CHAPTER 5
APPLICATION SERVICE ORIENTED NETWORK REQUEST IDENTIFICATION (ASNRI) TECHNIQUE FOR RESISTING DDoS ATTACKS IN IP AND MAC FRAMES

5.1 Introduction

An Internet host can spoof IP packets by using a raw socket, to fill arbitrary source IP addresses in their IP headers. IP spoofing is associated with malicious network behaviors, such as Distributed Denial of Service (DDoS) attacks. As one of the most difficult problems in network security, the DDoS attacks have posed a serious threat in internet services. Instead of collapsing the entire services, the DDoS attacks limit and block legitimate users’ access to victim server resources. The attackers hide the flooding sources in victim traffic by spoofing 32-bit source IP address in a random manner. The famous DDoS attacks, such as smurf and DRDoS (Distributed Reflection Denial of Service) attacks, are generated by IP spoofing. Such attacks imitate the source IP address of each spoofed packet in the victim’s IP address. It is difficult to counter IP spoofing, because of the stateless and destination-based routing of the Internet. The IP protocol is not efficient in preventing a sender from hiding the origin of its packets. Furthermore, destination-based routing does not maintain state information on senders, and forwards each IP packet towards its destination without validating the packet’s true origin. Overall, IP spoofing makes DDoS attacks more dangerous in internet services.

The Application Service Network Request Identification (ASNRI) technique proposed in this work comprises of components such as Application Services, network request, identifiers of the IP and MAC Frame packet streams, Bayes packet classifier and filters. These components work interactively to improve the response time of resisting App-DDoS attacks, maintain load balances and improve throughput of the application services. Application services are generated by network server to render various utility services to the clients. When there is a communication between active clients and target
servers, the users requests get denied by DDoS attacks, which are initiated by vulnerable servers. The client requests are in IP and MAC frame packet streams, to invoke application services from respective network servers. The DDoS attacker targets services at different bay, and the characteristics of the network request processing vary accordingly. In order to handle different packet attack variances, the proposed ASNRI technique identifies packet streams to its nature of propagation in the network and classifies it separately with Bayes packet classifier. The Bayes packet classifier presented in the early stage of the proposed work is integrated with the ASNRI technique to improve the throughput of the target network application services and to handle the load balances effectively.

5.2 Bayes packet classifier for IP and MAC frames

DDoS attacks often use special techniques such as 'packet-forgery' (creation of a false packet), 'IP spoofing' (altering an IP address within a packet) and other packet-level attacks to initiate (or to continue) an attack. The attacker generates malicious activities on a network packet that affects the target system, or any other component of the system to react, which in turn stimulates the attack on the target system. The attacks are generated during the communication between the systems either in a local network or over the internet.

It is well known that most DDoS attacks use spoofed source IP addresses. Moreover, the number of packets from the same spoofed source IP address is relatively small, compared to the number of packets of a real session. Consequently, to generate a huge amount of attack traffic, a large number of spoofed source IP addresses are needed. Based on these assumptions, traditional schemes use the ratio of the number of the new IP address to the total number of IP addresses, to detect attacks with spoofed source IP addresses.

By using traditional schemes, a database is required to store the information of all IP addresses that appeared in a certain period, which means that the required memory size is very large for large-scale Internet. As conventional schemes are not suitable for
large-scale ISP networks, the entropy of new IP addresses have been considered as a feature for detection. The complexity of calculating entropy for large-scale Internet can be extremely high. To detect DDoS attacks, the following features are used such as the ratio of SYN to SYN/ACK, the percentage of new IP addresses, and entropy of the IP address distribution. Features are important since they significantly affect the performance of detectors. The above mentioned existing features either do not lead to better performance of detectors, or require high storage/time complexity.

To address these deficiencies, this work proposes the ASNRI technique, which introduces a Bayes Packet Classifier for IP and MAC frames to efficiently extract features. It classifies the normal and attack traffic, and it is used to improve the accuracy of detecting attacks in both IP and MAC frames.

Attackers commonly spoof the source IP address field to hide the location of the attacking host. The key observation behind this task is to generate Application layer DDoS (App-DDoS) attacks. Most programs select source addresses at random for each packet sent. These programs include most popular distributed attacking tools such as, Shaft, Tribe Flood Network (TFN), TFN2k, trinoo, all variants of Stacheldraht, and Trinity. When a spoofed packet arrives at the victim, it sends an appropriate response to the faked IP address. Occasionally, an intermediate network device (such as a router, load balancer, or firewall) may issue its own reply to the attacks through Internet Control Message protocol (ICMP) messages. Again, these ICMP messages are sent to the randomly spoofed source address. Because attacker’s source address is selected at random, the victim’s responses are distributed across the entire internet address space, which causes a bad effect.

The features extracted from the measurement data are used for detecting Application layer DDoS (App-DDoS) attacks. To detect these attacks, the IHBCM technique is used to analyze the network traffic, but it is not clear for detecting the attacks at a low-data-rate. This proposed technique detects App-DDoS attacks, only for high-volume attack traffic, which causes significant changes in the power spectral density of
traffic. Since attacks having low-data-rate may not cause large changes in the power spectral density of traffic, the IHBCM technique is not suitable for detecting App-DDoS attacks at low-data-rate. To overcome this inconvenience, ASNRI addresses both high rate and low rate attacks.

Bayes classifier detects App-DDoS attacks for the IP and MAC framework. Specifically, it is used to detect the attacks induced by abrupt changes in statistical patterns of traffic, which is compared to the ‘normal traffic pattern’. However, the parameters of the existing algorithms are constant, and preset for a traffic pattern. The existing algorithm parameters do not have the capability to adapt dynamically when the traffic pattern changes. Testing the networks with a large IP address space, may significantly increase the time/storage complexity of existing detection algorithms. But the proposed Bayes classifier efficiently works in networks with a large IP address space. This classifier is used to protect the source address from spoofed App-DDoS attacks, by filtering unknown source IP addresses of all packets at edge routers. By inserting digital signature to IP packets, it prevents the source address spoofing.

5.2.1 Media Access Control (MAC) frame

MAC address table contains the MAC addresses available on a given physical port of a switch, and the associated Virtual Local Area Network (VLAN) parameters for each MAC address. After receiving a frame, the Bayes classifier searches for the destination MAC address in the MAC address table. All Catalyst switch models use a MAC address table for Layer 2 switching. As frames arrive on switch ports, the source MAC addresses are learned and recorded in the MAC address table. If an entry exists, the switch forwards the frame to the MAC address port, and it is classified by Bayes classifier in the MAC address table. If the MAC address table overflows, then the switch acts like a hub, and forwards the frame out to every port on the switch. It is referred to as MAC flooding attacks.
5.2.1.1 MAC address table overflow attack example

Figure 5.1 Bayes classification on MAC frame
For example, host A sends traffic to host B. The MAC address table overflow attack occurs in MAC address table which is limited in size. The attackers make use of this limitation to flood the switch with fake source MAC addresses until the switch MAC address table is full. Now the switch enters into fail-open mode, then it starts acting like a hub, and broadcast packets to all the machines on the network. As a result, the attacker can see all the frames sent from a victim host to another host without a MAC address table entry. In this situation, Bayes packet classifier (figure 5.1) is applied in the MAC frame to classify the normal packets, and attacked packets efficiently as well as ensure about the trustworthiness of the source IP. Then it filters the attacked packets and avoids the MAC flooding attacks.

If the switch cannot find the destination MAC in the MAC address table, then it copies the frame and broadcasts to every switch port. Host B receives the frame and sends a reply to host A. The switch then learns that the MAC address of host B is located on port 2, and writes this information into the MAC address table. Host C also receives the frame from host A to host B, now the host C has dropped that frame because the destination MAC address of that frame is host B. Now, any frame sent by host A (or any other host) to host B is forwarded to port 2 of the switch and not broadcast to every port.

5.3 Application Service Oriented Network Request Identification (ASNRI) technique

There are well-known attack techniques known as spoofing in both wired and wireless networks. The attacker constructs frames with the legitimate users’ addresses or identifiers with non-existent values, or values that belong to others. The attackers collect these legitimate values through sniffing.

An ASNRI technique for resisting App-DDoS attacks with IP and MAC frame is diagrammatically represented in figure 5.2. The proposed ASNRI model develops a counter mechanism to mitigate the potency of the resource attacks, and evaluate the efficiency. It provides a clear demarcation of wired (IP frame) service and wireless (MAC frame) service request.
The Access Matrix (AM) is introduced to capture the spatial-temporal patterns of normal flash crowd. The anomaly detector based on Hidden Markov Model (HMM), is proposed to describe the dynamics of Access Matrix (AM) and to detect the attacks. The HMM model is improvised to find the detection threshold for stationary objects in the popular website attacks.

ASNRI technique has the interaction with Bayes packet classifier for preventing the App-DDoS attacks. Then this Bayes packet classifier has the communication with Gaussian distribution factor for better detection rate even in stationary App-DDoS
attacks. The integration of Trust and AM based HMM and Bayes packet classifier with Gaussian distribution factor is called as IHBCM. In the Bayes packet classifier, resistance filters are activated to restrict the App-DDoS attacks in hybrid platforms.

5.3.1 Restriction of App-DDoS attacks by ASNRI

5.3.1.1 MAC Address Spoofing

In App-DDoS attacks, generally the attacker is in the manner of hidden state. The attackers inject the malicious frames that are observable by system administrators. But they fill the spoofed source MAC Address for the injected frames. So, these malicious packets are safe and no one identifies easily. Typical Access Point (APs) controls the access by permitting only those stations with known MAC addresses. Either the attackers compromise an AP, or spoof the legitimate MAC addresses of an AP. MAC addresses are assigned at the time of manufacture, even though setting the MAC address of a wireless card or the AP is randomly chosen by an appropriate software tool that has proper communication with the user acceptance. Such tools routinely include the MAC addresses when a station or AP is purchased. However, the attacker changes the MAC addresses programmatically, sends several frames to that address, and repeats this with another MAC address. In a period of a second, this can happen several thousands of times. In this case, ASNRI technique restricts this type of attacks by introducing IHBCM on MAC frame. Therefore, MAC addresses are filtered and cannot be changed. Known IP addresses are only used for efficient processing.

5.3.1.2 IP Spoofing

Replacing the true IP address of the sender (or, in rare cases, the destination) with a different address is known as IP spoofing. This is an essential operation for generating App-DDoS attacks. The IP layer of the Operating System (OS) simply trusts the source address, as it appears as a valid IP packet. It assumes that the received packets have been sent by the valid host. So, the IP layer of the OS normally adds these IP addresses to a data packet. The spoofer does not have communication with the IP layer but
directly to the raw network device. The attacker’s machine cannot simply be assigned the IP address of another host X. For spoofing these IP addresses, the attackers can use ‘ifconfig’ command or some other configuration tools. Other hosts will discover that there are two machines with the same IP address through the Address Resolution Protocol (ARP). IP spoofing is an integral part of many attacks.

IP Spoofing is restricted by ASNRI technique. This technique also has the interaction with IHBCM for efficiently detecting and filtering App-DDoS attacks. This technique uses the classifiers and activates the resistance filters to filter the illegitimate IP address. It checks whether an IP packet is valid or not while receiving any packet. So, this type of Spoofing is easily restricted by ASNRI technique.

5.3.1.3 Frame Spoofing

The attackers will inject the malicious frames, which is spoofed from the authenticated source addresses. So, it is not possible to be validated by 802.11 networks. When a frame has a spoofed source address, it cannot be detected unless the address is wholly bogus. If the frame to be spoofed is a management or a control frame, there is no encryption to deal with. If it is a spoofed data frame, it may be a part of the App-DDoS attack, and then the data payload must be properly encrypted.

Each computer on a network must have a unique IP address to communicate. IP addresses are virtual and assigned through software. IP and Ethernet must work together. IP communicates by constructing ‘packets’ which are similar to frames, but it has a different structure. These packets cannot be delivered without the data link layer. In ASNRI technique they are delivered by Ethernet, which splits the packets into frames by the Bayes packet classifier. Then it adds an Ethernet header for delivery, and sends them down the cable to the switch. The switch then decides which port to send the frame to, by comparing the destination address of the frame in the internal table which maps port numbers to MAC addresses.
ARP [Address Resolution Protocol] operates by sending the ‘ARP request’ packets. These packets are broadcast to all the computers on the LAN, even on a switched network. ASNRI technique examines each ARP request, checks if it is currently assigned the specified IP, and sends an ARP reply to its corresponding MAC address. To minimize the number of ARP request broadcast, the ASNRI technique keeps track of the ARP replies. When a computer receives an ARP reply, it will update its ARP cache with the new IP and MAC association. As the ARP is a stateless protocol, the ARP spoofing occurs easily in the network. This spoofing involves constructing forged ARP replies. But in this technique, there is no chance to construct forged ARP replies.

The Algorithm represents sequential steps to restrict the App-DDoS attacks efficiently. The input of the algorithm is the number of input traffic data streams (TS) in a victim network. The total number of traffic stream is represented by N. The observation time unit is represented by T. Let $S_a$ denote the source address, $S_d$ denote the destination address, to which the packet has to be sent, and $P_{id}$ denotes the packet id [Here packet id 1 and 2 refer to IP (wired) and MAC (wireless) respectively]. After classifying the streams, the Access Matrix (AM) is computed, and then Hidden Markov model (HMM) is used to observe the Abnormal Count (AC) in the traffic. For the input traffic, which is entered into the network, the detection threshold value is initialized. Probability of stream (P) is determined for each and every stream in the input traffic. Probability of stream determination (P) is the value function $Q(S, A)$. This estimates the positive streams to be obtained after every action is taken. If threshold probability P is greater than the default threshold value, the legitimate user is allowed to access the network resources. Else, the malicious user is prevented from the network. Simultaneously, this information is updated in Access Matrix. By comparing the AM with AC, App-DDoS attacks are returned if the access matrix value is greater than or equal to AC. Accordingly, anonymous streams are filtered by using resistance filters. Finally, anonymous packets are efficiently restricted. The proposed ASNRI algorithm is shown in figure 5.3.
Input : Number of Input Traffic data streams TS,
Output : Filtered APP-DDoS attacks in traffic streams
Step 1 : Let the total no. of traffic stream be N
        Let the observation time unit be T
Step 2 : For each packet in TS,
        {Identify the traffic stream S}
        \[ S = \text{ASNRI} \left( S_a | S_d | P_{id} \right) \]
        if \( P_{id} = 1 \)
        \( S = \text{IP Packets} \) (Proceeds further)
        Else if \( P_{id} = 2 \)
        \( S = \text{MAC Frames} \) (Proceeds further)
        End if
Step 3 : Compute the Access Matrix A
        \[ A_{N \times T} = [a_1, a_2, \ldots, a_N]^T \]
End For
Step 4 : After constructing Access Matrix, Form HMM
        Observed abnormal count AC
Step 5 : Initialized Detection threshold \( \Gamma \)
Step 6 : For every stream in TS
        \[ P(S, A) = Q(S, A) \]
        P \leftarrow \text{determine probability}(S)
        If \( \Gamma < \text{Threshold probability} \) P then
        Allow user enter into the network \{update A\}
        Else
        Prevent the DDoS attacks from the network \{update A\}
        End if
        If \( A \geq AC \) then
        Return DDoS attack

Figure 5.3 ASNRI algorithm for mitigating App-DDoS attacks
The architecture of the proposed ASNRI technique is diagrammatically represented in figure 5.4. This technique develops the counter mechanism to mitigate the
potency of the resource attacks and evaluate the efficiency. This technique provides a clear separation of wired and wireless service request.

5.4 ASNRI technique for resisting App-DDoS attacks

This work implements the algorithm using NS2 simulator, and the network topology is generated by this tool. The simulation consists of 1000 client nodes, each of which replays one user’s trace collected from real data sources. The ratio of randomly selected attack nodes to whole nodes is 10%. Using NS2, the superimposed DDoS attacks are generated in the network traffic, and ASNRI is deployed to mitigate these attacks efficiently. In the experiment, the traffic generation system is used to replicate the normal traffic collected from the operational network. The replicated traffic consists of a variety of TCP/IP services like FTP and HTTP, exchanged between several virtual machines, and a similar diurnal cycle is exhibited. The DDoS attacks are verified in the experiment in two different ways, namely, using CISCO switch and dedicated network instrument like probes.

5.4.1 Entropy of HMM

In this work, 12 consecutive observations have been grouped into one sequence. The ‘moving’ step is one observation unit, and a new sequence is formed using the current observation with 11 preceding observations. Thus, two consecutive sequences will have 11 overlapped observations. Then the simulation is conducted with 25 consecutive sequences, which last for 36 observation units or 3 minutes, to detect the anomaly accesses. Therefore, in every 5 seconds when a new observation is obtained, a new sequence is formed by 12 consecutive samples (corresponding to 60 seconds of traffic). This sequence is then measured by calculation of its entropy of the HMM. The moving average of entropies over 25 consecutive sequences (corresponding to 36 samples or 180 s of traffic) is used for the detection of App-DDoS attacks.

In the above ASNRI scenario, based on the entropy, the algorithm can detect the anomalies caused by the App-DDoS attacks. There exist significant differences in
entropy distributions between two groups. The normal web traffic entropies are larger than 6, but most entropies of the attacks traffic are less than 8. The statistical results of the entropy of normal training data, and emulated App-DDoS attacks are given as,

**Training data:**

Average (entropy) = - 4.0962

Standard deviation (entropy) = 0.3427

**Emulated Attacks:**

Average (entropy) = - 8.8193

Standard deviation (entropy) = 1.8285

In simulation, the value 5.3 has been set as threshold value of normal web traffic average entropy, the False Negative Rate (FNR) is 1%, and the detection rate is 90%. The contribution ratio helped to choose the first principal components (PC), because the number of the remaining principal components will disturb the high precision of detection. The results demonstrate the reasonable detection accuracy for ASNRI technique.

Simulation of ASNRI technique for resisting App-DDoS attacks are carried out to evaluate the performance in terms of the following.

- Delay
- Bandwidth
- Attack resistance rate (kbps)
- Throughput (kbps)
- Acceptance rate of legitimate user sessions
- Detection Rate
- False positive rate
5.4.2 Performance of False Alarm Rate

The detection curve crosses the equal-error line. At that point, the system achieves a detection rate of 96.2%, and a false alarm rate of 3.8%. The DDoS attacks mimic normal data points, and this causes false alarm. A restriction upon the system that requires 2 to 3 consecutive data vectors is recognized as ‘attack’ before the presence of an attack. In this experiment, although the false alarm rate is reduced significantly to the rate of 2%, the maximum detection rate goes down, as well. In fact, because of the consecutive alert restriction, the system is unable to detect DDoS traffic present at the beginning and ending edges of the test periods. Therefore, the maximum detection rate is below 100%.

5.5 App-DDoS attacks detection by ASNRI

![Figure 5.5 Evaluation of node 33’s request](image)
Figure 5.5 shows that the network topology is implemented using ASNRI technique. Here, the node 33 sends a communication request to node 8. Then the node 8 evaluates whether the nature of request of node 33 is legitimate or malicious. If it is legitimate, node 8 accepts its request, otherwise the node 33 is prevented from the network by ASNRI.

![Diagram of network topology with nodes numbered from 0 to 29, showing communication requests between nodes.]

**Figure 5.6 Evaluation of node 32’s request by node 22**

Figure 5.6 shows that the node 32 has an interaction request with node 22. The node 22 is monitored by ASNRI technique. Whenever the request reaches the node 22, this technique evaluates the nature of incoming request.
In Figure 5.7 the node 32 sends the communication requests to node 22 and node 23. These nodes ensure the trustworthiness of node 32. Simultaneously, the node 33 transfers a request to node 15. This technique efficiently identifies whether the request is raised by legal or illegal user.

Figure 5.7 Evaluation of node 32’s request by nodes 22 and 23, and node 33’s request by node 15

Figure 5.8 demonstrates the communication among the nodes. All the nodes in the network are monitored by ASNRI. Here, the node 32 sends the requests to node 23 and node 6. These nodes make sure about the nature of requests. Parallely, the node 33
conveys a request to node 2. This technique effectively determines whether the request is issued by legitimate or illegitimate user.

Figure 5.8 Evaluation of node 32’s request by nodes 23 and 6, and node 33’s request by node 2

Figure 5.9 shows that the nodes 1 and 6 have an interaction request with node 3 and node 23. The nodes are monitored by ASNRI technique. Whenever the request reaches the nodes 3 and 23, this technique evaluates the nature of incoming request.
5.6 Summary

This chapter introduces the ASNRI technique to prevent the malicious users from the victim network. First it classifies the IP Stream and MAC stream separately. Then it has the interaction with the IHBCM for effectively mitigating App-DDoS attacks from the victim resources. It gives importance only to the legitimate users, and identifies efficiently those who act like a legitimate user. Then, with the support of Bayes packet classifier, these illegitimate users are filtered from the network.