A Study on Various Defense Mechanisms Against DDoS Attacks

Ujwal Sadhu, Anil Kumar Kotagadda Vijaya, Krishna Seth, Md.Tauseef Riasat, Mirza Hasan and Omar Abuzaghleh
Department of Computer Science and Electrical Engineering,
University of Bridgeport, Bridgeport, CT, 06604.

Abstract—Distributed Denial of service (DDOS) attack is one of the biggest security threat to the Internet. This research paper attempts to study the DDOS attacks and its main types. The study will provide good knowledge to try for the defense measures for these attacks. The network is always vulnerable to this type of attack even after providing the security measures. This study will also focus on the ways to detect a DDOS attack and thus, start the processes to defense these attacks. The main objective is to understand the DDOS attacks and to find the security measures.

Keywords— DDoS, Intrusion detection, preventive measures of DDoS, defense mechanisms, defense models, game theory, application model defense, new enhanced model.

1. INTRODUCTION

THE usage of Internet has been growing enormously. All the services which were, previously, a single system are being transformed to multi user system. Even the most basic needs are performed on the internet. The purpose of the internet has shifted from communication to computing. Hence, the dependency on Internet has increased drastically. The computing side of the internet has enabled the user to perform many services. A huge loss is incurred if there is an interruption to these services. This urges the need to protect the network more than ever.

One of the Security issues is caused by like Distributed denial of service attack. This is one among the major problems faced by the internet users and the method to defend these attacks is very difficult. The result of the attack may be altering data through remote access or damage the systems causing data loss. Nevertheless the damage caused by these attacks on the internet causes a huge loss.

In this type of attack multiple hosts flood (sending to many packets) the victim to cause the DOS. As the network traffic to the server increases it causes the service denial for the users. If this process takes its threshold, it is impossible to be stopped. The result of the attack might be unauthorised access resulting in the data altering. Furthermore, worse than this is if the server is damaged due to the attack[1].

So the objective of this paper is to study DDOS attacks closely by understanding the way it exploits. We even study the process which makes the system vulnerable, in an effort to avoid such errors. We also look at the process of detecting a system under attack, as well as exploring the preventive measures.

The need for this problem is to look at many aspects of the network to find out the root cause. This study aims to provide knowledge on security measures that are to be taken or even more to improve the security issues[2].

The past attacks on internet has caused substantial damage to industries that rely on the internet. Attacks on Mastercard.com, PayPal, Visa.com. has caused severe damages to prominent banks like Fifth Third Bank, BB&T, Wells Fargo, Citigroup, and HSBC, Capital One , PNC, U.S. Bancorp, Bank of America. There is a hacktivist group called "Izz ad-Din al-Qassam Cyber Fighters" who had been attacking the major banking websites. One of the biggest attack is on the Cyber bunker with a record traffic of 300Gbps.[3]

The target of the Dos attack is not only confined to a certain domain (like banking), because there are many incidents which have encountered this situation.

DoS attacks generally initiates by entering into the peer systems which causes the DDoS attacks. The (CERT Computer Emergency Response Team) Coordination Center (CERT/CC) has been maintaining overall statistics on Internet attacks since its inception more than 15 years ago, and provide a general view of the trends.

Fig. 1 gives the number of attacks reported to the CERT/CC from 1993 through 2003. It shows a massive increase over the past 11 years. It demonstrates that the immense use of internet and communication medium is proportional to the DDoS attacks. The more usage of internet and data, the more chances are there of the attacks. As the incidents have been rising since the last decade, we cannot expect the end of these attacks in the coming future.[4]

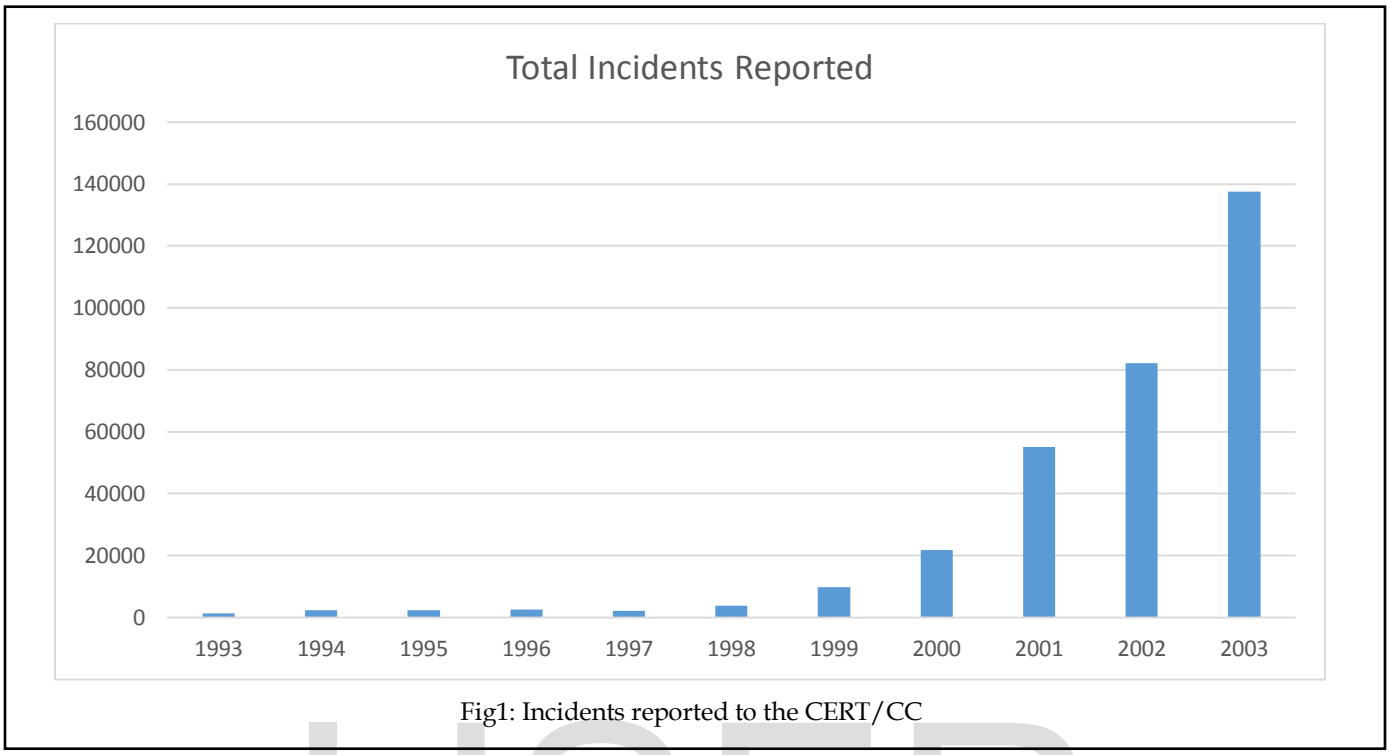

Fig1: Incidents reported to the CERT/CC

2. Related Work

According to the research paper on Distributed Denial of Service Attacks by lau, Stuart, Smith and Ljiljana. They have characterised the DDoS attacks in four types.[5]

- Flooding a network hence stop the network traffic
- Disrupt connections between system to stop access to service
- Deny a specific user from accessing server
- Deny service to a particular system or user

After studying these attacks, they came to conclusion by breaking down the process of attack into four steps. Firstly, victim receives a brunt attack. Then victim has to deal with the daemon agents which are the programs that conducts the attack. They are deployed from the host. To complete it, they have to access the host. The next step is to control the master program which coordinates the process of attack. Then finally the hacker or attacker uses this program to direct the attack.

This attack starts by sending an execute message to control master program which upon receiving the command, activates the daemons to attacks. These daemons then start the attack. All this process requires the attacker to infiltrate all the systems in the network making it a difficult process. So the attacker must know the topology of the network and the vulnerabilities which can be used during the attack.

The research also mentions about the defence mechanisms which can be implemented. Although these do not fully defend the attacks, but there are few security measures to follow. Disabling IP Broadcasts, filtering routers, disabling the unused services and performing intrusion detection are few mentioned mechanisms to be looked at.

They have tried to simulate the attack to check the best routing algorithm and filed a report which read that almost all the routing algorithms failed to provide the bandwidth to the user during the attack, except for class based queuing algorithm. Hence, they have concluded that the results due to simulation show that protection against these attacks can be achieved if the queuing algorithms are implemented.

According to the research done by Yoohwan Kim, et. al.; the DDoS defense scheme were made familiar. These schemes deny the packets that are based on statistical processing but supports online automated attack. Another research done by Jie Yu, Zhoujun Li, et. al. more prominently focus on the attacks on application layer.[6]

The network security faces many kinds of threats. Most prominent among them are the DOS attacks. The security of a computer is tested only if its data transfer reliability is maintained. Basically, much of the network system is

vulnerable to Denial of service attacks. They can easily crack through the application and the network layer of the network model.

The application layer is defenceless to the HTTP flooding. There is a huge flux of GET requests which start attacking the servers at an alarming rate, ultimately sucking all the image files from the server. It also results in firing multiple queries one after the other, often leading to a server jam. On the other side, the security measures of the network layer are exposed when its important entities like SYN, UDP and ICMP are flooded.[7]

Many a times, the links or the websites are inaccessible by the users. This may happen because they are attacked by the Dos attacks. To counter it, a normal profile is created with the help of the characteristics and the behavior it shows to access the website. This helps in identifying the normal user and the attacker. But while accessing a website, if the webpage takes more time to load up as compared to the user to understand its content, it is conspicuous that there is an application layer Dos attack.[8]

In here, the enhanced SVM plays an important role to prevent and detect the attack. ESVM, which has its string kernels, identify the profile of a normal user to that of an attacker traffic and encounter the incursion. The DoS attacks are prominently subject to the packet number. The framework specification of EVSM is also based on the packet number only, thus proving its usefulness.

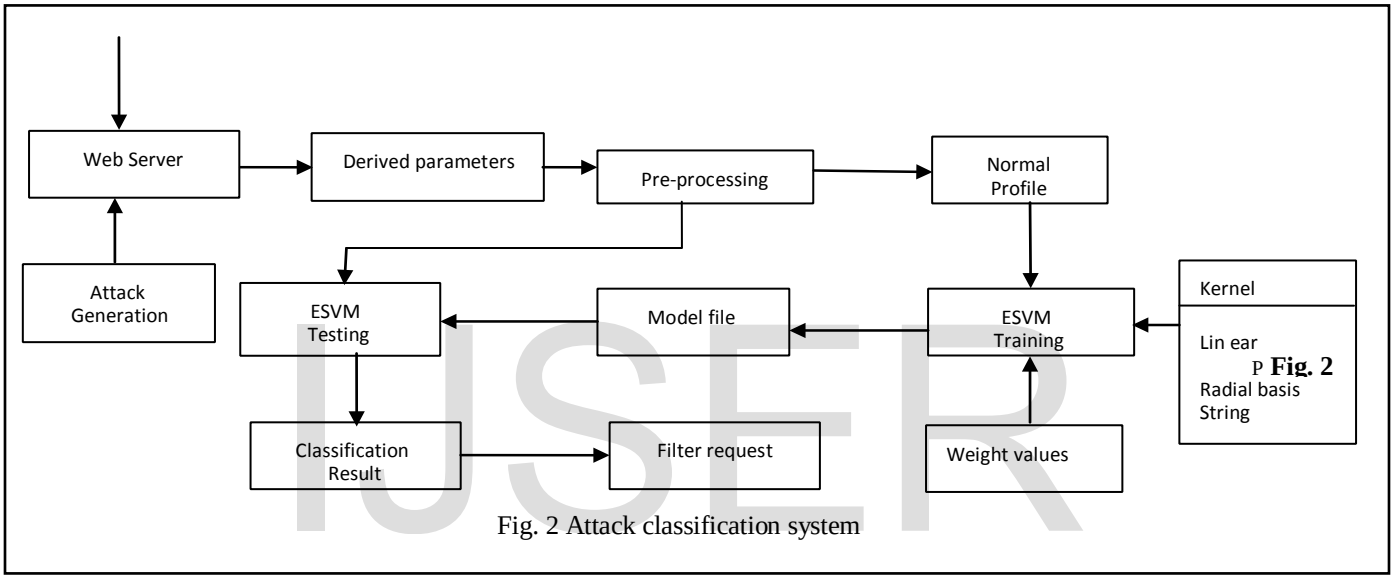

Fig. 2 Attack classification system

Fig. 2

3. DEFENSE MEASURES

3.1 DDoS Defense Mechanism

When DDoS flooding attack happens there is no other way but disconnecting the sufferer from the network and fixing the problem manually to get rid of the attack [1]. So a defense mechanism is very important to keep the system out of danger from DDoS attack. In this paper we have classified two types of DDoS flooding attacks so we have worked on the defense mechanism for those two DDoS flooding attack. These attacks are:

1 DDoS flooding attacks at Network/transport – level
2 DDoS flooding attack at Application-level

According to these attacks we have classified the defense mechanism into various criterions.

- **First criterion:** This classification is based on the principle that the defense mechanism works according to the location in which it is deployed. It has four categories:
  1. Destination based
  2. Source based
  3. Hybrid
  4. Network based
- **Second criterion:** The principle for classification is the point of time when the DDoS defense mechanism must response to a possible DDoS flood attack [2]. These are:
  1. Before the attack
  2. During the attack
  3. after the attack

3.1.1 Source based mechanism:

In this mechanism preventing DDoS flooding attacks are done by deploying the defense mechanism near the source [3].

- ❖ **Advantages:**

When the attack starts it can detect from the source and respond very quickly before the traffic attack wastes a lot of resources [4].

- **Disadvantages:**

1. Sometimes it becomes difficult to tell apart between genuine and the attack traffic at the source.
2. Filtering the attack flows accurately can be difficult because the sources are spread among different domains.

3.1.2 Destination based mechanism:

In this system the defense mechanism is applied at the destination of the attack.

- **Advantages:**

It is cheaper and easier than the other mechanisms to protect the system from DDoS attack because they are applied close to the destination hosts.

- **Disadvantages:**

Victims may get affected before the detection of the attack because it cannot perfectly detected to counter the attack before it reaches the victims and causes the damage to resources.

3.1.3 Network based mechanism:

These mechanisms are implemented inside of a network or mainly on the routers of the ASs. [10]

- **Advantages**:

This mechanism can detect and respond to the attack traffic at the middle networks closer to the source.

- **Disadvantages:**

1. The lack of adequate aggregated traffic destined for the victims can create difficulties for these mechanisms to detect attack.
2. On the routers it has high storage and processing over-head.

3.1.4 Hybrid mechanism:

It is a cooperation based mechanism between servers and users to spot and react to the attacks [10].

- **Advantages:**

1. More strong against DDoS attacks.
2. It has good amount of resources at various levels to deal with DDoS attack.

- **Disadvantages:**

1. There are lacking in incentives for the service providers to cooperate.
2. It needs reliable communication among various spread components in order to cooperate.
3. Because of the collaboration and communication among distributed components scattered all over the internet it has complexity and over heading.

Before the attack(Attack Prevention):

The time of the launching stage of the DDoS attack is the best time to stop it. So a prevention system can be designed at the attack sources, midway networks, destinations or a combination of them.

During the attack (Attack Detection):

The attack detection can be the next step after the attack prevention process. It can be deployed at sources, intermediate networks, destinations or a combination of them.

After the attack (attack source identification and response):

Blocking the attack traffic and identify the attackers or sources of attack is the main responsibility of this type of defense system which is placed after a DDoS attack has detected.

3.2 Classification of DDoS Defense mechanism:

According to different criteria there are two classification of DDoS defense mechanism. The DDoS defense mechanism depends on the two classifications which are activity deployed and location deployment.

Classification by activity

1. **Intrusion Prevention**

There are some DDoS defense mechanism which try to prevent systems from attackers.

Applying globally coordinated filters: Ingress filtering which is proposed by Ferguson and Senie, it is a mechanism to drop traffic with IP addresses where domain prefix connected router doesn't match. It is an outbound filter. This filters shows assigned IP address space leaves the network. This filter does not help to save resource hostage domain.

Disabling unused service: For unused service, the network service should be disabled for prevent attacks.

Applying security patches: The latest security patches for the bugs should be updated by the host computer. Latest available technique should be used for preventing DDoS attacks.

Changing IP address: For preventing local DDoS attacks, we can apply invalidation to the victim computer IP address with new one so that the edge router will drop attacking packet.

Disabling IP Broadcasts: For attacks like ICMP flood, smurf attack, host computer cannot be used by disabling IP broadcast.

2. Intrusion Detection

By recognizing anomalies in system, intrusion detection system detect DDoS attacks.

Anomaly detection:

Anomaly detection system depends on detecting system behavior which are abnormal comparing to other standard network.

Misuse detection:

This detection system observes the well-defined pattern of known exploitation and then search for occurrences of that pattern.

3. Intrusion Response.

IP Traceback: For achieving path characterization, it traces the attack back to their origin so that the true identity of the attacker can be found.

ICMP Traceback: In this traceback mechanism, using low probability every router samples the forward packets and then send ICMP traceback message toward destination

A link-testing traceback: this technique is proposed by Burch and Cheswick [12]. By flooding with large burst of traffic, this system infers the attack path.

CenterTrack [ll] this system is proposed by Stone. This system creates an overlay network of IP tunnels by connecting all edge routers to central tracking routers.

Hash-based IP traceback has been proposed by Snoeren, et al. Source path isolation engine (SPIE) generates audit trails of traffic and then trace origin of single IP address

Intrusion Tolerance

Intrusion tolerance can be classified into two parts. Fault tolerance and quality of Service.

The process of fault tolerance is to duplicate the network service and diversify its access point so the network can continue offerings its service when flooding traffic occurred in the network link [11].Quality of service (QoS) explains the assurance of ability of network to deliver predictable outcome for different types of application.

Classification by Deployment Location

According to the deployment mechanism, DDoS attack defense mechanism are divided into different categories:

Victim-Network Mechanisms: Most of the combating DDoS attacking system are designed to work on the victim side. Resource accounting, protocol security mechanism are examples of victim network mechanism.

Intermediate-Network Mechanisms: The attack can be handles easily when the intermediate network mechanism are effective. Traceback and pushback are the example of this mechanism.

Source Network Mechanisms: Before entering the internet core, this mechanism in the source network can stop attack flows from various sources.

3.3 Defense Mechanism ALPi: A DDoS Defense System for High-Speed Networks:

To counter the DDoS attacks, we are introducing the concept 'Packet Score' that identifies the DDoS attack, separates them from the real ones by using packet scoring and abandons the low scoring ones.

But sometimes, the complexity and performance take its toll over the working of Packet scoring. At this point of time, ALPi comes to rescue. Also the score computation is mitigated with the help of leaky-bucket overflow control scheme, which also increases the speed of the process with substantial standards[13].

Because of the increasing traffic, it is important to identify the any attack quickly, to prevent the obstruction of data flow. These problems are overcome by attribute-value-variation scoring scheme and enhanced control-theoretic packet discarding method.

The collaboration of these two methods excessively increases the ability to recognize the attack and also reduces the memory allocation. These qualities make ALPi, an immensely reliable DDoS defense system[9].

Packet Scoring:

Packet scoring [25] has been used by various network appliances like Stealthwatch and Webscreen [23] and [24]. A defense system must be able to handle and confront with any type of attack. It should also be able to provide appropriate solutions to the attack. These qualities are prominently included in packet scoring. It is a very efficient defense system, which has the ability to detect and block the first-timer attacks. It applies the packet-scoring approach to counter the attacks.

Every incoming packet which arrives, is given a specific score. These scores are given depending on the TCP/Ip protocols. If any of the packet has a score that exceeds a dynamic threshold, that packet is discarded.

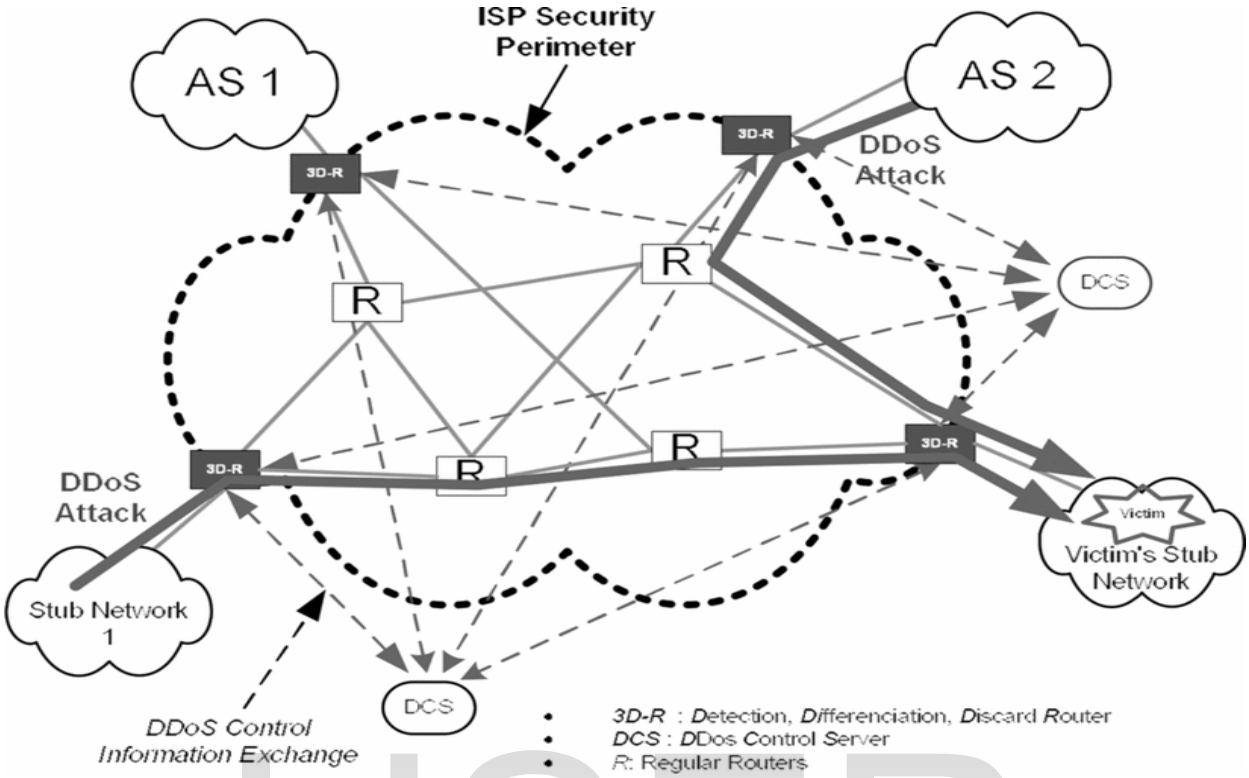

Fig. 3. Deployment of 3D-Rs and DCSs to tackle end-point DDoS attacks

II. CLP based PacketScore structure:

In this scheme, some routers (3D-Rs) [21] are introduced in the structure, which performs the main function of detection of attacks, separating them from the legitimate ones and discarding them. The 3D-Rs are implemented on the control servers of the DDoS.

Server is able to deal the control messages with the routers, which is the reason why it is placed separately from the normal data communication path. This structure keeps it safe from the attack. Moreover, the terminals within the DCS [22] are segregated in a certain domain.

Now, with a suitable environment to work in, PacketScore plays its crucial role. It uses CLP to sum up the score (tally) of all the packets which pass through the CLP-based scheme. It is processed in a triple phase:

i) Evidence to support the confirmation of any attack which is based on certain protocols including the detection and identification of victim. The DCS forwards this first report to the 3D routers. by supervising all the important traffic statistics of every protected target i..e. number of active flows, bits/sec, packets/sec and flow rate of new arriving packets. All this while, per-target states are kept to the lowest.

ii) A score is allotted to every packet to distinguish between the original and the attacking ones. Each of the packet has a traffic profile which is nominal and/or current. When these two are compared, a score is generated, then computed by CLP and saved in the shape of scorebooks. This results in the increase of the relative frequency of the attacker in the current profile. As a result, the attribute value shared by attacking packet will be given a lower score.

iii) Dynamic threshold is used to compares the score of the packet for removing the low score packets. Dynamic threshold, is adjusted according to:

1. The score distribution of all suspicious packets and
2. The congestion level of the victim.

Fig. 4 summarizes the Packet Score scheme.

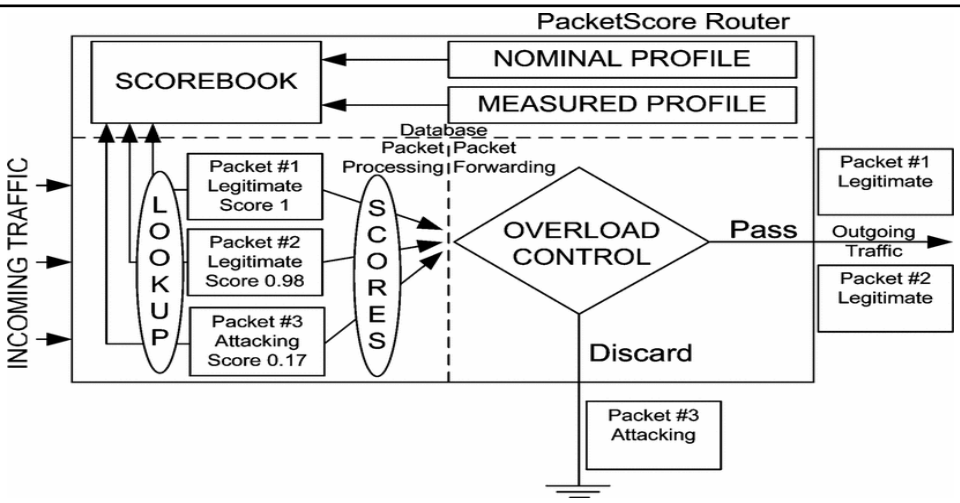

Fig. 4. Simple diagram of PacketScore scheme

3.4 Attack vs defense model

There is a need for finding the best process for DDoS defence mechanism. This is done by comparing the mechanisms on a scale. Here there is a need for measurement.

The defiance mechanism's performance can be measured by genuine traffic rate passed (GTRP) and attack traffic rate passed (ATRP).

$$\text{GTRP} = \frac{number\ of\ genuine\ traffic\ rate\ passed}{total\ number\ of\ genuine\ packets}$$

$$\text{ATRP} = \frac{number\ of\ attack\ traffic\ rate\ passed}{total\ number\ of\ attack\ packets}$$

Now, we measure the performance by dividing GTRP over ATRP as mentioned in the below formulae.

$$\text{Performance} = \frac{GTRP}{ATRP}$$

If the result is ∞ then the system is a perfect defence as ATRP is 0. On the contrary if the result is 0 then defence system is the worst case as the GTRP is 0.

So if we are to find the best defence mechanism than means the performance should me higher.

Assumptions

We have two non-negative functions of time continuous differentiable assume them as f(t), g(t). The minimum value of the functions are 0.

The probability of damage caused by the attack is proportional to the strength of the defence. This can be mathematically expressed as[16]:

$$\frac{dp}{dt} = -aq \qquad (1)$$

$$\frac{dq}{dt} = -bp \qquad (2)$$

Here p is the attack and q is the defence. 'a' is the rate at which the threat is minimised by the defence. 'b' is the rate at which the attack damages the defence.

Here we assume that a,b are independent of the strengths of attack and defence. They are also constant over time. At t=0

$$\frac{dq}{dp} = -\frac{-bp}{-aq} \qquad (3)$$

$$-aqdq = -dpbp \ (4)$$

If we integrate we get

$$a(q^2 - {q_0}^2) = b(p^2 - {p_0}^2) \quad (5)$$

As p(0)=p0 and q(0)=q0 at t=0 (6)

Lanchester's square law states :

$$K = a{q_0}^2 - b{p_0}^2 \quad (7)$$

Hence

$$aq^2 - bp^2 = K \ (8)$$

When

K≠0 that means the graph is hyperbola

K<0 that means the hyperbola intersects x axis this is when attack wins

K>0 that means the hyperbola intersects y axis this is when defence wins

K=0 that means the graph is a straight line

ANALYSIS

As stated above when the K is greater than 0 that means the attack is successfully defended. Hence at this point the equation is

$$(\frac{q_0}{p_0})^2 > \frac{b}{a} \quad (9)$$

As a,b are constant, increase in twice of the defence strength would result the attacker to improve his strength 4 times the original. Hence we can assume that if the system is more secure the attacker has to expand his attack more than the needed.

The equations (1) and (2) solving by (6) gives the following

$$q(t) = q_0 \cos\sqrt{abt} - p_0\sqrt{\frac{a}{b}}sin\sqrt{abt} \quad (10)$$

$$p(t) = p_0 \cos\sqrt{abt} - q_0\sqrt{\frac{a}{b}}sin\sqrt{abt} \quad (11)$$

The equation (10) is written as:

$$\frac{q(t)}{q_0} = q_0 \cos\sqrt{abt} - \frac{p_0}{q_0}\sqrt{\frac{a}{b}}sin\sqrt{abt} \quad (12)$$

According to the above equation the defence strength depends on the 2 values $\sqrt{\frac{a}{b}}$ and $\sqrt{abt}$. Here $\sqrt{\frac{a}{b}}$ represents the ratio of attack to the defence and their effectiveness. $\sqrt{ab}$ represents the intensity of the defence, attack. $\sqrt{ab}$ tells the time taken by either of the processes to end.

Achievements

This theoretical model hence is accustomed to know the attack and defense strength as well as their relationship with one other.

The procedure from which the output is produced through the input is recurring for every attack. Hence it predicts the output if attack is same.

Simulation

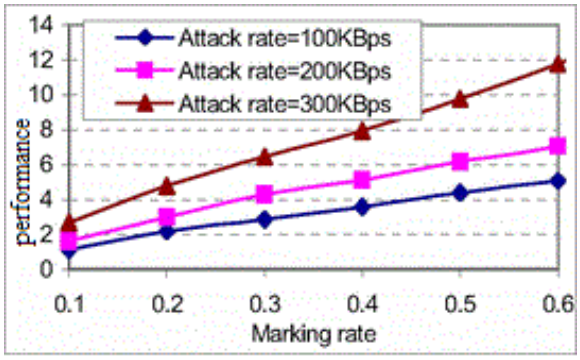

Fig3: Experimental values

SSFNet is the simulator used to test the defense performance. TFN2K is embedded into the simulator for the virtual attack. The defense is tested at 3 different internet speeds 100KBps, 200KBps, 300KBps. The graph is made according to the outputs. The inputs are taken form datasets of server at ipv4.20040120 on 09/Jan/2004[18]. The graph proves that the genuine traffic can be more and the attack traffic passes less. Hence this system is better than the current systems.

3.5 A Application layer level defense mechanism

The DDoS attacks are conducted at all the transport, application and network level. The reason for most attacks to be targeted on application layer is that the defence tools have low control over the transport layer. Hence the protection in the application layer is less as the attacker have to overcome only few security levels when compared to the other layers.

The DDoS attacks can be classified based on their detection by the defence system minor, transitional, modern [17].

Minor attacks are the majority of the attacks which are currently on the internet. The Http request for attacks done by the bots send either one or a specified limited number of requests to the victim. Based on these HTTP request implementation we can further subdivide them into 3 types. The HTTP requests containing an unknown user agent strings or a known malicious strings (type1), a string which is named as a spoofed crawler string (type 2) and named spoofed web browser string (type3).

Transitional attacks are the attacks better than the minor attacks. A random predefined sequence of the pages in a websites are requested by the bots which are used in the websites. This makes the traffic look genuine. To detect such type we need to compare the attack with genuine

Modern attacks the request sent is made to look like it is generated through a genuine web browser for a webpages.

Minor attacks can be detected through simple packet by packet inspection.

Transitional attacks are detected through the advanced methods but the defending them is a lot hard when compared to the minor.

Modern attacks are the high end attacks detected through high intelligent algorithms of data mining.

The Application-Layer DDoS Defense

The system consists of three stages of detection mechanism for all the 3 types of attacks. The stage one detects the minor type, transitional in stage 2 and the modern in stage 3 .This is mainly based on the suspicious detection hence may be few cases of human may be

considered as the suspicious. These are resolved by CAPTCHA tests or similar tests.

Stage 1 detects the minor attacks. AS discussed the minor attacks are classified into 3 which have a detection mechanism of their own. The type1 attacks are identified if they are from unknown string or which are already identified as the malicious. The type2 attacks are identified by checking if the IP address of the bot matches to the domain of the bot's string from the reverse engineering DNS lookup. The type3 attacks are identified if the behaviour is like a true browser.

Stage 2 detects the transitional attacks. These attacks are detected by verifying the sequence of browsing in a chronological order (BSC). Therefore the sequence is first taken from each session and then passed to stage 1. Then algorithms like ILOF, COD and DStream [20] are applied to identify the contents of the sequence and know the new or changed sequence [19]. The algorithm is implemented using the metric of the subsequence that is longest common which is normalized in length (LCSLN):

$$LCSLN(BSC_i, BSC_j) = 1 - \frac{|LCS(BSC_i, BSC_j)|}{\sqrt{|(BSC_i||BSC_j)|}}$$

If the sequence is marked suspicious it is not sent to stage 3. If CAPTCHA test fails the access to website is blocked

Stage 3 detects modern attacks. These are performed by inspecting the website and generating the sequence of request which are seemed to be human requests. An understanding of how a human browses is to be known in order to detect such attack an example of a characteristic feature is page viewing time. The content of the website, the content and visitor rate relation, time taken by the user to navigate from a page based on the content of the page are few parameters that are to be considered. System calculates the web session time then algorithms are implemented to know the system determined time. If the user time exceeds the systems time then the access to site is blocked.

During the attacks 92% of the attacks are identified as malicious. Also 27% of the human users are identified as malicious who are provided with CAPTCHA to prove human users.

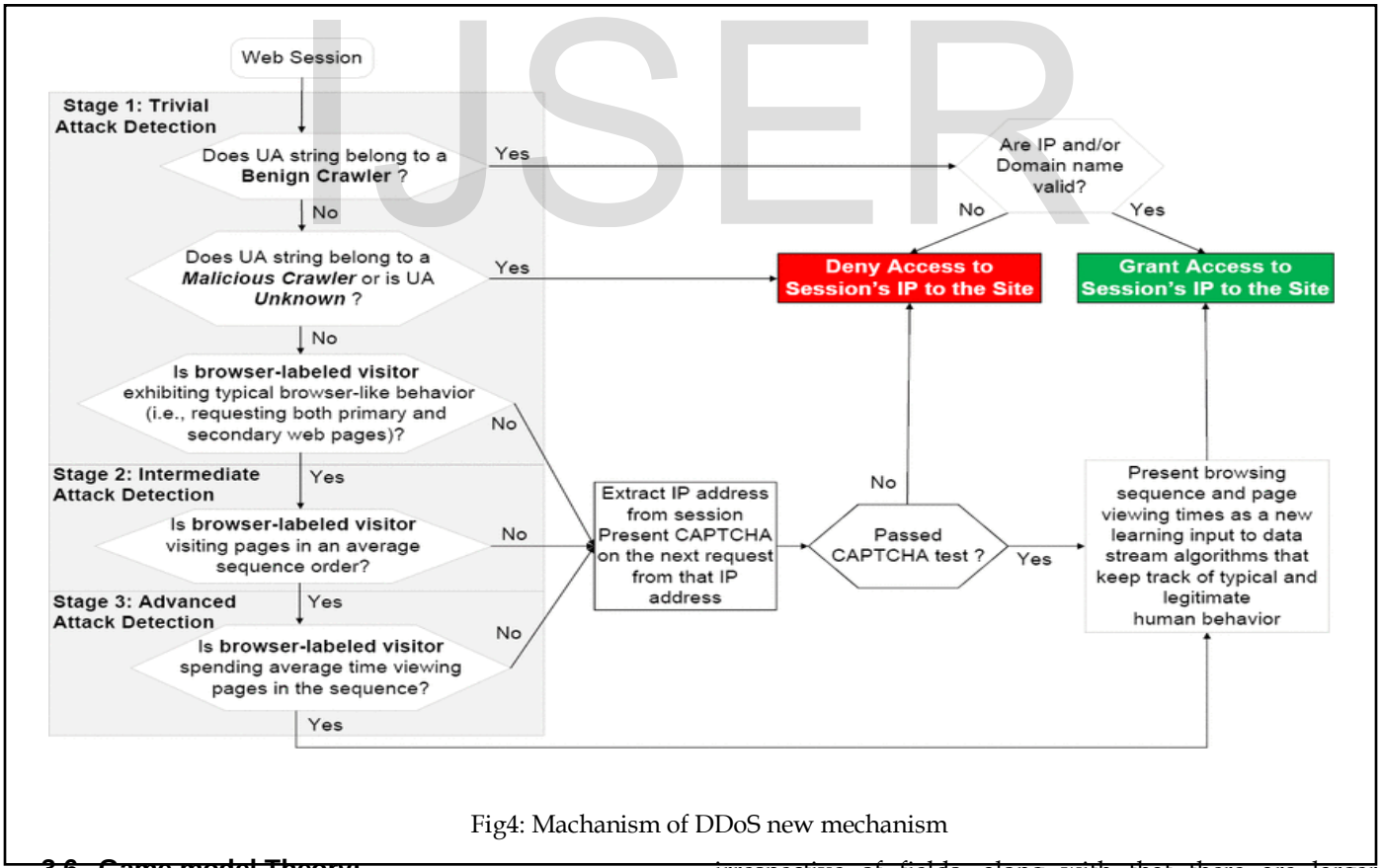

Fig4: Machanism of DDoS new mechanism

3.6 Game model Theory:

As the use of internet and network technologies have been increased tremendously in the day to day life irrespective of fields, along with that there are larger amount of threats and malicious attacks being equally taking place over the network which is causing a huge economic loss. Since the attacks are not targeted only for

common servers it has become difficult to analyze and prevent these attacks. To overcome these attacks, many mechanisms have been designed through the defense mechanisms. As the defense mechanisms deal with analyzing specific pattern of attacks and prevention of these similar attacks, the other common attacks have been left back. So, this paper not only elaborates defense mechanisms but also the other common DDoS attacks and their prevention. This paper is split into different sections and each section will discuss different DDoS attacks and their prevention.

Sec-1: Firstly we shall start with defense mechanism prevention techniques. The methods of defense mechanisms we propose are based on various methods of congestion control. The aim of this paper is to present DDoS defense mechanism in an effective and evaluated manner using game-theoretical methodology. A full strategic approach of game model is constructed for DDoS attack and defense environment. In this method, the comparing performance of network traffic control mechanisms such as Local Aggregated-based Congestion Control (ACC) and Pushback are showed by the results of utility function. At last, best possible results are provided to compare the DDoS attack prevention.

Distributed Denial of Service-DDoS attacks are the most common and threatening network attacks which tries to consume the network bandwidth and limits the host resources so as to have legitimate user's requests denied. In the past years these attacks on web servers have disabled not only the services but also caused a huge economic loss. So, in order to protect from these attacks defense mechanisms have been deployed in several locations. So there are different methodologies to compare the different evaluation methods for DDoS attacks, this paper mainly presents the quantitative evaluation and effectiveness of the attacks by strategic game opted by defense mechanism. Game Theory is a concept which is used to present exact scenario of DDoS attack and defense mechanism, a similar utility functions are constructed, which results in providing similar analysis of finding the DDoS attacks, which finally narrows the selection of defense mechanisms by providing both sides flows[14].

DDoS Defense Mechanism

As mentioned earlier defense method of approaching to DDoS attacks are entitled on the base of certain locations, these mechanisms can be deployed on source-based, medium network-based and client-based defense mechanisms on the network. These locations will monitor and control of the network or the packets which are been exchanged. This flow of the network will validate the credentials, between the sender and receivers end by following certain defined protocols. In this way the valid IP addresses will be recorded and avoid DDoS attacks, because sometimes attackers indulge in forging the IP address which will be framed by DDoS defense mechanisms.

This paper mainly focus on DDoS defense mechanisms based on network control and data speed limiting, which is mainly because: for network communication, to guarantee genuine users' communication quality and the victim's availability is a more direct proportion, and the packet filtering precautions can assure to provide service to legitimate users under DDoS attacks; although filtering methods do some damage to legitimate requests inevitably, proper rate limiting and congestion control can reduce loss of legitimate users to minimize the risk. In our evaluation model, we choose the most typical DDoS defense mechanisms based on rate limiting which are Local Aggregated-based Congestion Control (LACC) and Pushback to launch our awareness research.

Concept Briefing:

LACC (Local Aggregated-based Congestion Control) is a DDoS defense methodology which monitors and triggers when the traffic over the network overloads by discarding the packets at the routers. LACC uses an algorithm which identifies the traffic and extracts the packets which are responsible for the packet trafficking, the control algorithm is implements packet filtering and rate limiting which are responsible for the DDoS attacks.

Pushback mechanism is the added upstream concept of LACC, which not only restrict rate limiting but also sends messages to upstream routers for help according to the protocols. This concept was proposed by AT&T research lab. Its main goal is to maintain the network bandwidth and congestion users. Pushback categories the flow of users by good, poor and bad users. Bad flows are sent by the attackers and are responsible for traffic on the network good and poor are from legitimate users, however, poor flows have the same aggregate characteristics as the bad ones which make them to be identified as bad; while good flow will not have packet loss for the identification rules but it is possible that they would suffer packet loss due to network congestion [14].

Strategic mechanism of Game model Theory:

Game Theory is an efficient tool within the defense mechanism which rectifies the cause of congestion attack with its multi participant strategy.

There are different types of game models according to different scenarios, and we choose a strategic game as modeling prototype. This is a mechanism where all the participants choose his own action but only once and the selection happens at the same time. DDoS attack, the attacker and defense system are assumed players, and because the approach used by the both the parties are well known, we assume that both the parties have complete

information about the each other strategies. Game theory will give predictive results for both parties, which can instruct to choose DDoS defense mechanisms [14].

Strategic Game Model:

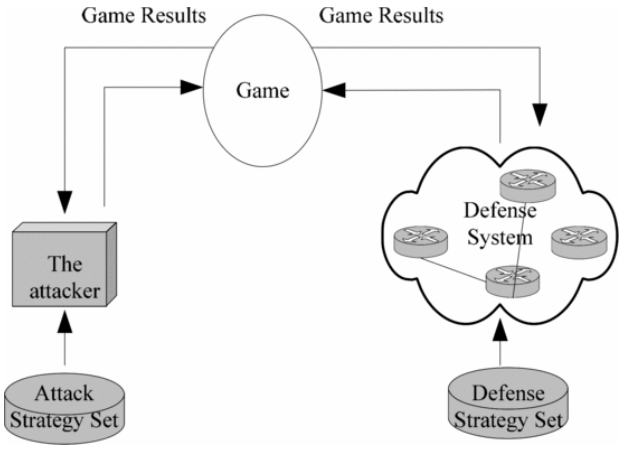

Fig 5: Game Theory representation of the attacker and defense system

Fig 5 represents separate game sets of defense system and attacker, with own strategies and the game result is computed. Say, the results affect the next move of both the parties. Let's define the DDoS attacks and defense mechanism strategy sets [14].

Def1 Game: A decision process between attacker and defense system, a game is denoted by a 3-tuple set,

G = {P, S, U} in which, P denotes the players set, S is the set of players' strategies, and U is the set of every player's utility functions.

P: Player set P= {Pr, Pq} where Pr indicates attacker and Pq indicates defense system.

S: Player's strategy sets S= {Sr , Sq} where Sr = {Sr1,Sr2 . . . Srm} indicates strategies of attackers and Sq = {Sq1,Sq2 . . . Sqm} for defense system.

U: Utility Position U= {Ur,Uq} where Ur indicates attackers strategy and Uq indicates defense strategy.

Attack Strategy Set	Defense Strategy Set
FAHR: Few attack Agents, many attack packets, High bit Rate	LACC
MALR: Many attack Agents, fewer attack packets, Low bit Rate	Pushback

Tab 1: General Strategy of two sides

The above table provides the strategy naming for both the sides.

Following are the utility functions for DDoS attacks and Defense System:

Attacker's Utility Function:

$$F_a = \alpha \frac{P_X}{P_B} + \beta \frac{P_Y}{P_B} + \gamma \frac{P_Z}{P_B}$$

Defense Utility Function:

$$F_b = \alpha' \frac{P_Z}{P_B} + \beta' \frac{P_Y}{P_B} + \gamma' \frac{P_X}{P_B}$$

Where

P_B = Bandwidth capacity of congestion link

P_X = Bandwidth of bad flows

P_Y = Bandwidth of poor flows

P_Z = Bandwidth of good flows

α, β, γ = Weight factors from the attacker's view and β, γ are negative.

α', β', γ' = Weight factors from the attacker's view and γ' is negative.

The above expressions are calculated as in a given network path we choose a percentage of three kinds of users good, bad and poor [14]. When DDoS attack occurs good flows also suffer packet lost as the network traffic are high because all the three kinds of data uses same network path. By comparing the flow we will import the parameter into the utility function.

4. A NEW COMBINED MODEL

After researching these models we would like to combine 3 models to give a unique defense mechanism. We use the theories proposed in 4, 6, 7 to form new model.

In the 6th model of Application layer we are implementing only for defense at application layer. 4th model focus on the traffic incoming and 6th model is a strategy mechanism. So we utilize these three systems to give more effective way.

In the new model we do this in the form of model 6. Here we implement 3 stages of mechanisms as that of the one in the model 6.

Stage one consists of detection mechanism to differentiate the genuine with that of attacking traffic and then sends to the other stage

Stage 2 consists of the game theory where Congestion Control and pushback are implemented.

Stage 3 is the application layer defense where the captcha is provided for the user.

Rather than the stages we may refer these to levels at which security are implemented. We use 3 different mechanisms one to detect other to defend and the third to mitigate the attacks caused hence the mechanisms is better than any of the 3 individual mechanisms.

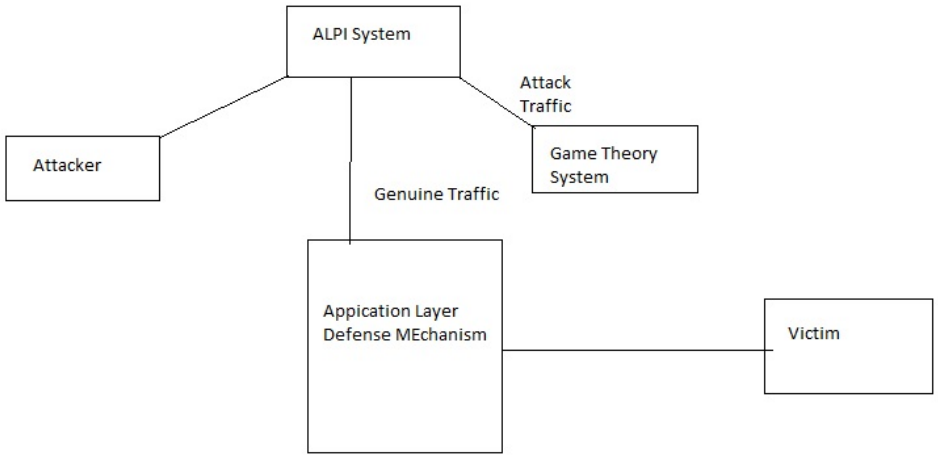

Fig 6: New proposed model

5. CONCLUSION

In the study we have studied different defense mechanisms and presented a combined mechanism against the DDoS attacks. We also studied different modes and classifications of attacks. This aids in the implementation of new model. There is still a need to defend against these attacks as the attacks have been evolving. The security should therefore be at the architectural level.

REFERENCES

1. Nagesh, H.R., K.C. Sekaran, and A.R. Kordcal. *Proactive model for Mitigating Internet Denial-of-Service Attacks.* in *Information Technology, 2007. ITNG '07. Fourth International Conference on.* 2007.
2. Habib, A. and D. Roy. *Steps to defend against DoS attacks.* in *Computers and Information Technology, 2009. ICCIT '09. 12th International Conference on.* 2009.
3. Dantas, Y.G., V. Nigam, and I.E. Fonseca. *A Selective Defense for Application Layer DDoS Attacks.* in *Intelligence and Security Informatics Conference (JISIC), 2014 IEEE Joint.* 2014.
4. Crocker, S.D., *Protecting the Internet from distributed denial-of-service attacks: a proposal.* Proceedings of the IEEE, 2004. **92**(9): p. 1375-1381.
5. Lau, F., et al. *Distributed denial of service attacks.* in *Systems, Man, and Cybernetics, 2000 IEEE International Conference on.* 2000.
6. Ramamoorthi, A., T. Subbulakshmi, and S.M. Shalinie. *Real time detection and classification of DDoS attacks using enhanced SVM with string kernels.* in *Recent Trends in Information Technology (ICRTIT), 2011 International Conference on.* 2011.
7. Mirkovic, J., G. Prier, and P. Reiher. *Attacking DDoS at the source.* in *Network Protocols, 2002. Proceedings. 10th IEEE International Conference on.* 2002.
8. Yi, X. and Y. Shun-zheng, *A Large-Scale Hidden Semi-Markov Model for Anomaly Detection on User Browsing Behaviors.* Networking, IEEE/ACM Transactions on, 2009. **17**(1): p. 54-65.
9. Ayres, P.E., et al., *ALPi: A DDoS Defense System for High-Speed Networks.* Selected Areas in Communications, IEEE Journal on, 2006. **24**(10): p. 1864-1876.
10. Zargar, S.T., J. Joshi, and D. Tipper, *A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks.* Communications Surveys & Tutorials, IEEE, 2013. **15**(4): p. 2046-2069.
11. Xiang, Y. and Z. Li. *An Analytical Model for DDoS Attacks and Defense.* in *Computing in the Global Information Technology, 2006. ICCGI '06. International Multi-Conference on.* 2006.
12. Stevanovic, D. and N. Vlajic. *Application-layer DDoS in dynamic Web-domains: Building defenses against next-generation attack behavior.* in *Communications and Network Security (CNS), 2014 IEEE Conference on.* 2014.

13. Douligeris, C. and A. Mitrokotsa. *DDoS attacks and defense mechanisms: a classification*. in *Signal Processing and Information Technology, 2003. ISSPIT 2003. Proceedings of the 3rd IEEE International Symposium on*. 2003.
14. Pan, S. and L. Yifeng. *Game-Theoretical Effectiveness Evaluation of DDoS Defense*. in *Networking, 2008. ICN 2008. Seventh International Conference on*. 2008.
15. Yang-Seo, C., et al. *Integrated DDoS Attack Defense Infrastructure for Effective Attack Prevention*. in *Information Technology Convergence and Services (ITCS), 2010 2nd International Conference on*. 2010.
16. Zhongwen, L. and X. Yang. *Mathematical Analysis of Active DDoS Defense Systems*. in *Computational Intelligence and Security, 2006 International Conference on*. 2006.
17. Stevanovic, D. and N. Vlajic. *Next Generation Application-Layer DDoS Defences: Applying the Concepts of Outlier Detection in Data Streams with Concept Drift*. in *Machine Learning and Applications (ICMLA), 2014 13th International Conference on*. 2014.
18. Yang, X. and Z. Wanlei. *Mark-aided distributed filtering by using neural network for DDoS defense*. in *Global Telecommunications Conference, 2005. GLOBECOM '05. IEEE*. 2005.
19. Idziorek, J., M. Tannian, and D. Jacobson. *Attribution of Fraudulent Resource Consumption in the Cloud*. in *Cloud Computing (CLOUD), 2012 IEEE 5th International Conference on*. 2012.
20. Idziorek, J. and M. Tannian. *Exploiting Cloud Utility Models for Profit and Ruin*. in *Cloud Computing (CLOUD), 2011 IEEE International Conference on*. 2011.
21 J. Ioannidis and S.M. Bellovin, *Implementing pushback: Routerbased defense against DDoS attacks*, in Proc. Netw. Distrib. Syst. Security Symp., Feb. 2002, pp. 79–86.
22. Yau, D.K.Y., J.C.S. Lui, and L. Feng. *Defending against distributed denial-of-service attacks with max-min fair server-centric router throttles*. in *Quality of Service, 2002. Tenth IEEE International Workshop on*. 2002.
23. Webscreen Technology. [Online]. Available: *http://www.webscreentechnology.com*
24. Lancope. [Online]. Available: *http://www.lancope.com*
25. Yoohwan, K., et al. *Packetscore: statistics-based overload control against distributed denial-of-service attacks*. in *INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies*. 2004.