyses them. It is deployed at the victim-side.

This paper developed an automated defense mechanism for detecting DoS and DDoS attacks. This work proposed an efficient technique for Detecting Distributed Denial Attack (DDDT). It is a network monitor at victim-side which provides an efficient detection to both DoS and DDoS attacks.

The proposed network monitor is hybrid of statistical and knowledge based techniques. It monitors the incoming packets every T interval of time. If the observe the flow in this duration is similar to previously observed flows then it assumes that there is no attack. The rigorous analysis of the incoming packet is done based on its content and source based packet. The proposed DDDT technique is able to detect DDoS attacks approximately 14% faster than the existing HRS detection technique.

Keywords: DoS, DDoS, network monitor, DDDT.

1. INTRODUCTION

The Internet was not designed with security in mind; it was rather designed to provide connectivity between end hosts, and to facilitate the process of information sharing. For providing services to end-hosts, the Internet follows a client-server model. In this model, the server is responsible for answering service-requests sent by one or more clients. This design model was later utilized for executing threats such as Denial of Service (DoS) and Distributed Denial of Service (DDoS) which aim to disrupt the functionality of the serving entity (1, 2, 3).

DoS and DDoS are attacks intended to prevent legitimate users from accessing network resources. The main difference between a DoS and DDoS is that in the former, the attack originates from one source, alternatively, the latter requires multiple attack sources (One-to-One Vs. Many-to-One). DoS and DDoS attacks can be executed in different forms. For example, Domain Name System (DNS) Amplification is a form of a DDoS attack through which the DNS components themselves are exploited in an attempt to magnify the flooding attack consequence. This can be done by making use of the fact that small DNS queries can generate large responses(1).

In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting computer and its network connection, or the computers and network of the sites you are trying to use, an attacker may be able to prevent from accessing email, websites, online accounts (banking, etc.), or other services that rely on the affected computer.

Many DoS attacks, such as the HTTP flooding, Ping of Death and Teardrop attacks, exploit limitations in the TCP/IP protocols. But, like viruses, new DoS attacks are continuously being caused by attackers. An attempt of DoS as shown in Figure 1.

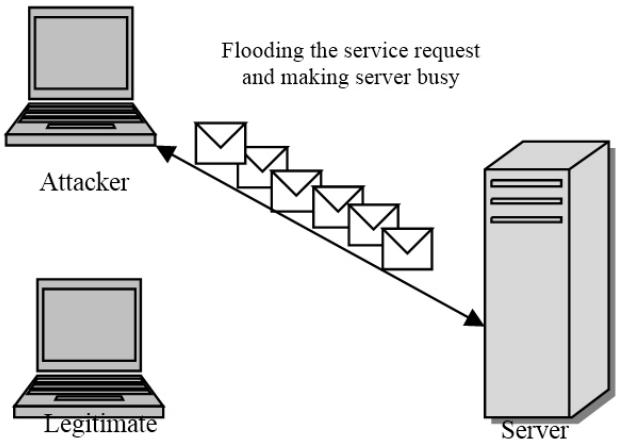

Figure 1: Denial of Service Attack

A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. They target a wide variety of important resources, from banks to newschallenge to making sure people can publish and access important information. websites, and present a major Victims of a DDoS attack consist of both the end targeted system and all systems maliciously used and controlled by the attacker in the distributed attack.

In a DDoS attack, the incoming traffic flooding the victim originates from many different sources potentially hundreds of thousands or more. This effectively makes it impossible to stop the attack simply by blocking a single IP address, it is very difficult to distinguish legitimate user traffic from attack traffic when spread across so many points of origin.

DDoS attacks come in many different forms, from Smurfs to Teardrops, to Pings of Death. Common categories of DDoS attacks are TCP Connection Attacks - *Occupying connections*, Application Attacks - *Targeting applications*, Fragmentation Attacks -*Pieces of packets,* Volumetric Attacks- *Using up bandwidth.* Compromised hosts from distributed sources overwhelm the target with illegitimate traffic as shown in Figure 2.

The DDoS attacks are global problem as seen in the statistic of 2014 given in Figure 3 collected by the authors(10,11). Figure3describes the percentage of attacks detected in top ten countries. The statistic shows that countries like United States, Japan and China are highly affected. Whereas some countries less are affected like

Turkey, Russian federation and Thailand. However, at present around 8.26% attacks in India are DDoS this number may grow as the application of Internet increases if corrective measures are not taken now.

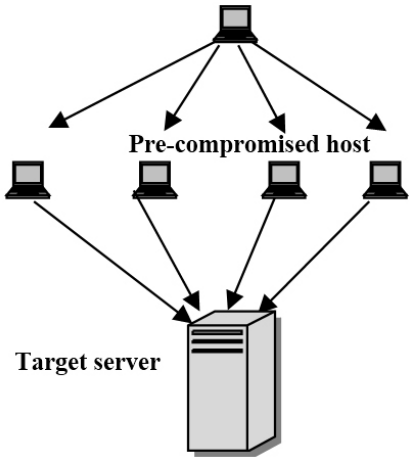

Figure 2: Distributed Denial of Service

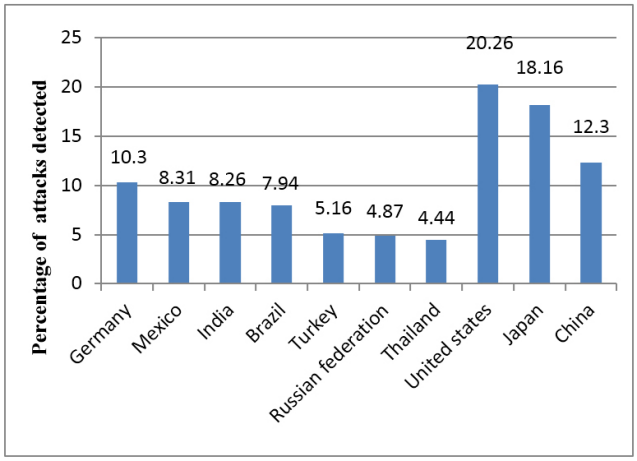

Figure 3: Statistics of Attacks Detected Globally

In client/server model, sever is responsible for answering sent by one or more service request. There are some malicious clients which intended to crash the server by sending the requests in a loop. This loop requests may prevents legitimate clients getting services from the server. This may leads to DoS and DDos attacks.

The present work aims to develop an automated mechanism for detecting DoS and DDoS attacks. This system proposes a network monitor at victim-side network which is used to inspect the traffic flow of incoming packet. Network monitor checks the traffic is malicious or not.

The rest of the paper in organization as follows, chapter 2 discusses about the literature survey, while in chapter 3 discusses about system design. Chapter 4 deals with implementation and explains modules in the paper and the software environment used in the paper and finally partial code which has been required in the paper chapter5 deals with results and analysis involved in the paper chapter6 explains the conclusion.

2. LITERATURE SURVEY

This section surveys the statistics various types of DDoS attacks and presents the existing techniques for detecting them.

2.1. DDoS Attack Manifestation

Many DDoS and DoS attacks are observed (4) in August 1999, when a DDoS tool called Trinoo was deployed in at least 227 systems, to flood a single University of Minnesota computer, which was knocked down for more than two days. The first largescale DDoS attack took place on February 2001. On February 7, Yahoo! was the victim of a DDoS attack during which its Internet portal was inaccessible for three hours. On February 8, Amazon, Buy.com, CNN and eBay were all hit by DDoS attacks that caused them to either stop functioning completely or slowed them down significantly. Figure 4 shows the steps to disrupt the victim host in the DDoS attack (2).

1. *Selection of agent:* Attacker selects the agents based on the vulnerabilities present, some machine are compromised to use as agent for performing attacks. This may lead to powerful attack stream to be generated.

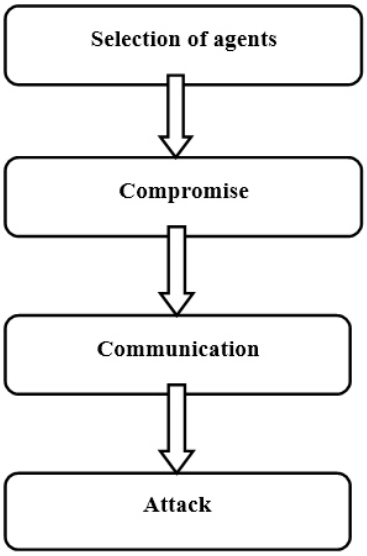

Figure 4: Steps of DDoS

2. *Compromise:* In this step direct DDoS attack strategy, the compromised nodes, i.e., zombiesbetween the attacker and victim are recruited unwitting accomplice hosts from a large number ofunprotected hosts connected through the Internetin high bandwidth.
3. *Communication:* There are communications among the attackers and handlers can be via various protocols, such as ICMP, TCP, or UDP. Based on configuration of the attack network, agents can communicate with a single handler or multiple handlers.
4. *Attack:* The attacker initiates the attack. The victim, the duration of the attack as well as special features of the attack such as the type, length,TTL, and port numbers can be adjusted

2.2. Types of DDoS

The DoS and DDoS attacks target different vulnerabilities of the network resources and effect in different ways, the following section discusses the various types of DDoS attacks known.

2.2.1. HTTP Flooding (12)

An HTTP flood is an attack method used by attackers to attack web servers and applications. It consists of seemingly legitimate session-based sets of HTTP GET or POST requests sent to a target web server. These requests are specifically designed to consume a significant amount of the server's resources, and therefore can result in a denial-of-service condition (without necessarily requiring a high rate of network traffic). Such requests are of tencausebotnet, increasing the attack's overall power.

HTTP flood attacks may be one of the most advanced non-vulnerability threats facing web servers today. It is very hard for network security devices to distinguish between legitimate HTTP traffic and malicious HTTP traffic, and if not handled correctly, it could cause a high number of false-positive detections.

2.2.2. SYN Flooding (13)

The attack involves having a client repeatedly send SYN (synchronization) packets to every port on a server, using fake IP addresses. When an attack begins, the server sees the equivalent of multiple attempts to establish

communications. The server responds to each attempt with a SYN/ACK (synchronization acknowledged) packet from each open port, and with a RST (reset) packet from each closed port.In a normal three-way handshake, the client would return an ACK (acknowledged) packet to confirm that the server's SYN/ACK packet was received, and communications would then commence. However, in a SYN flood, the ACK packet is never sent back by the hostile client. Instead, the client program sends repeated SYN requests to all the server's ports. A hostile client always knows a port is open when the server responds with a SYN/ACK packet.The hostile client makes the SYN requests all appear valid, but because the IP addresses are fake ones, it is impossible for the server to close down the connection by sending RST packets back to the client.

2.2.3. Internet Control Message Protocol ICMP Flooding (14)

It is a connectionless protocol used for IP operations, diagnostics, and errors. An ICMP Flood - the sending of an abnormally large number of ICMP packets of any type (especially network latency testing "ping" packets) - can overwhelm a target server that attempts to process every incoming ICMP request, and this can result in a denial-of-service condition for the target server.

2.2.4. User Datagram Protocol UDP Flooding (15)

It is a connectionless and session less networking protocol. Since UDP traffic doesn't require a three-way handshake like TCP, it runs with lower overhead and is ideal for traffic that doesn't need to be checked and rechecked, such as chat or VoIP. However, these same properties also make UDP more vulnerable to abuse. In the absence of an initial handshake, to establish a valid connection, a high volume of "best effort" traffic can be sent over UDP channels to any host, with no built-in protection to limit the rate of the UDPDoS flood. This means that not only are UDP flood attacks highly-effective, but also that they could be executed with a help of relatively few resources.

2.2.5. DNS Amplification Attacks (1)

Is an exploit in which an attacker takes advantage of vulnerabilities in the domain name system (DNS). DNS servers are the "roadmap" of the Internet, helping requestors find the servers they seek. DNS amplification attack is a sophisticated denial of service attack that takes advantage of DNS servers' behavior in order to amplify the attack. In order to launch a DNS amplification attack, the attacker performs two malicious tasks. First, the attacker spoofs the IP address of the DNS resolver and replaces it with the victim's IP address. This will cause all DNS replies from the DNS servers to be sent to the victim's servers.

2.2.6. Voice Over Internet Protocol (VoIP) Attacks (17)

It has been widely deployed since the integration of the voice and data networks reduces management effort and cost. The VoIP DoS attack is intended to overwhelm limited resources to disrupt VoIP operations, typically through a flood of messages. This leads to degradation of response time, thus preventing subscribers from effectively using the service.

In a Distributed DoS, multiple systems are used to generate a massive flood of packets. To launch a massive DDoS attack the hacker previously installs malicious software on compromised terminal devices (infected with a Trojan) that can be triggered at a later time to send fake traffic to targeted VoIP components. Targeted DoS attacks are also possible where the attacker disrupts specific connections.

The next sub-section presents the statistics of different types of the attack observed in 2014.

2.3. Statistics of Different Types of Attacks

The statistics of different types of DDoS attack in 2014 is as shown in Figure 5(10). The Figure 5 describes percentages of different types of attacks are seen in 2014. These volumetric attacks can take out an entire data center by exhausting its incoming network bandwidth, as compared to other DDoS attacks that may target a single server. Infrastructure attacks are typically easier for an attacker to launch and require fewer resources through the use of reflection and amplification techniques against open and vulnerable servers.

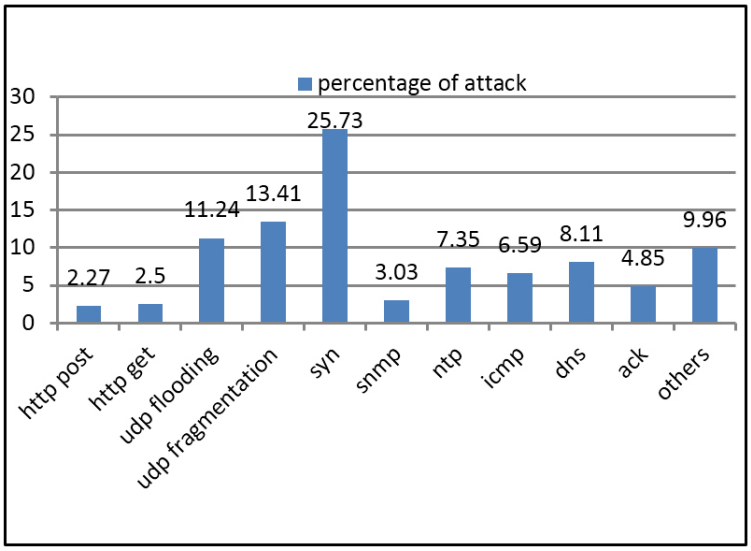

Figure 5: Statistics of types of DDoS Attacks in 2014

Network Time Protocol (NTP) attacks, a type of reflection-based in restructured attack, declined significantly with 56 percent –compared to previous quarter of year. The use of SYN floods, a perennial favorite infrastructure attack vector, increased 45 percent this quarter when compared to previous quarter of year.

The increase in infrastructure-based attacks was largely mirrored by a15 percent decrease in application-layer attacks. PUSH floods, which increased 133 percent, were the only application-layer attack that was used more compared to previous quarter of year.

The above sections state how the DDoS attack manifests itself and the statistics of its different jargons. A network monitor is used to inspect network traffic to detect the DoS and DDoS attacks. The network monitor can be deployed at various places in the network. The following section describes the various localities for deployment of Network monitor which is the DDoS defense mechanism.

2.4. DDoS Detection Network Monitors (1)

Network monitor is used to inspect network traffic, apply traffic filters and trigger events in case a certain pattern of traffic occurred (1). The deployment of the network monitor is in three localities i.e. victim-end, source-end, and intermediate router defense mechanisms (4).

2.4.1. Source-End Defense Mechanism

In this defense mechanism component is added to impose rate on going traffic connections. It is used incoming and outgoing traffic statistics with some predefined normal profiles. It is the best defense mechanism for detecting and stopping DDoS attack. It prevents the possibility of flooding not only on the victim side, but also in the

whole intermediate network. The main difficulty with this approach is that, detecting DDoS attack sat source end is not easy. This is because in these attacks, sources are widely distributed and a single source behaves almost similarly as in normal traffic. Another problem is the difficulty of deploying system at the source end.

2.4.2. Intermediate Network Defense Mechanism

The intermediate network defense scheme balances the trade-offs between detection accuracy and attack bandwidth consumption, the main issues in source-end and victim-end detection approaches. This mechanism, generally collaborative in nature and the routers share their observations with other routers. Detection and trace back of attack sources are easy in this approach due to collaborative operation.Routers can form an overlay mesh to share their observations. The main difficulty with this approach is deployability. To achieve full detection accuracy, all routers on the Internet will have to employ this detection scheme, because unavailability of this scheme in only a few routers may cause failure to the detection and trace back process.

2.4.3. Victim-end Defense Mechanism

It is deployed in the router of victim network. This mechanism used to detect intrusion either offline or online, using either misuse based intrusion detection or anomaly based intrusion detection. The reference data stores information about known intrusion signatures or profiles of normal behavior. This information is updated by the processing elements as new knowledge about the observed behavior becomes available. The security manager often updates the stored intrusion signatures and also checks for other critical events such as false alarms. Detecting DDoS attacks in victim routers is relatively easy because of the high rate of resource consumption. It is also the most practically applicable type of defense scheme as Web servers providing critical services always try to secure their resources for legitimate users.

Source-end and Intermediate network defense mechanism require reconfiguring all the routers on the Internet, which may not be practically possible. Thus, the Victim-end defense mechanism is most feasible option to implement. The following section surveys the various existing Victim-end defense techniques.

2.5. Existing Methods for DDoS Attack Detection at Victim-end

These methods are based on the architecture discussed above namely, victim-end. Here, they discuss these schemes without considering their practical deployability in real networks. Group of classifiers have also performed satisfactorily with high detection rates. These DDoS detection methods are classified in to into four major classes as follows (3)(4).

2.5.1. Statistical Technique

Statistical properties of normal and attack patterns can be exploited for detection of DDoS attacks. Generallya statistical model for normal traffic is fitted and then a statistical inference test is applied to determine if anew instance belongs to this model. There are few recent researches like TBST, PBDA, LPM, Segregation method.

2.5.2. Traffic Based on Statistical Test (TBST) (22)

In this study a new detection method for DDoS attack traffic based on two-sample t-test. They first investigate the statistics of normal SYN arrival rate (SAR) and confirm it follows normal distribution. The method identifies the attack by testing (1) the difference between incoming SAR and normal SAR, and (2) the difference between the number of SYN and ACK packets. The experiment results show that the possibilities of both false positives and false negatives are very low. The mechanism is also demonstrated to have the capability of detecting DDoS

attack quickly. In this study, it is a simple, robust and efficient DDoS detection mechanism. Two statistical *t*-tests are applied to detect the possible DDoS attack. This method can effectively differentiate between normal and flooding traffic. Indeed, this method can detect even very subtle attacks only slightly different from normal behaviors. The scheme does not hold the three-way handshaking states but only count the SYN and ACK packets, thus making low computation overhead. The efficiency of this detection mechanisms validated by experimental simulations. The evaluation results show that the detection mechanism has low false positive and false negative rate, and short detection time.

2.5.3. A Prediction-based Detection Algorithm Against Distributed Denial-of Service Attacks (PBDA)

In this study, first briefly they review research efforts on DDoS attacks, and then discuss a method to define and quantify attacks to sever based on available service rates. This is because the server is often the direct victim of DDoS attacks and the one-point failure of the entire service system. No matter whether there are attacks undergoing, if sever is overloaded even by normal service requests, the effect imposed to a service system is equivalent to that of attacks. Then a prediction method for the available service rate of the protected server, which applies the Auto Regressive Integrated Auto Regressive (ARIMA) model. Finally, they investigate the prediction method to predict DDoS attacks through simulation studies withNS2. The simulation results show that the prediction algorithmic effective to predict most attacks. In this study they discussed a prediction-based detection algorithm against Distributed Denial-of-Service (DDoS). The existing prediction algorithm adopts historical available service rates of a server to predict the server availability in the future by using the autoregressive integrated moving average model (ARIMA). Based on this prediction, they can detect abnormal states of the protected server, which might be caused by ongoing DDoS attacks. In fact, this prediction algorithm tries to alarm any possible abnormality of sever in terms of its available service rate in the future.However, using prediction for DDoS attacks has been seldom mentioned in the literature, and there are many issues to be addressed further such as the determination of empirical parameter in the model.

2.5.4. Linear Prediction Model DDoS Attack Detection (LBM) (26)

In this study a simple and efficient ARMA prediction model is established for normal network flow. Then a DDoS attack detection scheme based on anomaly detection techniques and linear prediction model (DDAP) is designed. Furthermore, an alert evaluation mechanism is developed to reduce the false positives due to prediction error and flow noise. LBM distinguishes the normal network flow and abnormal network flow contains DDoS attacks there is an issue it decrease the false alarm rate but not completely.

2.5.5. Segregation Method (27)

In this survey DDoS attack aims at occupying the victim resources soas to defy the legitimate requests from reaching it. Even though the attack traffic is generated in intimidating measures, the attack traffic mostly is disguised as the genuine traffic. Hence most of the mitigation methods cannot segregate the legitimate flows from the attack flows accurately. As the result, legitimate flows have also been filtered while appeasing the DDoS flood. In this survey a statistical segregation method (SSM) has been introduced, which samples the flow in consecutive intervals and then the samples are compared against the attack state condition and sorted with the mean as the parameter, then the correlation analysis is performed to segregate attack flows from the legitimate flows. SSM is compared against various other methods and the blend of segregation methods are identified for alleviating the false detections effectively. Determining a threshold and behavior among the flows to distinguish legitimate traffic from attack traffic is a solution to avoid large number of false-positives which indeed remains as a challenge.

There are lots of methods to detect DDoS attacks which are proactive and reactive methods. One of them is to detect TCP hosted DDoS attack at the earliest is to check incoming traffic against outgoing traffic which varies massively than the normal. If the preliminary detection of attack is positive then the sampling method is invoked. Sampling method instantaneously assigns a separate rate counter for each IPaddress.

SSM Implementation is done once the flow is sampled; the mean and standard deviation are immediately calculated. Using the Insertion sort organizes the flows in a descending order with mean as the primary key before recording into the database. Moreover, an artificial neural network technique is used to automate the segregation method and to limit the manual intervention. This SSM is used to decrease the false positive, but not completely.

2.5.5.1. Existing Sampling Techniques for Detecting DDoS(1):

The network monitor for attack detection relies on packet sampling can be a reasonable alternative for detecting events such as elephant flows (i.e. a flow with a large number of packets) or for detecting attack patterns without having access to all the packets sent. However, when it comes to detecting attacks that require inspecting all the packets of a certain type, sampling will not be sufficient due to the following limitations: Flow-Shortening: Only a small fraction of the flow packets are observed. Flow-Reduction: Not all the flows are observed. To overcome these limitations, few sampling techniques such as are used:

(a) *Sampling Based (1):* Basically, detection applications are developed on top of the network monitor. Once applications detect a suspicious activity, an action is immediately taken (e.g., using OpenFlow to install dropping rules on the switch) to separate the source of this activity from the rest of the network. Applications in this approach are developed on the northbound (i.e., loosely-coupled from the controllers) and multiple controllers are used to ensure diversity and replication. From this sampling technique, the flow-shortening reduction problem can be minimized by increasing the sampling rate. Though, there will be a sampling bias which will result in false-positives and false alarms.

(b) *High Resolution Sampling (1):* In this, the sampling resolution can be better through grouping traffic with like characteristics (e. g, same protocol type) together and then sampling the traffic of individual groups. An additional component is attached compared to previous sampling technique i.e. Filter device. A component that collects traffic of some type (e.g., UDP traffic) and sample the trafficback to the network monitor. Though this design increased the sampling efficiency compared to the sampling technique, the problem of Flow shortening was not completely solved. This is a trade off from using sampling (to decrease the overhead, traffic has to be reduced).

5.5.2. Knowledge based Technique

In these methods, predefined rules or patterns of attack are checked against connection events to test their legitimacy. There are few recently implemented methods for victim-end are Net Bouncer, TCP/IP header, Augmented attack tree.

2.5.2.1. NetBouncer (38)

In this method, it uses legitimacy tests to distinguish legitimate traffic, high performance through the use of network processors and a flexible two-tiered QoS-oriented traffic management scheme. NetBouncer, placed in environments where even under DDoS attack conditions, legitimate requests from high priority clients to critical services can be guaranteed availability and quality-of-service. It is more advantage for e-commerce sites since they would ideally prefer not to incur any loss of legitimate traffic as this translates directly to loss of revenue.

2.5.2.2. TCP/IP Header (40)

This method proposes to find DDoS attack signatures by analyzing the TCP/IP packet header against predefined rules and distinguishing normal and abnormal traffic. They focus on TCP/IP, ICMP, and UDP flooding attacks.

2.5.2.3. Augmented Attack Tree (39)

This method presents a formal and methodical way of modeling DDoS attack by the method of Augmented Attack Tree (AAT), and presents an AAT-based attack detection algorithm. This modeling explicitly captures the particular subtle incidents triggered by DDoS and the corresponding state transitions from the view of the network traffic transmission on the primary victim server. Two major contributions are given in this method: (1) an AAT-based DDoS model (ADDoSAT) is developed to assess the potential threat from the malicious packets transmission on the primary victim server and to facilitate the detection of such attacks; (2) an AAT-based bottom-up detection algorithm to detect all kinds of attacks based on AAT modeling

2.5.3. Soft Computing

In this techniques apply problem solving technologies such as fuzzy logic, probabilistic reasoning, neural networks and genetic algorithms. Soft computing is a general term for describing a set of optimization and processing techniques that are tolerant of imprecision and uncertainty. There are few recently implemented methods for victim-end are Traceback with decision tree, Ensembles of neural classifier.

2.5.3.1. Traceback with Decision Tree (32)

Denial-of-service attacks, as the term suggests, attempt to deny legitimate users the services that the servers provide. An attacker could modify the source IP addresses in the packets (i.e., IP spoofing), tracing back the origin of an attack becomes very difficult. In this design a system that detects DDoS attacks quickly and traces back the origins of DDoS attacks quite accurately. The system could detect the DDoS attack with the false positive ratio about 1.2–2.4%, false negative ratio about 2–10% with different attacks and attack sending rates and find the attack path in trace back. The misidentified attack edgeratio is about 8–12% and misidentified normal edge ratio about 12–14%. The result indicates that their system is capable of detecting the attacks and tracing them back with high accuracy and within a short time.

2.5.3.2. Ensembles of Neural Classifier (35)

This Paper Reviews the Detection of DDoS Attack. This DDoS attacks could be detected using the existing machine learning techniques such as neural classifiers. These classifiers lack generalization capabilities which result in less performance leading to high false positives. This study evaluates the performance of a comprehensive set of machine learning algorithms for selecting the base classifier using the publicly available KDD Cup dataset.

2.5.4. Data Mining and Machine Learning Technique

To protect network servers, network routers, and client hosts from becoming Handlers, zombies, and victims of DDoS flood attacks an effective defense system should be present. IP-based public network on the Internet is protected by the NetShield system. There are few recently implemented methods for victim-end are New information metrics, FireCol, and An entropy based approach.

2.5.4.1. New Information Metrics (48)

Distributed denial-of-service (DDoS) attacks typically exhaust bandwidth, processing capacity, or memory of a targeted machine, service or network. Despite enormous efforts in combating DDoS attacks in the past decade, DDoS attacks are still a serious threat to the security of cyberspace. In this survey there outline the efforts of this

research group in traceback of DDoS attacksIt proposes two new information metrics: (i) generalized entropy metric and (ii) information distance metric, to detect low rate DDoS attacks. They identify the attack by measuring the distance between legitimate traffic and attack traffic.

2.5.4.2. FireCol (50)

Distributed denial-of-service (DDoS) attacks are a major threat to security issues. The control and resolving of DDoS attacks is difficult in a distributed network. The primary problem till date is the attacks are detected close to the victim and hence cannot be resolved. It is essential to detect them earlyin order to protect vulnerable resources or potential victims. FireCol comprises multiple intrusion prevention systems (IPSs) located at the Internet service providers (ISPs) level. These multiple Intrusion Prevention Systems (IPSs) act as traffic filters. Based on threshold values it passes information. The efficient system of FireCol is demonstrated as a scalable system with low overhead.

2.5.4.3. An Entropy Based Approach (51)

Internet suffers from various threats, VoIP, which effects QoS. One of the major QoS threats is Server Availability. Attackers defeat the server processing capability and gain control over the server by flooding lot of messages or requests and make server resources unavailable to the genuine user, resulting in DDoS (Distributed Denial of Service). DDoS and Flash crowd creates abnormal traffic condition, from this abnormal traffic, legitimate user or genuine traffic is able to access the service availability. In order to develop efficiency of server there should be mechanism that varies legitimate and malicious requests. This study observes the traffic condition and the purpose of dealings varies which helps in outwitting the attackers.

There are many techniques for DDoS detection have been reported in the literature, but only a only some of them have been applied in an actual network environment and work efficiently. Designing and implementing the principle and practical DDoS defense system is really difficult. The main challenges that any DDoS defense scheme should overcome to become ideally usable are given below.

1. More emphasis must be given to speed over accuracy of detection because faster detection scheme usually consumes higher processing power which can also affects detection accuracy.
2. Real time detection of low rate DDoS attacks with detection accuracy high and low false alarm could be a challenging task, since such traffic follows the normal traffic distribution.
3. Real time DDoS detection systems are expected to be scalable for use in high speed real networks.
4. Developing a combined approach based on both supervised and unsupervised approaches with the capability of detecting both known and unknown attacks real time or near real time is of utmost necessity.
5. Accurate segregation of high-rate DDoS attack traffic from normal flash crowds with minimum resource consumption or low false alarm rate in real-time or near real time is a challenging task.
6. Transparency to existing Internet infrastructure is incredibly important in terms of deployment. So, a DDoS defense scheme should be deployable in real networks.
7. High speed traffic analysis for detecting DDoS attacks is a difficult task. A defense scheme capable of real time detection should perform well with high speed traffic.
8. Real time updating of network statistics and quick identification of randomized spoofed IP addresses are challenges.
9. A DDoS defense mechanism aiming to give a near real time solution may have to be based on an incremental clustering algorithm to segregate the attack from normal traffic. This requires an appropriate proximity measure that works sensibly, quickly and reliably.

3. SYSTEM MODEL

This section presents the system model for detecting DDoS attack. The network packet stream is observed using a Network Monitor. This network monitor reads the incoming packets and analyses them. It is deployed at the victim-side as shown in Figure 6.

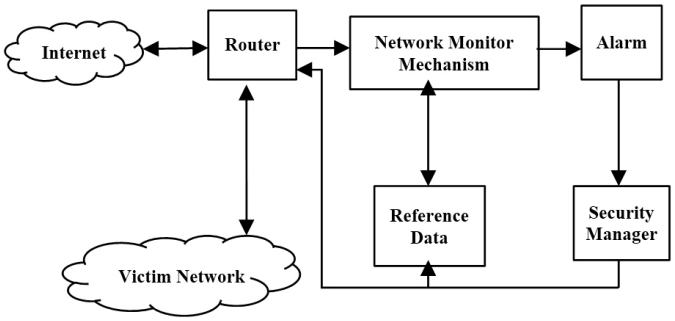

Figure 6: Flow of Proposed System

Network monitor mechanism, in which monitors the network for problems caused by overloaded and/or crashed servers, network connections or other devices. For example, to determine the status of a webserver, monitoring software may periodically send an HTTP request to fetch a page. For email servers, a test message might be sent through SMTP and retrieved by IMAP or POP3.

This section presented the system model. The DoS and DDoS attack detection mechanism as proposed is discussed in the following section.

4. AN EFFICIENT TECHNIQUE FOR DETECTING DISTRIBUTED DENIAL OF SERVICE ATTACK

In this DDoS attack, the attackers disturb the sequence of the three-way handshake either by not responding to SYN-ACK from the server or by sending a SYN packet continuously from anon-existent IP (spoofed IP).In the three-way handshake, the responding server maintains queue for sending the SYN-ACKs. During the attack, the client doesn't respond to the SYN-ACK sent from the server so that the server is made unavailable. The server maintains a queue of SYN-ACK for all the SYN packets received from the spoofed IP address. At one time, the queue overflows and the server become unavailable.

The proposed workis quick, simple and provided us relevant information on exactly what was happening on their network at that instant, as well as providing an array of history and analytical based functions and features. Furthermore, it also gives us the ability for victim-side network to login and view their own traffic within their network exactly in the same way, providing real time information to the complete metrics of any data traveling over their network.

4.1. Request Response Time

In this DDoS attack, this specific client (attacker) disrupts the server's serving entity by sending request to access large file. Response time is the total amount of time it takes to respond to a request for service. That service can be anything from a memory fetch, to a disk IO, to a complex database query, or loading a full web page. Ignoring transmission time for a moment, the response time is the sum of the service time and wait time.

In the proposed network monitor, victim-side router set a threshold range for incoming packets to router. Incoming request is verified by detection mechanism; if the request is beyond the threshold value

then it blocks the request and makes it as a potential threat. From this threshold value improves the server efficiency.

4.2. Source Based Packet Analysis

The source of the packet is analyzed as follows to detect a possible attack

4.2.1. Invalid User Agent

Invalid user agent is forging the packets which are sending by the legitimate user to server. It is form of DDoS attack; it can also be a method of attack used by network intruders to defeat network security measures, such as authentication based on IP addresses. This method of attack on a remote system can be extremely difficult, as it involves modifying thousands of packets at a time. This type of attack is most effective where trust relationships exist between machines). By spoofing a connection from a trusted machine, an attacker may be able to access the target machine without authentication.

In the proposed network monitor mechanism, implementing a filter in router checks the source IP field of IP packets it receives, and drops packets if the packets don't have an IP address in the IP address block, to which the interface is connected. Incoming packets coming into the network are filtered if the network sending it should not send packets from the originating IP address. If the end host is a stub network or host, the router needs to filter all IP packets that have, as the source IP, private addresses.

4.2.2. Same IP Address Asking Multiple Requests

Same IP address asking multiple requests is a form of DDoS attack in which flooding the request to server in certain and make server utilization high and it leads to failure of serving entity of server of legitimate user.

In proposed work, network monitor mechanism will focus on the distributed denial of service attacks in victim-side network to have access to information. Initially all the services need to be registered prior to take part in the communication. System will use detection of the malicious client in the network during the verification phase. The service request before entering in the network must pass the verification test defined by attacked packet detection algorithm. The difference between time at which client sends the request and receiver receives the request must be less than threshold value for the client request to pass the verification test. According to network monitor mechanism, the victim-side router sets a range, so all the requests in its range can communicate with it, However any malicious request lying outside the range of the victim-side can send the verification request so for that request the difference of the sending and receiving the request at the victim-side will be more than threshold value so it can be detected. However, if any client manages to pass the verification test and becomes a part of the network then system can detect it by allocating them time slots. After the client has passed the verification test and it becomes the part of the network. Victim-side router will allocate the time slots to the request for communication. Since the malicious request will continuously flood the control messages, so the victim-side router can easily detect which client is sending more than average number of requests received by it in particular time slots assigned to the respective requests.

4.2.3. IP Addresses Forming Some Pattern

The incoming of the requests to the victim-side network system was bypassing the caching system, forcing the system to render and respond to every request. This was bringing about system failures as the server quickly became overwhelmed by the requests. For illustration purposes, here getting requests like this every second:

75.118.29.205 - - (20/Jan/2014:19:32:06 -0500) "GET /?458739416183768700 HTTP/1.1" 200 440 "http://movies.netflix.com/WiPlayer?movieid=70136122&trkid=7882978&t=Weeds" ""

173.245.56.201 - - (20/Jan/2014:19:32:06 -0500) "GET /?458726993617499500 HTTP/1.1" 200 440 "http://landing.pcwhatsap.com/1/?offer_id=3534&aff=1788&url_id=5618&sub_id=whatsa

79.19.41.22 - - (20/Jan/2014:19:32:06 -0500) "GET /?458741338856272200 HTTP/1.1" 200 440 "http://www.rumoreweb.it/index.php?option=com_news_portal&view=category&id=21&Itemid=259" ""

From the above illustration the multiple IP's are asking same service request intentionally to slow down the performance of the server, this forms some pattern. The proposed mechanism, each incoming request with some pattern is store in history of database with some signature. If the incoming packets are suspicious, checks the history and block the packet and stop the services which are requested.

The working of the network monitor can be observed in the Algorithm There are three types of time interval recording. In whole interval time sampling, the system observe the flow for a few seconds at designated intervals and notice whether the behaviour occurs for the whole interval that the system is looking for it (mark "yes" or "no" as to whether this behaviour occurred for the whole time that observed). In partial time interval recording, the system mark whether the behaviour occurred at least once during the short observation interval. In momentary time sampling, the system looks up immediately at pre-designated points and notice whether the behaviour is occurring at that precise moment. In all three types, the system then figures the percent of observations that the behaviour occurred. Interval recording is used for the same behaviours as time duration recording, but this procedure takes less time and effort, and does not require that the traffic flow will be observed continually.

The traffic flow is not suspicious then accesses the web services which are requested by the network. If traffic flow is suspicious then the flow is observed for double duration of time interval. This double duration may be done by observing the pattern by other factors of traffic flow.

In the observation of double duration, if system finds no suspicious activity in the flow then send the request to server through the router to access the request. If suspicious then trigger the alarm and block the flow not access the services of the internet.

Algorithm for efficient detection technique for DDoS attack( ):

Begin

for (every T interval)

{

calculate the utilization $U_{current}$

if ($U_{current} > U_{exepected}$)

{

observe for pattern for next T interval of time

if (pattern)

{

Observe for 2T interval

if (pattern exists && $U_{current}$ on 2T > $U_{exepected}$)

then trigger alarm

}

else

{

Update $U_{exepected} = \frac{U_{exepected} + U_{current}}{2}$

}

}

else

Do nothing.

}

5. RESULTS AND SIMULATIONS

This chapter presents the simulation results of the proposed technique as compared to the existing HRS technique. The key parameter are used for comparison are time for detection of attack and accuracy of attack detection. As discussed in following sections.

5.1. Effect of Percentage of Malicious Packet on Detection Time

The graph in the Figure 7 shows the performance of proposed and existing techniques in terms of detection time as percentage of malicious packet increase in the traffic flow. It is observed that when percentage of malicious packet is less than it does not completely disrupt services but reduces and slows the services provided. Hence, the utilization of the system is impacted. The proposed technique DDDT monitors the system utilization and hence, is faster in its detection as observed in the figure. The proposed observes the utilization of server and detects approximately 18-20% time faster than the existing technique which uses random sampling. However, when medium range (40-60) is23%and higher range(70-100) is 21%.

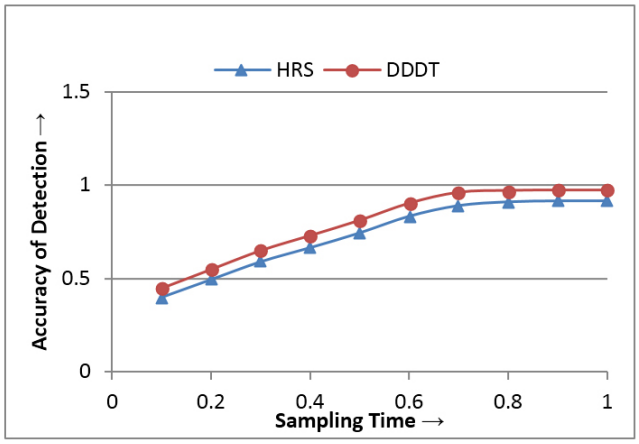

Figure 7: Sampling period Vs. Accuracy of Prediction

5.2. Effect of Sampling Period on Accuracy of Attack Detection

The graph in Figure 8 shows the effect of sampling period on accuracy of attack. It is observed as the sampling duration increases the accuracy of the attack detection improves for both proposed (DDDT) and existing (HRS) techniques. However, when sampling duration is low the proposed DDDT technique is more accurate. This is

because DDDT uses multiple patterns for analysis. When compared to the existing system the proposed system get approximately 14% better.

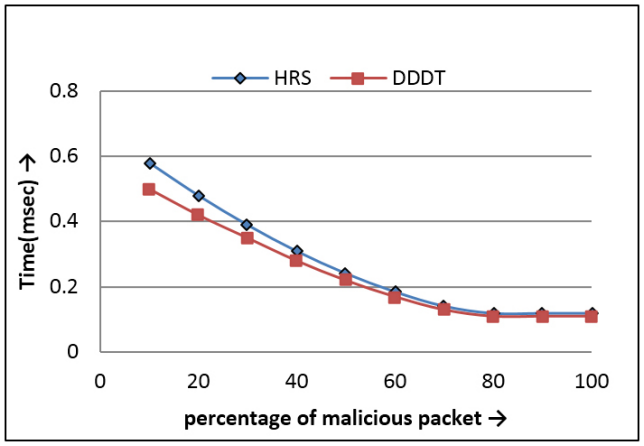

Figure 8: Percentage of malicious packet on detection time

6. CONCLUSIONS

Denial of Service (DoS) attack has been used by the attackers to disrupt the services provided to the legitimate users. It has manifested over the year in the form of the Distributed Denial of Service (DDoS) attack. The statistics reveal that they are ever increasing and may disrupt the services of a server for days together causing huge loss of business.

This project developed an automated defense mechanism for detecting DoS and DDoS attacks. Various network monitor techniques exist in literature for the same at the Source Side, Intermediate Level and Victim Side. This work proposed an efficient technique for Detecting Distributed Denial Attack (DDDT). It is a network monitor at victim-side which provides an efficient detection to both DoS and DDoS attacks. It is a hybrid of statistical and knowledge based techniques.

The proposed technique (DDDT) overcomes there limitations of the existing technique by providing monitoring the incoming packets every T interval of time. Observes the incoming flow in T interval was higher than the expected flow as observed from history it starts performing rigorous analysis of each incoming packet for 2T interval. The rigorous analysis was done on the packet by observing its content and the source.

However, for any received incoming packet if its deadline permits its accuracy detection is also improved. The existing technique also does detection of DDoS attack but the not completely. The proposed networks monitor mechanism considered the flow of the packet on previous history of flow. However, the proposed system does the attack detection done more precisely and with low false alarm rate. The proposed DDDT technique is able to detect DDoS attacks approximately 14% faster than the existing HRS detection technique.

This project proposes a new technique for fast and accurate detection of the DDoS Attack.

Limitations:

1. The proposed technique observes for T interval of time and compares utilization based on historical data. However accuracy of historical data may be limitation to this technique.
2. The accuracy at cost of higher detection time of detection mechanism can be increase by the soft computing and data mining.

REFERENCES

[1] A. Zaalouk, R. Khondoker, R. Marx, K. Bayarou, "Orchsec: An Orchestrator-Based Architecture For Enhancing Network-Security Using Network Monitoring And Sdn Control Functions" IEEE, 2013.

[2] S. Zargar, J. Joshi, and D. Tipper, "A Survey Of Defense Mechanisms Against Distributed Denial Of Service (DDos) Flooding Attacks." IEEE, 2013.

[3] Dileep Kumar G, Dr CV Guru Rao, Dr Manoj Kumar Singh, Dr Satyanarayana G, "A Survey On Defense Mechanisms Countering Ddos Attacks In The Network", IJARCCE, 2013.

[4] Monowar H. Bhuyan, H. J. Kashyap, D. K. Bhattacharyya, and J. K. Kalita, "Detecting Distributed Denial Of Service Attacks: Methods, Tools And Future Directions", The Computer Journal, 2012

[5] Bhuyan, M. H., Bhattacharyya, D. K., and Kalita, J. K. (2011),"Surveying Port Scans And Their Detection Methodologies". Comp. J., 54, 1565–1581.

[6] Kashyap, H. J. and Bhattacharyya, D. K. (2012), "A Ddos Attack Detection Mechanism Based On Protocol Specific Traffic Features". Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology, Coimbatore, India, 26-28 October, pp. 194–200. ACM.

[7] Specht, S. M. and Lee, R. B. (2004)" Distributed denial of service: Taxonomies of attacks, tools, and counter measures". Proceedings of the ISCA 17th International Conference on Parallel and Distributed Computing Systems, San Francisco, California, USA, 15-17 September, pp. 543–550. ISCA.

[8] Gogoi, P., Bhattacharyya, D. K., Borah, B., and Kalita, J. K. (2011) A survey of outlier detection methods in network anomaly identification. Comp. J., 54, 570–588.

[9] Mirkovic, J. and Reiher, P. (2004) A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Computer Communication Review, 34, 39–53.

[10] Akamai (2014), Akamai's State of the Internet Report: Security attacks on 2014, https://www.stateoftheinternet.com.

[11] Kaspersky (2012). Kaspersky Internet Security & Anti-virus. http://www.kaspersky.com/. Russian Federation.

[12] Jin Wang; Min Zhang; X. Yang; Keping Long; Chimin Zhou, "HTTP-SCAN: Detecting HTTP-flooding attack by modeling multi-features of web browsing behavior from noisy dataset", Communications (APCC), 2013 19th Asia-Pacific Conference on Year: 2013 Pages: 677 - 682, DOI: 10.1109/APCC.2013.6766035

[13] D. Nashat; X. Jiang; S. Horiguchi, Detecting SYN Flooding Agents under Any Type of IP Spoofing, e-Business Engineering. ICEBE '08. IEEE International Conference on 2008

[14] J. Udhayan; R. Anitha "Demystifying and Rate Limiting ICMP hosted DoS/DDoS Flooding Attacks with Attack Productivity Analysis", Advance Computing Conference. IACC 2009. IEEE International, 2009.

[15] K. Verma; H. Hasbullah; A. Kumar, "An efficient defense method against UDP spoofed flooding traffic of denial of service (DoS) attacks in VANET" Advance Computing Conference (IACC), IEEE 3rd International, 2013

[16] M. J. Chen; K. P. Chien; C. Y. Huang; B. C. Cheng; Y. S. Chu, "An ASIC for SMTP Intrusion Prevention System" Circuits and Systems, ISCAS 2009. IEEE International Symposium, 2009.

[17] R. H. M. Zargar; M. H. Y. Moghaddam, "An entropy-based VoIP flooding attacks detection and prevention system", Computer and Knowledge Engineering (ICCKE), 4th International eConference, 2014

[18] A. Dailianas; Y. Yemini; D. Florissi; H. Huang, "MarketNet: market-based protection of network systems and services-an application to SNMP protection" INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE, 2000.

[19] Vaithiyanathan; S. R. Gracelin; E. N. Edna; S. Radha, " A Novel method for multiple attacks in NTP based routing algorithm ",Wireless Communication and Sensor Computing. ICWCSC 2010. International Conference, 2010.

[20] Mirkoviac, J., Prier, G., and Reiher, P. (2002), "Attacking DDoS at the source". Proceedings of the 10th IEEE International Conference on Network Protocols,

[21] Saifullah, A. M. (2009), "Defending against distributed denial-of-service attacks with weight-fair router throttling". Technical Report 2009-7. Computer Science and Engineering, Washington University, St. Louis, USA.

[22] Chen, C. L. (2009), "A New Detection Method For Distributed Denial-Of-Service Attack Traffic Based On Statistical Test. Journal Of Universal Computer Science", 15, 488–504.

[23] Zhang, G., Jiang, S., Wei, G., and Guan, Q. (2009), "A Prediction-Based Detection Algorithm Against Distributed Denial-Of-Service Attacks". Proceedings of the International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly, Leipzig, Germany, 21-24 June, pp. 106–110. ACM.

[24] Akella, A., Bharambe, A., Reiter, M., and Seshan,S. (2003) Detecting DDoS attacks on ISP networks.Proceedings of the Workshop on Management and Processing of Data Streams, San Diego, CA, 8 June, pp. 1–2. ACM.

[25] Peng, T., Leckie, C., and Ramamohanarao, K. (2004) Detecting distributed denial of service attacks using source IP address monitoring. Proceedings of the 3rd International IFIP-TC6 Networking Conference, Athens, Greece, 9-14 May, pp. 771–782. Springerverlag.

[26] Cheng, J., Yin, J., Wu, C., Zhang, B., and Li, Y. (2009) DDoS attack detection method based on linear prediction model. Proceedings of the 5th international conference on Emerging intelligent computing technology and applications, Ulsan, South Korea, 16-19 September, pp. 1004–1013. Springer- Verlag.

[27] Udhayan, J. and Hamsapriya, T. (2011), "Statistical Segregation Method To Minimize The False Detections During Ddos Attacks". International Journal of Network Security, 13, 152–160.

[28] ¨Oke, G. and Loukas, G. (2007) A denial of service detector based on maximum likelihood detection and the random neural network. Comp. J., 50, 717□727.

[29] Jalili, R., Imani-Mehr, F., Amini, M., and Shahriari, H. R. (2005) Detection of distributed denial of service attacks using statistical pre-processor and unsupervised neural networks. Proceedings of the Internationational conference on information security practice and experience, Singapore, 11-14 April, pp. 192–203. Springer-verlag.

[30] Karimazad, R. and Faraahi, A. (2011) An anomalybased method for DDoS attacks detection using rbf neural networks. Proceedings of the International Conference on Network and Electronics Engineering, Singapore, pp. 44–48. IACSIT Press.

[31] Gavrilis, D. and Dermatas, E. (2005) Real-time detection of distributed denial-of-service attacks using RBF networks and statistical features. Computer Networks and ISDN Systems, 48, 235–245.

[32] Wu, Y. C., Tseng, H. R., Yang, W., and Jan, R. H. (2011), "Ddos Detection And Traceback With Decision Tree And Grey Relational Analysis". International Journal of Ad Hoc and Ubiquitous Computing, 7, 121–136.

[33] Nguyen, H.-V. and Choi, Y. (2010) Proactive detection of DDoS attacks utilizing k-NN classifier in an Anti-DDoS framework. International Journal of Electrical, Computer, and Systems Engineering, 4, 247–252.

[34] Shiaeles, S. N., Katos, V., Karakos, A. S., and Papadopoulos, B. K. (2012) Real time DDoS detection using fuzzy estimators. Computers & Security, 31,782–790.

[35] Kumar, P. A. R. and Selvakumar, S. (2011) Distributed denial of service attack detection using an ensemble of neural classifier. Computer Communication, 34, 1328– 1341.

[36] Scott, C. and Nowak, R. (2005) A neyman-pearson approach to statistical learning. IEEE Transaction on Information Theory, 51, 3806–3819.

[37] Gil, T. M. and Poletto, M. (2001) MULTOPS: a datastructure for bandwidth attack detection. Proceedings of the 10th conference on USENIX Security Symposium - Volume 10, Berkeley, CA, USA, 13-17 August 3. USENIX Association Berkeley.

[38] Thomas, R., Mark, B., Johnson, T., and Croall, J. (2003) NetBouncer: Client-legitimacy-based high performance DDoS filtering. Proceedings of the 3rd DARPA Information Survivability Conference and Exposition, Washington, DC, 22-24 April, pp. 111–113. IEEE CS, USA.

[39] Wang, J., Phan, R. C. W., Whitley, J. N., and Parish, D. J. (2010) Augmented attack tree modeling of distributed denial of services and tree based attack detection method. Proceedings of the 10th IEEE International Conference on Computer and Information Technology, Bradford, UK, 29 June-1 July, pp. 1009–1014. IEEE CS.

[40] Limwiwatkul, L. and Rungsawang, A. (2004) Distributed denial of service detection using TCP/IP header and traffic measurement analysis. Proceedings of the IEEE International Symposium Communications and Information Technology, Sapporo, Japan, 26-29 October, pp. 605–610. IEEE CS.

[41] Zhang, G. and Parashar, M. (2006) Cooperative defence against DDoS attacks. Journal of Research and Practice in Information Technology, 38, 1–14.

[42] Lu, K., Wu, D., Fan, J., Todorovic, S., and Nucci, A. (2007) Robust and efficient detection of DDoS attacks for large-scale internet. Computer Networks, 51, 5036–5056.

[43] Hwang, K., Dave, P., and Tanachaiwiwat, S. (2003) NetShield: Protocol anomaly detection with datamining against DDoS attacks. Proceedings of the 6th International Symposium on Recent Advances in Intrusion Detection, Pittsburgh, PA, 8-10 September, pp. 8–10. Springer-verlag.

[44] Chen, Z., Chen, Z., and Delis, A. (2007) An inline detection and prevention framework for distributed denial of service attacks. Comp. J., 50, 7–40.

[45] Lee, K., Kim, J., Kwon, K. H., Han, Y., and Kim, S. (2008) DDoS attack detection method using cluster analysis. Expert Systems with Applications, 34, 1659– 1665.

[46] Sekar, V., Duffield, N., Spatscheck, O., van der Merwe, J., and Zhang, H. (2006) LADS: large-scale automated DDoS detection system. Proceedings of the annual The Computer Journal, Vol. ??, No. ??, ????

[47] Rahmani, H., Sahli, N., and Kammoun, F. (2009) Joint entropy analysis model for DDoS attack detection. Proceedings of the 5th International Conference on Information Assurance and Security - Volume 02, Xian, China, 18-20 August, pp. 267–271. IEEE CS.

[48] Xiang, Y., Li, K., and Zhou, W. (2011) Low rate DDoS attacks detection and traceback by using new information metrics. IEEE Transactions on Information Forensics and Security, 6, 426–437.

[49] Shannon, C. E. (1948) A mathematical theory of communication. Bell system technical journal, 27, 397–423.

[50] Francois, J., Aib, I., and Boutaba, R. (2012), "Firecol: a collaborative protection network for the detection of flooding ddos attacks". IEEE/ACM Transaction on Networking, 20, 1828–1841.

[51] Jeyanthi, N. and Iyengar, N. C. S. N. (2012), "An Entropy Based Approach To Detect And Distinguish Ddos Attacks From Flash Crowds In Voip Networks". International Journal.