Detecting DRDoS attack by Log File based IP pairing mechanism

P.MOHANA PRIYA[1] V.AKILANDESWARI[1] S.MERCY SHALINIE[2]

Department of Computer Science and Engineering
Thiagarajar College of Engineering
Madurai – 625016, Tamil Nadu,
India
amshika11@gmail.com, akilavembu@gmail.com, shalinie@tce.edu

Abstract: - As the number of security threats and attacks increase the need for developing flexible and automated network security mechanism also increase. The main objective of this paper is to propose a Reflection Attack Log File (RALF) based IP pairing detection method to detect the TCP-SYN reflection attack. The proposed RALF based IP pairing detection method is best suitable for all the types of protocols such as TCP, UDP, ICMP packets and it belongs to the category of protocol independent detection method. The RALF based IP pairing detection method involves log files which comprises the details of source and destination addresses that are considered to be the comparative parameter for detecting the TCP-SYN reflection attack. In the experimental analysis, the performance of the proposed method is analyzed with Distributed Denial of Service (DDoS) and Distributed Reflection Denial of Service (DRDoS) attack traffic. This method achieves (99%) of True Positive Rates (TPR) and less (1%) of False Positive Rate (FPR) when compared to existing reflected attack detection method. The proposed RALF based IP pairing detection method effectively detects the TCP-SYN reflection attacks before the attack reaching the target server. The results show that the proposed RALF based IP pairing detection method detects the highest probability of attack traffic.

Key-Words: - DDoS attack, DRDoS attack, Reflection attack, TCP-SYN Reflection attack, High-rate flooding attacks, Log file.

1 Introduction

The origin of Denial of Service (DoS) attack created a very big challenge to the ever developing internet infrastructure. The intention of Denial of Service (DoS) attack [5] is to stop the requested services by the clients (or) users. The attacker takes control over a single machine in a unique network to achieve DoS attack at the target server. Later, in order to distribute the DoS attack, attacker takes control over a large of machines remotely residing in different networks. This kind of attack is termed as Distributed Denial of Service (DDoS) attack. The attacker then spreads their attack range using reflector components by directing the response packets to the target server [9]. The characteristics of DDoS and DRDoS attack traffics [8] are compared which clearly indicates that DRDoS attack created a very big challenge to the researchers as the source IP address is spoofed. This special characteristic of DRDoS attack is termed as anonymity (or) anonymous. DRDoS attacks are broadly classified as bandwidth exhaustion attacks and resource consumption attacks.

The DRDoS attacks are used to exploit the protocols such as TCP, UDP, ICMP, HTTP etc. This paper concentrates on the TCP-SYN reflection attack and its proposed RALF based IP pairing detection method to identify the TCP SYN- ACK reflected response packets. The normal working procedure of TCP involves the client sending a SYN request to the server for connection establishment. Server then acknowledges the SYN request by sending the SYN-ACK (acknowledgement for the SYN request) to the client. The client then sends the ACK (acknowledgement for the SYN-ACK packet) to the server.

The steps for an attacker to launch TCP-SYN reflection attack is divided into two parts. The first part of an attacker is to spoof the source IP address of the origin which is same as target datacenter server. In this step, the TCP-SYN request is sent to the reflector from an attacker with the destination address as the reflector. The second part involves reflector machines as the origin (source IP address) whose nature is to flood the TCP SYN-ACK response packets to the target datacenter server as the destination address which gets spoofed by an attacker. This TCP-SYN reflection attack consumes the entire bandwidth of the target data center server by continuously flooding the TCP SYN-ACK response packets from the reflector server to the target server which results in half open connection of the normal working procedure of the Transmission Control Protocol (TCP). Researchers are more concerned about this attack as the source IP address of the origin gets spoofed which is equal to that of target server. When the spoofed SYN request reaches the reflector component, the SYN-ACK responses are flooded with an intention to amplify the bandwidth of the target datacenter server.

The rest of this paper is organized as follows: Section 2 reviews the related works of DRDoS attack detection methods. Section 3 is devoted for describing the proposed detection method and the simulated experimental setup is given in Section 4. Section 5 provides detailed prospective about TCP-SYN reflection attack. Section 6 highlights the performance analysis of DDoS and DRDoS attack traffic. Finally Section 7 contains the short conclusion and also the future work directions.

2 Related Works

In this section, the author's insight the state of art for DRDoS attack with its detection methods. DRDoS attack can be detected using the proposed request-response relationship [2]. Here the detector is placed next to the victim that stores the every incoming response packets with the stored request packets in the buffer. The buffer contains the potential response packets for each incoming request packet. The request-response relationship is categorized into two types such as one-to-one relationship and the many-to-one relationship. For the identified response packet, there exists only one request and response flow. Attack packets can be identified by the ambiguous packets. This relationship is also called as many-to-one relationship. The advantage of using this request-response based relationship is, simple to deploy, computational cost becomes low when compared to other detection methods.

The pairing based filtering (PF) method is proposed [1], where the incoming reply packets can be paired with the corresponding request packets at the edge routers of the Internet Service Provider (ISP) perimeter in a distributed manner so that the malicious packets can be identified which is far away from the victim. In addition, the PF method is implemented using two level filters namely Legitimate Packet List (LPL) and Source Filtering List (SFL). LPL consists of valid response packets. If the incoming SYN-ACK response packets found in the LPL, then the packets are considered to be the valid packets and it is allowed to pass to the victim's network. If the incoming SYN-ACK response packets not found in the LPL, the packet is marked and then a search is made in the SFL, if not found, those packets are dropped.

The Rank Correlation based Detection (RCD) method is proposed, which is a protocol independent method and it is suitable for TCP, UDP, ICMP [7]. The incoming response packets can be ranked according to their positions in the ascending order. The ranking can be done using the spearman's rank correlation coefficient algorithm [11]. Pearson's coefficient algorithm is used but because of the deviation in the linearity, spearman's correlation coefficient algorithm is preferred. Threshold value is defined in default as +1 and -1. If the computed rank value is equal to +1, then the packet can be classified as the legitimate packet else the rank value is equal to -1, then the packets are attack packets. By this, RCD can effectively and efficiently differentiate attack packets from the malicious packets.

Some of the anticipation methods for DRDoS attacks is proposed [3], to prevent those attacks such as protecting a client, protecting a server, preventing reflection to server exploitation, ISP'S responsibility and the attacking platforms responsibility. The first method is protecting a server, the services provided by the high numbered service ports needs to be blocked if the SYN/ACK traffic is high from these service ports but it is difficult to stop the inbound traffic from these ports. The second method is about protecting a client. Client-profile machines cannot be protected because of these reflection flows. The third anticipation method is regarding ISP's responsibility. Internet Service Provider (ISP) should have to take care of their clients by analyzing the reflection flows (or) spoofed IP address to stop the malicious flows from entering into their network in which the attack gets stopped far away from the victim.

The CARD (Continuous and Random Dropping) method is proposed in [4], which is an advanced queue method that drops the packets from the queue when it reaches certain probability. It is similar to the token bucket algorithm in which the packets are discarded when it reaches the maximum boundary value of the bucket. If the queue length is lesser than the minimum threshold value then the incoming packet is allowed to enter into the network. If the queue length is between the minimum and the maximum threshold values then a check has been made for the randomly selected packet with the current packet. If both the packets have the same identity then packet is dropped otherwise enquires the coming packets. If the queue length exceeds the maximum threshold value, then the packets drop continuously.

In [10], a cooperative based detection method is proposed. In this detection method, the client detector and the server detector is placed. The client detector is deployed at the edge routers of the innocent hosts to monitor the suspicious events, it then notifies the protected server of a DDoS attack. The server detector is located at the t server by actively sending queries to the client detectors to confirm the alert for an attack. The client detector employs modified bloom filter which has a hash table inside it. This hash table records the destination IP address. When the detection method observes the SYN-ACK packet, it can alert the suspicious alarm to the client detector. If the rate of suspicious alarm exceeds the threshold score, a DDoS warning will be sent to the protected server.

In [11], a Protocol Independent Detection and Classification (PIDC) system is proposed to detect and classify the TCP and DNS amplification attacks from the attack traffic. In [12], probabilistic neural network based attack traffic classification classifies DDoS attack from the large volume of network traffic. However, it does not address the DRDoS attack.

3 RALF based IP pairing detection method

In this section, the proposed RALF based IP pairing detection method is explained. The block diagram of the proposed RALF based detection method is shown in Figure 1. The proposed method contains the two vital components such as detection engine and comparator. Here the detection engine comprises of log files as data structures. These log files act as a buffer to store both the incoming TCP-SYN request packets and TCP SYN response packets. The following set of packet attributes, such as {source IP address, source port, destination IP address, destination port, source IP prefix and Time-to_live value} are extracted from the outgoing request and incoming response packets. These extracted values are maintained in the log file by its Time-to-Live value.

The comparator is used to compare the incoming SYN response packets with their corresponding SYN request packets. If the response packets attributes are matched with the stored request packets attributes then these packets are considered as the valid packets. If the comparator does not find any matching attributes for the incoming response packets then these packets are considered as reflected attack packets. The target server accepts the incoming response packets only when the comparator gives the messages as “IP found”. For the reflected attack packets, the comparator gives the “IP not found message” to the target server.

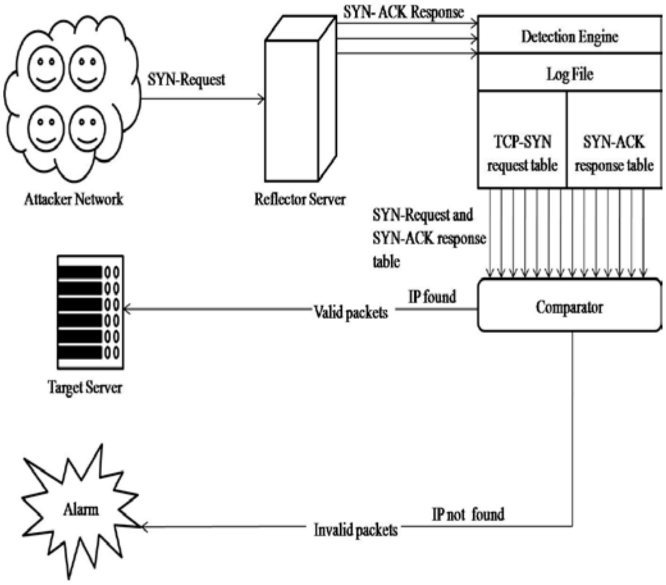

Fig.1 Proposed RALF based IP pairing detection method

The normal and reflected attack packets are classified according to the default threshold value. If the alert counter value exceed the default threshold value then packets are considered as reflected attack packets, else if the alert counter value is less than the default threshold value, then packets are considered as legitimate packet and so the alarm will trigger suddenly to alert the target server.

Fig.2 describes the RALF detection algorithm for TCP-SYN reflection attack. The detection engine extracts the matching attributes such as Request packet (R_q), Response packet (R_s) from the incoming traffic and these are stored in the Log File (*LF*). Then, the comparator compares the incoming TCP SYN-ACK packets and the appearance of their corresponding TCP-SYN request packets with their IP address, Time to Live (*TTL*) value and source IP prefix. If both the ‘R_q’ and ‘R_s’ gets matched along with the IP address and *TTL* value, then the Alert Counter (*AC*) value will not greater than the default

Threshold Value (*TV*), (i.e.)., ($AC < TH$). These kinds of traffic are known as legitimate traffic and they are directly forwarded into the target Server (*TS*). If it fails to satisfy the above condition then ($AC > TH$) then the attack alarm will trigger and those packets are directly dropped without reaching the Target Server (*TS*).

```
RALF Detection Algorithm at Intermediate Network

for each incoming SYN-ACK response packet, $R_s$,

and its corresponding request packet, $R_q$,

 received at log file, $LF$ and

 going to target server, $TS$

Alert Counter , $AC$
        1. if ( response packet $R_s$ and its request
           packet $R_q$ is in the $LF$)
              a. $AC < TH$
                     ❖ Pass $R_s$ to $TS$
        2. else
              a. $AC > TH$
           Drop $R_s$
```

Fig.2 RALF detection algorithm

4 Experimental Network Structure

In this section, the proposed RALF based IP pairing detection method is evaluated with real time DRDoS attack dataset.

4.1 Reflector Network Structure

As shown in Fig.3, the reflector attack network structure is simulated with various networks such as attacker network, zombie network, reflector network and target datacenter server.

In this architecture, attacker network consists of four network nodes, zombie network consists of seven network nodes and reflector network consists of ten network nodes. The operating system of the all the network nodes and the target server is Linux ubuntu 12.04. Several servers such as SSH/SFTP server, web server and DNS server are working in the target datacenter server. The reflector attack network is connected to the campus network in order to generate the normal traffic between the reflector network and target data center server during the experimental period.

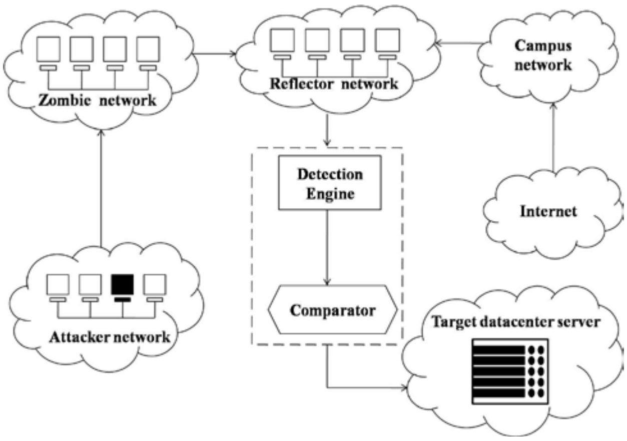

Fig. 3 Architecture of Reflector Network Structure

4.2 Reflected DDoS Attack

For the generation of reflected DDoS attack in this reflector network architecture, attacker takes an entire control of the zombie network nodes and reflector network nodes. Each network nodes have their own IP address which is referred in Table 1 in the name of original IP address. First, the attacker fixes the victim system which they want to send the reflected flooding attack packets and identifies the victim system’s (i.e. target datacenter server) ip address. The attacker randomly compromises the zombie network nodes and spoofs these nodes IP address with target datacenter server IP address. Here the target datacenter server IP address is 10.4.2.2. The attack scripts are uploaded into the zombie network nodes and these are invoked at the scheduled time. Additionally, these scripts enable the reflector network nodes to amplify the incoming attack request and also throw the amplified responses to the target server.

Next, each node in the zombie network uses the basic DDoS flooding techniques with an added layer of obfuscation by spoofing. While spoofing, the attacker initiates the attack scripts which cause the DDoS flooding attack towards reflector network with random packet arrival rate. These intermediary network nodes respond to the attacker requests by sending the response traffic to the requested IP address (i.e. 10.4.2.2). Ultimately, these network nodes send the high volume of response traffic to target server which degrade the server performance by utilizing the entire bandwidth hence it named as bandwidth attacks. Now, target datacenter server is overwhelmed with malicious responses. Sometime, target datacenter servers reply the response packets with flag packets towards itself which creates the loop that exhausts resources of the intended server.

4.3 TCP-SYN Reflection Attack

For generation of TCP-SYN reflection attack, the attacker sends a basic TCP-SYN flooding with spoofed IP address of the target server to reflector network nodes. Here, nodes send the request to the intermediary nodes and these nodes are receiving the packets with random arrival rates. It meant that the attacker invokes the attack scripts at random time with random packet arrival rate. The attacker modifies the incoming TCP-SYN requests with the parameters such as source IP address, source port number, destination IP address and destination port number to produce a large packet response from the reflector server than the original request. The SYN reflection attack is generated between the attacker network and target server through reflector network. Fig.4 explains TCP SYN reflection attack.

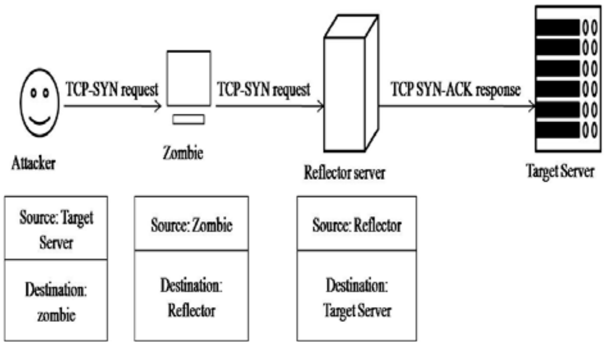

Fig.4 Scenario of TCP-SYN reflection attack

4.4 Reflected Attack Generation

The attacker have modified their attack network structure with two types of IP addresses namely, original IP address and spoofed IP address as in Table 1. Attacker spoofs their source IP address as same as the target server to achieve the first part of reflection attack, and sends the TCP-SYN request to the zombie network. This network contains five number of network nodes and utilizes the spoofing technique to spoof the nodes original IP addresses with target server IP address. The attacker then amplifies the target datacenter server's bandwidth by sending the TCP-SYN request to the reflector network which has six network nodes. Now, the reflector server floods the TCP SYN-ACK responses to the spoofed IP address (i.e.) target server IP address, to achieve highest amplification factor. The attacker does not spoof the reflector server original IP address because they are very much innocent; it only throws the amplified incoming request to the destination IP address. After the attack has been launched, the entire bandwidth of the target server gets occupied by an attacker. By this time, the target server is not able to provide access to the legitimate users. This results in low Quality of Service (QoS) which creates less interest in the field of web services.

4.5 DRDoS Attack Data Collection

The reflector attack traffics are captured between the reflected network and target data center server. The normal traffic is generated by the internet connected to the campus network. First, normal traffic profile is collected with the estimated legitimate traffic values and also total traffic rate. The normal traffic profile consists of various packet attributes in single and joint distributions. The joint distributions are often better to represent the uniqueness of traffic distribution and hard for hackers. These set of packet attributes estimated from normal traffic profile are named as legitimate packet attributes. The attack traffic profiles are gathered during the time of reflected attack. With help of uploaded attack scripts, the TCP SYN reflection attacks are generated in scheduled time. The collected attack traffic profile includes the normal and attack traffic which are used to evaluate the performance of proposed detection algorithm. Table 2 shows the collected traffic in different period of time. For the purpose to inspect the spoofed reflected attack traffic, Time-to-Live value and Source IP prefix are collected in reflected attack traffic profile.

Table1. Attack network structure details

Network Details	Original IP address details	Spoofed IP address details
Attacker network	192.168.1.2	10.7.5.198
Zombie	10.2.5.193	10.7.5.198

network	10.2.5.185	10.7.5.198
	10.2.5.178	10.7.5.198
	10.2.5.173	10.7.5.198
	10.2.5.144	10.7.5.198
Reflector network	10.5.2.155	Not spoofed
	10.5.2.130	Not spoofed
	10.5.2.134	Not spoofed
	10.5.2.164	Not spoofed
	10.5.2.190	Not spoofed
	10.5.2.200	Not spoofed
Target datacenter server	10.7.5.198	Not spoofed

4.6 DRDoS Attack Detection

The proposed detection algorithm is an intermediate solution for reflected attack. This solution utilizes the two parts namely, detection engine and comparator, which is placed next to the reflector network. During the attack, the basic parameters of TCP-SYN packet attributes namely, source IP address, source port number, destination IP address, destination port number, Time-to-Live value and Source IP Prefix are investigated by the detection engine. The traced incoming packet attribute values are stored in the log file. This log file consists of TCP-SYN request table and TCP SYN-ACK response table to identify the authentic incoming request and response packets. The comparator continuously monitors the outgoing and incoming normal and reflected attack traffic between reflector network and target datacenter server. Then, it compares the alert counter value with the threshold value for each incoming SYN request and SYN response packets. If the alert counter value is lesser than the threshold value, then it is considered to be the legitimate packet and is forwarded to the target server. The alarm indicates about the appearance of reflected attack packets when the alert counter value is greater than the threshold value. Now, the unmatched SYN-ACK response packets are considered as the malicious (or) attack packets.

Table 2. Reflected Attack Traffic Profile

Normal + Attack Profile	**SYN ACK Flooding**	
	Original Response	**Reflected Response**
Period 1	25%	73%
Period 2	20%	78%
Period 3	13%	81%
Period 4	7%	90%
Period 5	5%	94%

5. Results and Discussions

In this section, the effectiveness of the proposed detection algorithm is evaluated with simulated experiments. The TCP-SYN reflection attack can be potent and damaging when compared to DDoS attack. It utilizes the high amount of target server resources such as bandwidth, CPU and memory, to stop service to the legitimate clients. The attack scripts generate the TCP SYN request packets to the reflector network nodes. The Figure 6 shows traffic traces which are originated from the zombie network nodes. The traffic created from these nodes is considerably small but it can denial the target server resources by amplified number of TCP SYN ACK response packets. The attacker generates the traffic with increasing and decreasing rates in every seconds. Figure 7 shows the incoming traffic traces to the zombie network nodes. This traces show the absence of incoming packets in the experimental period due to the spoofing techniques of reflector attack. Some unknown packets are appeared in the initial period of experiments.

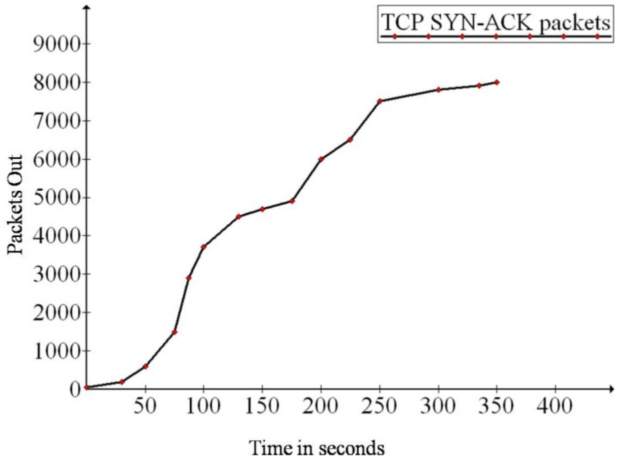

Fig.6 Number of outgoing TCP SYN packets to the reflector network nodes.

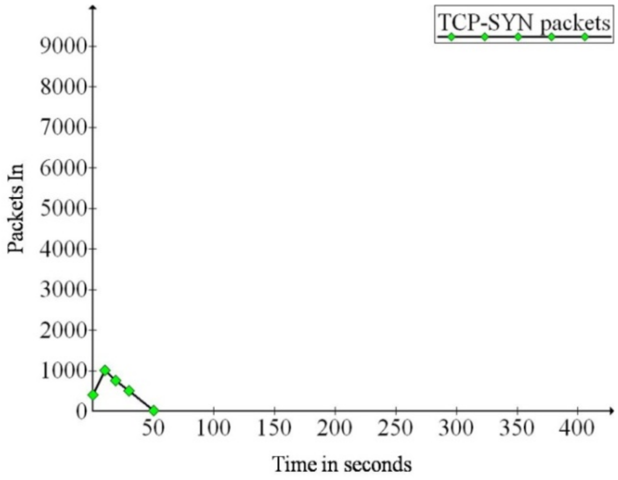

Fig.7 Number of incoming packets into zombie network nodes

During the evaluation, the reflector network nodes receive the traffic from the campus network and zombie network. The campus network produces the normal traffic into these nodes. Here the normal traffic traces have the combination of various types of protocols such as TCP, UDP, ICMP and DNS. The figure 8 shows the incoming TCP SYN packets arrival rate.

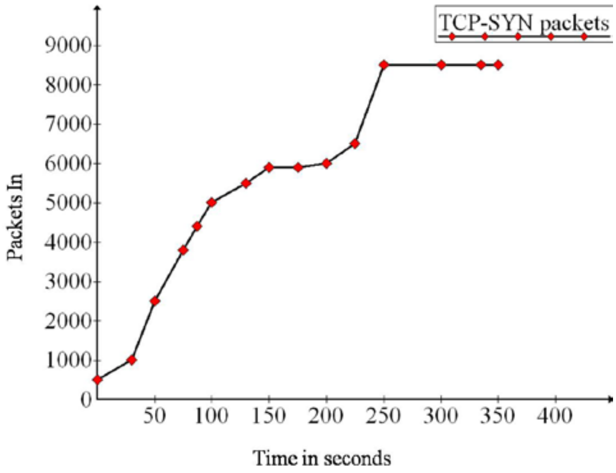

Fig.8 Number of incoming TCP SYN packets to the reflector network nodes

The TCP SYN attack traffic and the legitimate SYN request are separated using the [2] algorithm. Figure 9 shows TCP SYN attack traffic and TCP SYN normal traffic.

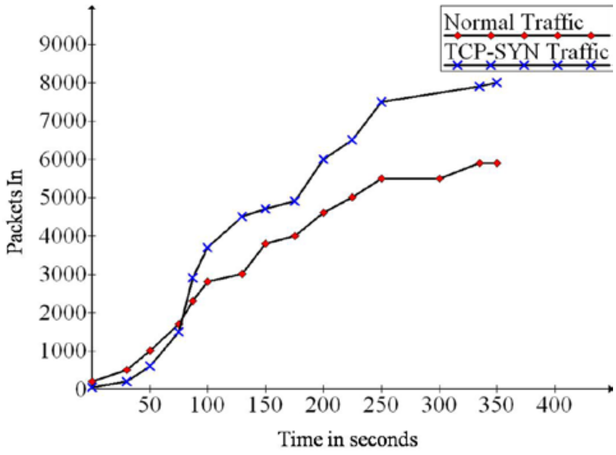

Fig.9 Number of incoming TCP SYN Normal and attack packets into the reflector network.

The reflector network replies the received SYN and other packets. The campus network receives the reply packets and redirects to the original request source. The SYN attack traffic responses are directed to the spoofed IP address. The total number of response packets originated from the reflector network is shown in Figure 10. This origination includes the TCP SYN-ACK to the target server and includes various response packets to various servers which are requested from campus network.

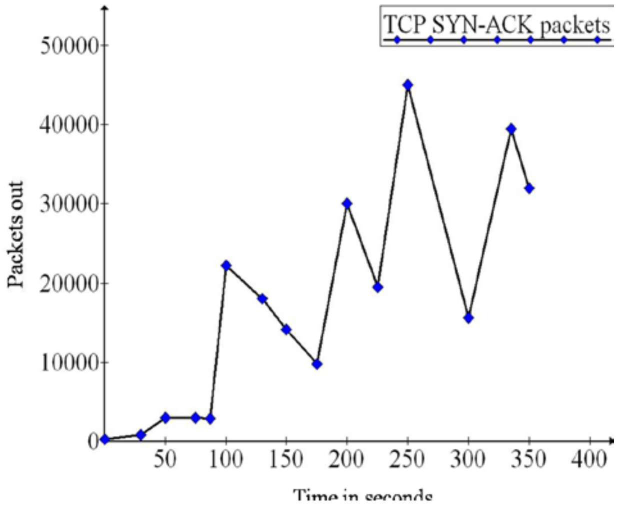

Fig.10 Number of SYN response packets from the reflector network nodes

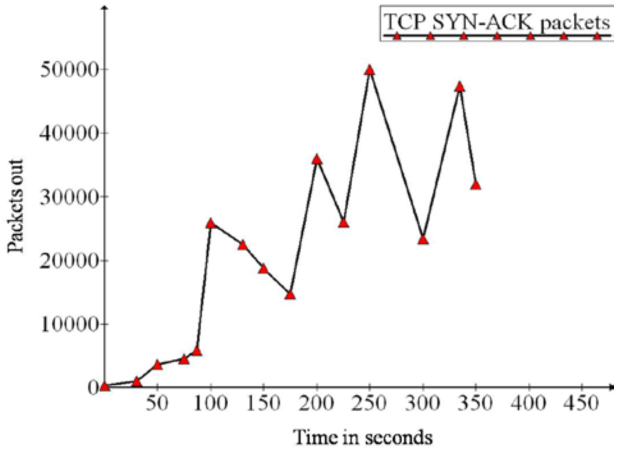

Fig.11 Number of Reflected SYN response packets from the reflector network nodes

The SYN request from the attack network multiplied with some random factor for achieving the highest amplification. The amplified response packets generated from the reflector network to target server is shown in Figure 11. The amplification factor is calculated using the (1).

$$Amplification\ Factor = Size\frac{(\ Response\ )}{(\ Request\ )} \qquad (1)$$

Figure 12 shows the amplification ratio between received requests from reflector network versus reflected responses to the target server.

The amplified response traffic entered in target server and it restricts the incoming legitimate traffic. Figure 13 shows total number of SYN response packets and separate the DDoS and DRDoS attack traffic. The TCP-SYN reflection attack acquires high bandwidth to stop providing access to the legitimate clients. The impact of SYN flooding attack is slightly lesser when compared to SYN reflection attack. The SYN flooding attack utilizes the server resources such as CPU, memory and disk and high amount of network bandwidth. The TCP SYN reflection attack exhausts the entire server resources and bandwidth. Due to this reason, the resource and bandwidth distribution to the legitimate requests are minimum otherwise these are unavailable to these requests.

Horizontal axis indicates the attack scenario and it is measured in terms of time in minutes and the vertical axis indicates the bandwidth utilization of TCP SYN-ACK packets as a measure of bytes per second.

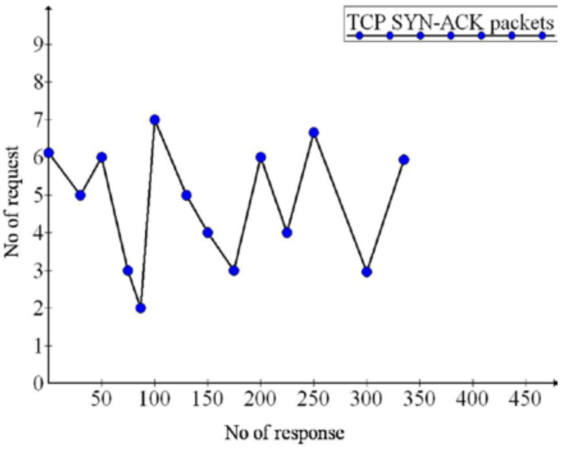

Fig.12 Amplification factor

During the initial stage of attack, some amount of legitimate traffic enters into the server for 40 seconds. After the TCP-SYN DRDoS attack, the entire bandwidth of the target server is utilized by the reflectors for SYN reflected response packets. It ultimately denies the service of the legitimate requests. Both the malicious traffic and the legitimate traffic are inversely proportional to one another. When the amplification factor (Number of SYN-ACK response packets for the incoming TCP SYN-Request packets) gets decreased, simultaneously the legitimate traffic gets increased.

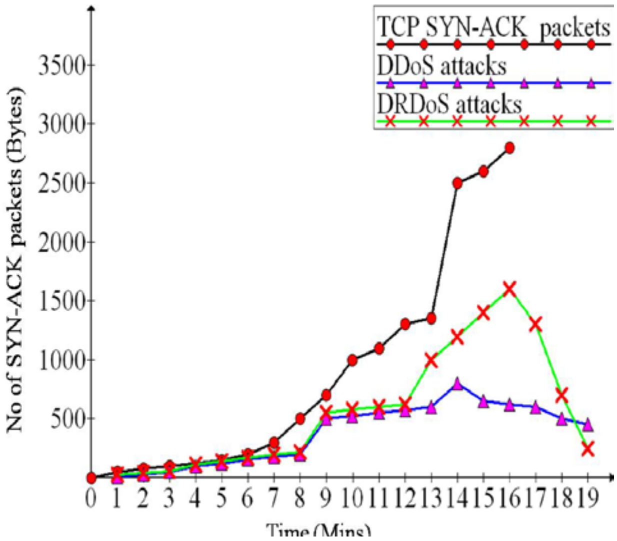

Fig.13 Packet arrival rate at the target server during attack

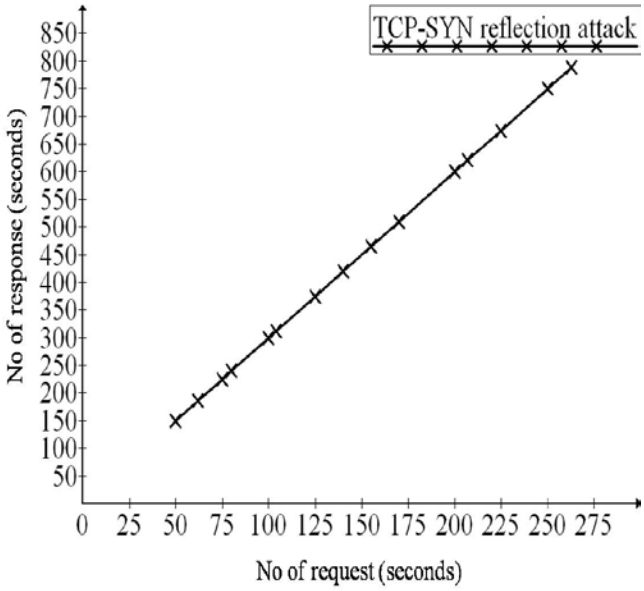

Fig.14 Reflection attack at the target server

The Figure 14 shows the request and their corresponding amplified response packets. The response packets are linearly increasing with spoofed SYN request packets. The amplification factor is used to measure the bandwidth utilization of target web server with the parameters such as incoming request packets and the outgoing response packets.

Figure 15 shows the bandwidth utilization of legitimate, DDoS and DRDOS attack traffic. The legitimate traffic is inversely proportional to the DDoS and the DRDoS attack. The exhaustion of bandwidth is huge in reflected attack when compared to DDoS attack. By this observation, it clearly shows that DRDoS attack is more harmful than DDoS attack.

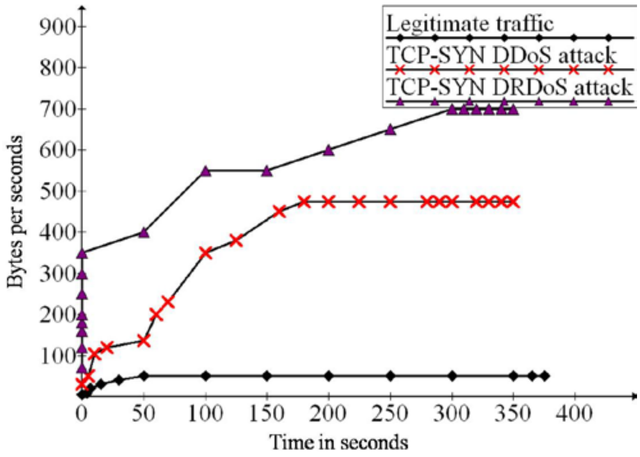

Fig.15 Bandwidth utilization of reflection attack at the target server

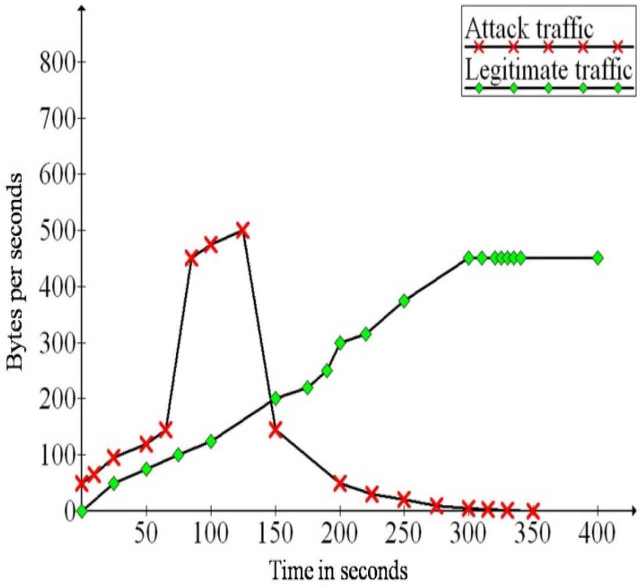

Fig.16 Performance of proposed RALF based IP pairing detection method

The Reflection Attack Log File based IP pairing detection method receives the TCP SYN request packet from the target server. The incoming request packets information are stored in the log file. These information are compared with the incoming SYN response packets for identifying the reflected response packets. The proposed RALF based IP pairing detection method is applied as the intermediate network based solution.

The proposed RALF based IP pairing detection method detects the TCP SYN-ACK response packets. The proposed detection method is evaluated with the 350 secs of captured reflected attack traffic. The performance of the proposed detection method is explained in figure 16. In this, the proposed detection method is applied at the time period of 150 seconds. During the attack, the arrival of rate legitimate packets is inversely proportional to the reflected packets. The proposed detection method decreased rate of reflected response packets and increased the legitimate request response packets. The CPU, memory and disk resource distribution to legitimate requests are also increased. This method achieves (99%) of True Positive Rates (TPR) and less (1%) of False Positive Rate (FPR) when compared to existing reflected attack detection method. The table represents the performance comparison of various detection method which is used to detect the reflected attack traffic. The results show that proposed RALF based IP pairing detection method effectively detects the TCP-SYN reflection attacks before the attack mount on target server.

Table 3. Comparison between existing and proposed detection method

Existing detection methods	True Positive Rate	False Positive Rate
PF detection method	95%	4%
Request response relationship based detection method	94%	3%
CARD based detection method	88%	7%
RCD method	98%	2%
Proposed Reflection Attack Log File based IP pairing detection method	99%	0.5%

6. Conclusions and Future Work

This proposed RALF based IP pairing detection method identifies the SYN reflected attack packets. This reflected attack packets degrade the performance of network server by crashing application and operating system. The proposed method detects the reflected attack packets by extracting the attributes of the outgoing request packets. The extracted packet attributes are compared with the incoming response packets. These attributes information are stored in log file and these are maintained for the average Time-to-Live value. So the proposed method can manage the high packet arrival rate. This method can tackle all kinds of reflected attack traffic such DNS, UDP, ICMP and NTP reflection attack by extracting protocol based packet attributes. It forces selective packet discarding and overload control at the high packet arrival rate.

In the performance evaluation, it provides high detection rate and low false positive rate for SYN reflection attack traffic. The True Positive Rate (TPR) and False Positive Rate (FPR) are higher in the RALF based IP pairing detection method when compared with the existing reflection attack detection methods. However, the proposed RALF based IP pairing detection method is developed to perform protocol independent detection for all types of protocol both in large volume and low volume of attack traffic. Finally, this method achieves 99% of True Positive Rates (TPR) and low False Positive Rate (FPR) of 1% before the reflected responses mount at the target server. In the extension of this methodology, a protocol independent mitigation algorithm will develop for reflected Distributed Denial of Service attacks by considering additional packet attributes both for detection and mitigation method.

References:

[1] Basheer Al-Duwairi and G. Manimaran, Distributed packet pairing for reflector based DDoS attack mitigation, *Computer Communications*, Vol.29, No.12, 2006, pp.2269-2280.

[2] Hiroshi Tsunoda, Kohei Ohta, Atsunori Yamamoto, Nirwan Ansari, Yuji Waizumi and Yoshiaki Nemoto, Detecting DRDoS attacks by a simple response packet confirmation mechanism, *Computer Communications*, Vol. 31, No. 14, 2008, pp. 3299-3306.

[3] Reeta Mishra, Anticipation methods from DRDoS attack, *VSRD International journal of*

Computer Science and Information Technology, Vol.2, No.11, 2012, pp. 890-894.

[4] Rupa Rani, A.K.Vatsa, CARD (Continuous and Random Dropping) based DRDOS Attack Detection and Prevention Techniques in MANET, *International Journal of Engineering and Technology*, Vol.2, No. 8, 2012, pp.1449-1456.

[5] Shuiyu, Wanlei zbou, Weijia jia, Song Guo, Yong Xia and Feilong Tang, Discriminating DDoS attacks from flash crowds using flow correlation coefficient, *IEEE transactions on Parallel and Distributing Systems*, Vol.23, No.6, 2012, pp. 1073-1080.

[6] Shuiyu, Wanlei zbou, Weijia jia, Song Guo, Yong Xia, Feilong Tang, Trace Back of DDoS attacks using entropy variations, *IEEE Transactions on parallel and Distributed Systems*, Vol .22, No.3, 2011, pp. 412-425.

[7] Wei Wei, Feng Chen, Yingjie Xia and Guang Jin, A Rank Correlation based Detection against Distributed Reflection DoS Attacks, *IEEE Communications letters*, Vol.17, No. 1, 2013, pp. 173-175.

[8] Yonghui Li, Yulong Wang, Fangchun Yang and Sen Su, TraceBack DRDoS Attacks, *Journal of Information and Computational Science*, Vol.8, 2011, pp.94-111.

[9] Yoohwan Kim, Wing Cheong Lau, Mooi Choo Chuah and Jonatan Chao, Packet Score: A Statistics-Based Packet Filtering Scheme against Distributed Denial-of-Service Attacks, *IEEE Trans. On dependable and secure computing*, Vol. 3, No. 2, 2006, pp. 2594-2604.

[10] Xiao, Bin, Wei Chen, and Yangxiang He, A novel approach to detecting DDoS Attacks at an Early Stage, *The Journal of Supercomputing*, Vol. 36, No. 3, 2006, pp. 235-248.

[11] Mohana Priya P, Akilandeswari V, Mercy Shalinie S, Lavanya V, Shanmuga Priya M, The Protocol Independent Detection and Classification (PIDC) System for DRDoS Attack, *Fourth International IEEE Conference on Recent Trends in Information Technology (ICRTIT)*, 2014.

[12] Akilandeswari V, Mercy Shalinie S, Probabilistic Neural Network based attack traffic classification, *Fourth International IEEE Conference on Advanced Computing (ICOAC)*, 2012.