Chapter 7

Conclusion and Future Work

In this research, I discuss different approaches to defend against DDoS attacks. As discussed in chapter 1, near real time detection is a key criteria for DDoS defense system. A DDoS defense system also should be able to separate the attack packets from benign packets. One of the major concern associated with DDoS attack is IP spoofing. Due to IP spoofing it becomes very difficult to separate attack packets from benign packets. Hence, it is necessary that a DDoS defense system has the capability to detect spoofed packets. Another issue that I address in the thesis is IP traceback, which attempts to reveal the actual source of the attack packets by sniffing them up to their LAN. I report a DDoS attack generation tool named as TUCANNON as an appendix to the thesis.

7.1 Thesis Contribution

Here I summarize the contributions made in the thesis

(a) A Light Weight DDoS Detection Mechanism: A light weight DDoS detection mechanism has been developed which monitors the number of sources communicating with the victim. Also, the packet rate of the sources are monitored. An attack alarm is generated if there is any sudden change in these two observed parameters. Change point detection method has been used to detect sudden change in these parameters. We used both test bed generated attack traces as well as publicly available attack traces to validate our method. Experimental results show that our detection mechanism is capable of detecting an ongoing DDoS attack in near real time.

(b) A DDoS attack detection and mitigation system: Based on observing the bi-directional nature of a communication a DDoS detection and mitigation system has been developed. Our approach is not only capable of detecting an attack at near real time but also can filter the attack packets from normal packets more accurately. We have performed extensive experiments to show the behavior of our model at different attack situations such as constant rate attack, subgroup attack, randomly spoofed attack, low rate attack and high rate attack.

(c) Packet marking based anti spoofing techniques: In this work we first propose a path encoding scheme called as XORID, which enables a packet to carry a code in its 16-bit ID field. We demonstrate the advantages of our proposed method over other existing similar methods. Further, we propose and demonstrate a source end packet marking scheme called as SEM to overcome some of the drawbacks associated with path based marking schemes. Our experimental results show that SEM is superior in terms of both false positive rate as well as false negative rate than the existing schemes.

(d) A logging based IP traceback mechanism: An effective logging based traceback mechanism has been developed, which is capable of tracing back a flow up to its originating LAN. Our mechanism requires comparatively less storage in an intermediate router than the existing schemes. We demonstrate both theoretically and experimentally that our method has a zero false negative rate and a low false positive rate of attack source identification.

7.2 Discussion

In the above section, I mentioned different pieces of my contributory works in the research. Here, I summarize these different pieces to make a complete picture. To discuss how these different techniques fit into a single picture, I first categorize a stream of DDoS attack packets based on the nature of the SIPs of the attack packets as follows.

1. *Spoofed attack packets:* In this category an attack packet carries a different SIP other than the actual SIP of the sender of the packet. Spoofing can be grouped as two different types.

(a) *Random spoofing:* In random spoofing, the attacker changes the SIP addresses of the attack packets randomly and dynamically.

(b) *Selected spoofing:* In selected spoofing, the attacker spoofs the SIPs of the attack packets with the SIPs of one or more specific sources.

2. *Non spoofed attack packets:* In this category the attack packets received by the victim always carry the genuine SIPs of the senders of the packets, such as the stream of packets received by a victim during a DRDoS. Based on the type of the OSI reference layer of the attack, non spoofed attack packets can be categorized as

   (a) *Network layer non spoofed attack packets:* This category includes the stream of packets which does not contain spoofed SIP, but violates Internet communication pattern. For example, a huge surge of reply packets from a set of devices towards the victim which never sent the request packets.

   (b) *Application layer attack packets:* In an application layer attack the goal is to overwhelm the computational resources of a server by issuing it huge number of requests. In this type of attack, the attacker uses its genuine SIP and also participates in a valid Internet communication with the server.

Based on the above classification, In Table 7.1, I mention the strengths and limitations of my proposed techniques.

Table 7.1: Strengths and limitations of the proposed techniques against different types of DDoS attack traffic

	Spoofed attack		Non spoofed attack	
Technique	Selected	Random	Network layer	Application layer
DDM	Ineffective	Degraded	Effective	Ineffective
XORID/SEM	Effective	Degraded	Ineffective	Ineffective
SFT	Effective in combination with other defense mechanisms	Effective in combination with other defense mechanisms	Not applicable	Not applicable

In this research, I discuss mainly about network layer DDOS defense mechanisms. Hence, my proposed solutions are not applicable and thus ineffective against application layer DDoS traffic.

DDM performs effectively against non spoofing network layer DDoS attacks such as DRDoS where, the attack packets received by the victim always carry the genuine SIPs of the senders of the packets. In case of a random spoofed attack, DDM's performance degrades as it has to rely on a *white list* which allows packets only from known SIPs during an attack. However, DDM is ineffective against a selected spoofing attack as it can not distinguish an attack packet from a benign packet if both the packets carry the same SIP.

XORID and SEM are packet marking techniques which allow a packet to carry an identification mark that is consistent with respect to a particular sender, irrespective of the SIP used in the IP header of the packet. These defense mechanisms maintain a table to map the SIP addresses to their corresponding identification marks. Unknown SIPs are verified by sending them a probe request packet (such as TCP ACK) and then comparing the identification marks of the original packet and the response packet corresponding to the request packet. Thus, such a defense mechanism is effective against selected spoofing attack where, the SIP of the incoming packet can be verified based on its mark. However, under a random spoofing attack most of the SIPs are unknown. Verification of each SIP under this situation might create a huge load on the network which, in turn might help the attacker to achieve its goal. The situation is handled in the same way as it was done in DDM, i.e., allowing packets only from known SIPs with valid identification marks. Thus, a random spoofing attack degrades the performance of the defense system.

SFT is a traceback mechanism which, when provided with a list of SIPs, can reach the actual sources of the communications. Thus, SFT is effective against both selective and random spoofing attacks, as it can potentially reach and block the attack packets at their sources. However, SFT needs a DDoS defense mechanism which can pinpoint the malicious SIPs and initiate the traceback procedure.

7.3 Future Research

In this section, I briefly discuss some of the topics to explore to continue the research in the future direction.

7.3.1 Software Defined Network(SDN) Based DDoS Solution

SDN is an emerging technology which allows to configure ang manage a network pragmatically. An SDN decouples the routing process called as control pane from the forwarding process called as data plane, which allows all the logic processing task of a network to push to one or more centralized units called as SDN controller. Following are some of the major advantages provided by SDN paradigm to defend against DDoS attacks

1. SDN allows a network administrator to monitor and process network wide traffic characteristics from a single point. Thus detection of a DDoS attack becomes easier in SDN as a more global view of the network is available to the defense system.

2. Since in SDN the control plane does all the routing processing, efficient SDN programs can be written easily to block attack traffic at an upstream router and redirecting traffic to specific point. Thus, a real time DDoS attack mitigation system can be constructed using SDN.

3. SDN allows the controllers to communicate through standard APIs. Thus, such a network of SDN controllers can be used to perform trace back operations.

Even if SDN offers many different features which can be used to construct an efficient DDoS defense system, due to the centralized controller based structure SDN suffers from single point failure problem. How to prevent an SDN controller from being a victim of DDoS attack is another research direction.

7.3.2 DDoS Attack in Cloud Computing Environment

Cloud computing is the technology that allows dynamic accusation of software, hardware and services. based on deployment cloud computing can be categorized as public, private and hybrid cloud. A public cloud resource is shared by many organization, while on the other hand private cloud is restricted to mainly a single organization. Hybrid cloud is partially public and partially private. Following are some of the differences of DDoS attack defense system in cloud computing environment and traditional DDoS defense system.

1. In a cloud computing environment resources are controlled by the cloud providers rather than the user whereas in traditional DDoS defense system the protected servers and other resources are assumed to be under the defender's controlled network.

2. In cloud computing environment the resources are dynamically allocated based on requirement through visualization. Hence in cloud computing environment a DDoS defense system must be able to accommodate the dynamic topological changes.

3. In cloud computing environment the same network infrastructure is shared by different users. Thus, a DDoS defense system in cloud computing environment should not affect other cloud users.

A future direction of my research is to explore the DDoS defense mechanism in a cloud computing environment.

7.3.3 DDoS Mitigation System Against IoT Based Botnet

In September 2016, computer security consultant Brian Kreb's website was hit with massive 620 Gbps DDoS attack [165]. This attack was different from all other previously encountered DDoS attacks in many different aspects such as it was approximately double the size of the largest DDoS attack seen till that point of time, the attack did not use any reflection servers to amplify their attack traffic towards the victim site and most of the attack traffic appeared to be generic routing encapsulation (GRE) data packets. As spoofing is not possible in GRE data packets and no amplification technique was used, the attack traffic must have been generated from thousands of infected devices. Another similar type of attack [166] except, many times bigger (1.1 Terabits per second) than the attack on Krebs website was launched against a French Web host within two months of the first attack. The postmortem of the attack traffic towards the victim sites revealed the presence of an IoT based botnet, called as "Mirai" [157] behind these attacks. Following Mirai, within a few months, there appeared many different variants of IoT based botnet such as Hajime[161], Bricker Bot[160], Satori[159], JenX[158], OMG[162], Wicked[163] and IoTroop[164], performing DDoS attacks at different speed and frequency. All these IoT based botnets primarily dig their tunnel by circumventing the feeble protection mechanism of the IoT devices. In [36, 48, 50], the authors provide a detailed description of different security issues associated with IoT, IoT

based bonets and some of the preventive techniques against such botnets. A direction of my research is to explore different security related issues associated with IoT in order to prevent IoT botnet based DDoS attacks.

7.3.4 DDoS Mitigation System Against Critical Infrastructure Systems

Now a days availability of critical infrastructure networks such as power grids, transportation system, health care system and drinking water supply system are becoming survival factor .

The most vital component of such a critical infrastructure network is Supervisory Control and Data Acquisition (SCADA) system. SCADA is the regulatory unit of a critical infrastructure system responsible for monitoring and managing the core functionalities of the critical system. Although, traditionally such SCADA systems were isolated from public communication networks, the invent of IoTs made such systems more and more connected to the public networks [150]. As a result, critical infrastructure networks are being exposed to a plethora of legacy cyber attacks, including DDoS, more than ever. Some glimpses of the threat against critical infrastructure network were already demonstrated by the attackers in the recent past such as DDoS attack against Swedish railway systems [148], the WannaCry ransomware attacks [149], DDoS attack on Danish rail operator [147] and DDoS attack against heating distribution systems in eastern Finland [146]. A successful DDoS attack against an organization might vary from financial loss to negative impact of the organizations brand name, however, a successful DDoS attack against a critical infrastructure network might have serious impact on peoples life and health. Realizing the extent of damage which can be caused by an attack at the critical infrastructure, researchers have already put a great deal of effort in developing possible mitigation system against such attacks. A remarkable contribution towards the research is the development of Secure Water Treatment (SWaT) testbed [152]. SWaT is a scaled down version of a real-world industrial water treatment plant which allowed data collection both under normal and attack scenario. Their published datasets contain both physical properties such as reading of different sensors and actuators as well as network traffic among different units of the SCADA system. Another critical infrastructure based dataset is published in [155], containing 5 different operational scenarios namely normal, anomalies, breakdown, sabotages, and cyber attacks. In [156], the authors propose a Controllerin-the-Middle (CitM) scheme to provide flexible experimental environment for CPS security research. In

[151], the authors used recurrent neural networks to detect abnormal operational conditions in Cyber Physical Systems (CPS). A graphical model based technique is developed in [154] to model normal operational conditions based on the SWaT dataset. In [153], the authors proposed the use of unsupervised learning techniques to detect the abnormal conditions in a CPS. Following these above mentioned research work, another future direction of my research is to investigate and develop near real time DDoS attack mitigation system against critical infrastructure networks.