Asian Journal of Computer Science and Technology
ISSN: 2249-0701 Vol.7 No.3, 2018, pp. 62-67
© The Research Publication, www.trp.org.in

Vulnerability Analysis of Existing Distributed Denial of Service (DDoS) Defense Frameworks

Shaveta Gupta[1], Dinesh Grover[2] and Abhinav Bhandari[3]
[1]Assistant Professor, Department of Information Technology, PGGC, Sector 11, Chandigarh
[2]Ex-Professor & Head, Department of CSE, PAU, Ludhiana
[3]Assistant Professor, Department of Computer Science and Engineering, Panjabi University, Patiala
E-Mail: shaveta.83@gmail.com

Abstract **- The world is quickly moving towards an era of digitization. Scope and volume of the network are becoming vast that makes these machines more prone to cyber-attack due to vulnerabilities of the network. There are various types of cyber-attacks but most common and equally impactful is DDOS attack. A foolproof defense mechanism is need of the hour. Analysis of various existing defense mechanism frameworks has been done and their shortcomings have been reported by us. This analysis will help to define a framework which can provide better accuracy, lesser detection time and reduced false negative and positive rates. It will further ensure better response and mitigation against the attack.**

Keywords**: DDOS Attack, Flash Events, Vulnerability Analysis, Mitigation**

I. INTRODUCTION

The term DOS, denial of service attack, used to refer the attack which hinders the availability of services and these services are meant for legitimate users but unable to avail as attacker either send large volume of malicious traffic or by sending the packets that exploit a software vulnerability to crash the system. And most common and equally impactful denial of service attack is distributed denial of service attack in which malicious traffic is originated from multiple sources although coordinate from one central site. This makes a DDoS attack much hard-bitten to block than one originating from a single IP address. Figure 1 demostrates different vulnerabilities present in the network. Today there are avast tools available those have ability to generate attack traffic having similar characteristics as those of legitimate traffic and can easily circumvent the existing ddos defence mechanisms [3].

World's biggest companies like Amazon, ebay, Flipkart etc. were affected by DDoS attacks as a result the sites of these companies are inaccessible to end users and companies had to face extremely large financial losses. In the last quarter (Q3 2017), Corero customers experienced an average of 237 attacks per month, an increase of 35% compared to Q2 2017 (175 attacks). DDoS attacks can be classified into three types: Volume-based DDoS attacks(HRDDoS), the attackers typically flood the victim with immense volume of packets to saturate the bandwidth of the destination network. Application DDoS attacks can target web applications [16]. It is the attack on layer 7 of protocol stack. This attack is very difficult to identify and mitigate. Pro- tocol DDoS attack: It is an attack on layer 3 or 4 on protocol suite [24]. Under these attacks, the target of attacker is server resources.

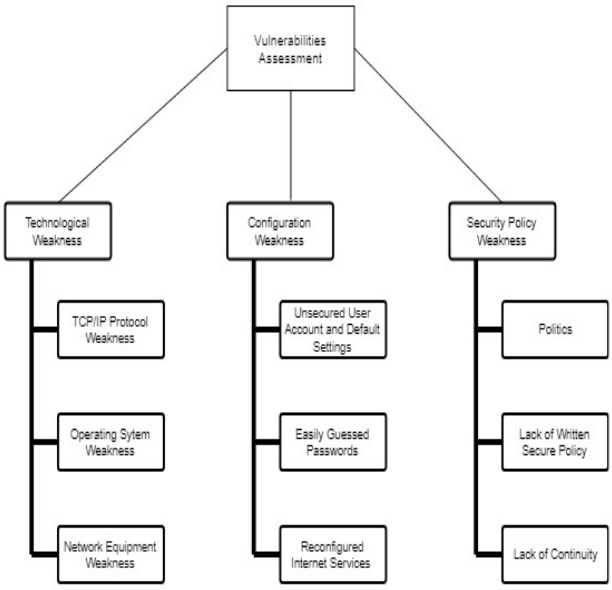

Fig. 1 Vulnerabilities in Network

In addition to above type of attacks, there is different type of network traffic whose popularity increases day by day among the security researchers and that is Flash Event [5, 9]. An FE is comparable to an HR-DDoS attack, but in this traffic is generated by thousands of legitimate users instead of bots to approach a particular computing resource such as website simultaneously. This sudden rush in legitimate traffic is mainly due to some breaking news happening around the world like publishing Olympic schedule or new product launch by top companies like Apple, Samsung etc [4]. A flash event occurred against the Australian census website on August 21, 2016.

Numerous schemes are projected to deal with DDoS and Flash Event but none of them gives us complete solution against them. More importantly, these attacks are very generic and dynamic and thus, they can easily escape from existing defense systems therefore, the way to defend against FE's and DDoS is vital research issue [6]. The remaining paper is organized as follows: Section II defines

the different phases which are a part of defense Frameworks. Section III focuses on literature of existing defense frameworks. Section IV demonstrates different techniques used in various phases of different defense Frameworks in tabular form and their corresponding vulnerabilities.

II. DEFENSE FRAMEWORK

Defence Framework is amalgamation of attack detection, characterization, Response and Mitigation modules [12, 7, 15] as shown in figure 2.Detection is the way towards identifying victim network or server attack after the launch of the attack [1]. A decent defense framework aims to detect the attack near the source end so that there is less collateral damage. It requires traffic observing and its refined behavioral examination. Characterization method involves discriminating attack traffic from legitimate traffic. This step is difficult to execute as attack and legitimate traffic look alike. Attack response: When attack is detected, or enough warning signs are captured then the next step is to minimize attack impact on legitimate users and network resources. This is covered under attack response. Techniques under Response include traceback, Filtering, Rate Throttling and Reconfiguration. Attack tolerance and mitigation approach count on that it is impossible to save you or forestall DDoS completely [17]. Therefore, it focuses on minimizing the attack effect and attempts to offer surest level of service as per quality of its service requirement to valid customers while the service provider is being attacked.

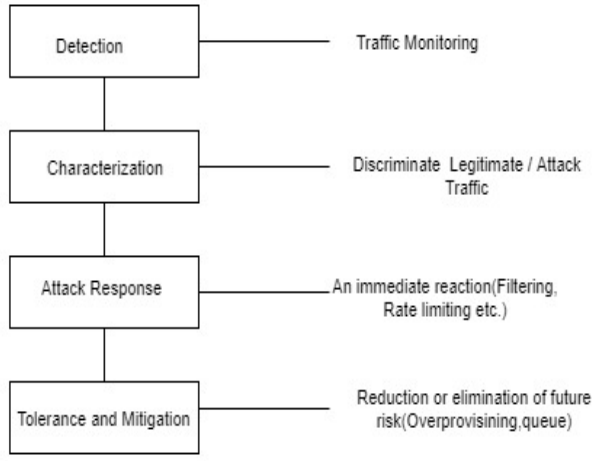

Fig. 2 Modules in Defense Framework

Mitigation is all about being proactive and take preliminary actions, it helps to determine the probability of its occurrence and corresponding impact is recognized at an advance stage to prevent deleterious affects. In short, Mitigation follows Prevention is better than cure. This step includes Over provisioning, Router Queue management, Router traffic scheduling, Target roaming.

III. EXISTING DEFENSE FRAMEWORKS

In this section we have reiterate the work done in the field of existing Defense Frameworks. The main objective of this summary is to analyze the different phases in the defense framework and obtain the vulnerabilities that exist in the frameworks.

Ahmed Redha Mahlous *et al.* [18] proposed a Multipath Traffic Filtering framework against flooding-based DDoS attacks.This framework computes various possible paths to the attacker using modified variant of Dijkstra's algorithm. It triggers an alert to the closest gateway of those paths to block all the traffic originating from attack source. The policy module (Detection phase) in this framework categorizes the incoming traffic in various flows based on source address and destination address of packets. Once the policy module recognizes an undesired flow it directs a filtering and rate limiting request to Multipath traffic filtering algorithm (Attack Response). Effectiveness of IP traceback scheme is checked by computing the number of packets needed for reconstructing a path. Multipath traceback technique uses the least number of packets needed to reconstruct a path.

Vincenzo Gulisano *et al.* [14] presents a framework, named STONE, that is potentially comparable to an expert system for effective DDoS detection and mitigation. The fundamental principle of STONE is to detect attacks by monitoring traffic and to filter out the illegitimate flow using predefined threshold limits. Major detection parameter used under STONE is Source IP Clustering. Upon detection of an attack, STONE permits legitimate users to access the service uninterrupted while discarding doubtful one. Mitigation phase uses queue management and traffic volume shaping techniques. Results obtained after implementing STONE on the real network traces shows that it detects attacks swiftly and facilitates least degradation to legitimate clients.

Abhinav Bhandari *et al.* [8] Packets based entropy approach has been used to detect flooding-based DDoS. Furthermore, the next step under this framework is to trace the edge routers point which act as entry points within ISP domain. This task has been accomplished by entropy-based trace back method by using NS2 simulator to validate this approach.

Mohammed A. Saleh *et al.* [22] proposed Flexible, Collaborative, Multilayer, DDoS Prevention Frame- work (FCMDPF) to handle HTTP based DoS/DDoS attacks. FCMDPF framework encompasses three sub- sequent multilayer points for detecting and preventing HTTP DoS/DDoS attacks. The Primary layer of FCMDPF framework is an outer attack blocking (OB) at the entry point (edge router) and it blocks Source IP if it is a part of Black List Table, while the second layer of FCMDPF framework is service traceback oriented architecture (STBOA) that is designed to evaluate if the incoming request is launched by legitimate user or bots. The third layer of FCMDPF framework is flexible advanced entropy based (FAEB) layer that is employed to detect anomalies in HTTP network traffic and to differentiate whether it is flash event or HRDDoS attacks.

Narmeen Zakaria Bawany *et al.* [2] proposed the design of SDN-oriented ProDefense framework that is modular. Three major components of this framework are traffic flow collector, policy engine, mitigation engine and attack detector. Traffic flow collector gathers the information regarding flow of the incoming traffic from OpenFlow switches. Rules are structured in policy engine for detection of attack and its mitigation. Three kinds of filters are configured to effectively detect the attacks and these are HR filter, LR filter and IR filter. The traffic flow collector gives its output to the attack detector module that generates security alerts with respect to the policy defined in Policy Engine. These security alerts trigger the mitigation module for taking relevant action. For attack mitigation, policy engine works on the defense strategies including dropping packets, traffic redirection and blocking ports.

Alberato Compagno *et al.* [11] proposed collaborative push-back approach to counter interest flooding. Poseidon is a set of algorithms that are carried out on routers to identify traffic anomalies and mitigate their effects. Poseidon detects an attack when detection parameters exceed their respective thresholds. Poseidon restrains the rate of incoming interests from interface. In order to signal about possible flooding attack is under progress, Poseidon implements a mechanism, knowns as push-back, which sends alert/message to the same interfaces.

Yang Xiang *et al.* [23] proposed two new information metrices to detect an attack several hops earlier named as generalized entropy metric and information distance metric. It combines two security approaches, IP traceback and filtering technology, to make collaborative and robust defense mechanism to counter various attacks related to network security.

K. Giotis *et al.* [13] works on Software Defined Networks (SDNs) specifically on the OpenFlow (OF) protocol. The architecture of our proposed mechanism involves three main modules the Collector, the Anomaly Detection and Mitigation. Collector module collects flow informa- tion and periodically transfers them to the Anomaly Detection module that will identify a potential attacker or the victim of the attack. The Anomaly Mitigation module blocks the looked-for malicious traffic.

A heavy drop in the Destination IP and Destination port metrics would result in Flash Crowd. A White List function is implemented manually or automated that maintains a list of IP addresses/ports that is related to legitimate network traffic. Anomaly Mitigation module inserts a drop rule in the switch, if it is not in Whitelist table.

Dhruv A Patel *et al.* [21] proposed mechanism that will examine server-load by using memory and CPU processor parameters and comparing it with predefined limit. It purposefully ignores the detection mechanism if server load is within the predetermined limit. But, if server load is on higher side then it evaluates the packet to find IP addresses. These IP addresses then get compared with Whitelist table. If result is positive then it will go to the further stage. However, if result is negative then it will go to HIP (Human Interaction Page) to differentiate attack traffic from normal traffic, if user gives answer positively then that user entry will be added in white list database to avoid unnecessary round trip through HIP. And this strategy further uses rate limiter or even denies access mechanism that will monitor requests from a specific IP in stipulated time.

Chaintanaya Buragohain *et al.* [10] proposed an SDN framework for data centers named FlowTrApp. Under this flow duration and rate are used to detect attacks across the ranges, be it on upper side of rate(HRDDos) or even at the lowest one(LRDDos), similarly for short lived or long lived durations, with the use of SDN engine. When new traffic flow reaches at the designated switches, it computes the flow statistics on a per flow basis.

If the traffic pattern comes under any one of the mentioned attack patterns/categories, then that specific flow is monitored by the Mitigate algorithm to determine about number of attempts made by the source address to attack the system. If this evaluated counter value is higher than a random legitimate value, then it blocks the source address for predefined duration. Otherwise, a flow from such source address can be passed uninterrupted.

Arpita Narayan *et al.* [20] presented a detection approach for DNS reflection attacks using request flow records to detect the attack on target. To differentiate between DNS traffic from legitimate user threshold concept has been introduced under this scheme. Next phase is to filter out the attack traffic for this hop count-based filtering scheme has been implemented.

Seung Yeob Nam *et al.* [19] proposed a mechanism that is based on two key principles. The former one is whitelist-based admission control scheme to protect the servers from surprises, for example if there is a sudden spike or surge of attack flow. Under second key idea, busy period concept defined for client and server IP has been introduced to detect attack flows.

IV. VULNERABILITY ANALYSIS OF EXISTING DEFENSE FRAMEWORK

Myriad Frameworks have been analyzed in above section and we try to delve the different techniques used under various phases of defense frameworks and result is presented in tabular form in table I furthermore, their corresponding vulnerabilities are depicted in table I.

TABLE I DEFENSE FRAMEWORKS WITH DIFFERENT PHASES

S. No.	Author/ Year	Type of Attack	Detection Phase			Response Phase		Mitigation Phase
			Classification based on timings (Passive / Ontime/Proactive)	Parameter	Detection Meteric	Attach source path identification (Trace- back)	Filtering /Rate Limiting /Recon figuration	(Overprovising/ Queue management/ traffic scheduling/ traffic Roaming)
1	Ahmed Redha Mahlous *et al.* [18] /2015	volume based	Ontime	Source address, destination address	False Positive Ratio	Packet Marking	Filtering+ Rate Limiting	N/A
2	Vincenzo Gulisano *et al.* [14] /2015	volume based	On time	Source IP clustering	Detection Time	N/A	Filtering	Queue man- agement+ traffic volume shaping
3	Abhinav Bhandari *et al.* [8] / 2015	volume based	Proactive	Destination Address	Average entropy, Standard Deviation	Link testing	Filtering	N/A
4	Mohamme d A. Saleh *et al.* [22] / 2014	Application	Hybrid (Proactive+ Active)	Source Address,User agent, Accept, Host, Request- method, web pages	Entropy	Messaging (puzzle solving)	Filtering	Queue Management
5	Narmeen Zakaria *et al.* [2]/ 2017	Application	Proactive	Flow based	Entropy	N/A	Filtering	Drop packets+ Block Ports+ Traffic Redirection
6	Alberato Compagno *et al.* [11] / 2013	Interest Flooding	on time	Interest data ratio, Adaptive PIT size threshold	N/A	N/A	Rate limiting	Drop Interests if detection per router Poseidon local: Limits PIT size Poseidon distributed: PL+ alarm downstream peer
7	Yang Xiang *et al.* [23]/ 2011	LRDDoS attacks	on time	Source IP address, packet size	Generalized Entropy, Informa- tion Distance Metric	Hop by hop IP Tracing	filtering	N/A
8	K. Giotis *et al.* [13]/ 2013	volume based	on time	Source IP address, destination IP address, the source port and the destination port	Entropy	N/A	Filtering	Drop packets
9	Dhruv A Patel *et al.* [21]/2014	Application layer	On time	Memory, CPU usage	Server Load	Messaging (Human Interaction Page)	Rate limiting	N/A
10	Chaitanya Buragohai n *et al.* [10]/2016	HRDDOS and LRDDOS	on time	Flow based on IP or MAC Flow rate, Flow duration	N/A	N/A	Filtering	Block source address
11	Arpita Narayan *et al.* [20]/2016	DNS	on time	Flow based, Request count	Accuracy, False Negative Rate, False Positive Rate, Detection Rate	Hop count	Filtering	Drop packets
12	Seung Yeob Nam *et al.* [19]/2014	Application Layer	N/A	Source IP, destination IP	Server load, count, Client induced server busy period	N/A	filtering	Drop packets

TABLE II VULNERABILITIES IN DIFFERENT FRAMEWORKS

S. No.	Author/Year	Vulnerabilities in the Frameworks
1	Ahmed Redha Mahlous *et al.* [18] /2015.	1. Multipath calculation results in Computation and storage overhead. 2. Unable to detect and control high bandwidth attacks. 3. Routers must perform complex computation to get right marking. 4. Vulnerable to fake marking made by attackers. 5. Packet marking requires large number of packets per flow.
2	Vincenzo Gulisano *et al.* [14] /2015.	1. Can't prevent attacker to exploit victim's vulnerability. 2. Does not differentiate between DDoS and Flash events. 3. If deployed on real world vantage point then challenging to maintain information in online fashion and how to share it with mitigation center.
3	Abhinav Bhandari *et al.* [8] / 2015.	1. Unable to detect isotropic DDoS attacks. 2. Discrimination between legitimate and attack traffic is challenging task. 3. Packet filtering is not effective if flooding attack use legitimate services. 4. Management overhead, higher dependency on admin, any mismanagement to assist the traceback will make it further slow, or even completion could be impossible. 5. Not suitable intermittently occurred attacks or when the attacker is aware of the traceback techniques used because link testing technique is based on the assumption that attack remains active until the completion of traceback.
4	Mohammed A. Saleh *et al.* [22] / 2014	1. Unable to detect and prevent all flash events. 2. Failed to validate and traceback all incoming requests. 3 Less accuracy rates. 4. Adds further delay to the legitimate users by asking them to solve puzzles to authenticate. 5. Difficult to maintain queues.
5	Narmeen Zakaria *et al.* [2]/ 2017	More Prone to malicious applications which can easily damage the network through controller.
6	Alberato Compagno *et al.* [11] / 2013	1. Poseidon additionally correlates the number of current PIT entries. These approaches lack the option to isolate more specifically because all nodes behind the throttled interface will be affected by this limitation. 2. Performance and accuracy issues. 3. Legitimate users will experience degraded services.
7	Yang Xiang *et al.* [23]/ 2011	1. For Hops more than 5 traceback time is larger. 2. ISP involvement. 3. Less scalable. 4. Discrimination between good and bad packets is a challenging task.
8	K. Giotis *et al.* [13]/ 2013	1. Detection near victim end so comparatively high collateral damage. 2. Discrimination between legitimate and attack traffic is challenging task. 3. Filtering is not effective if flooding attack use legitimate services.
9	Dhruv A Patel *et al.* [21]/2014	1. Difficult to implement rate limiting. 2. Hard to differentiate legitimate traffic from malicious traffic. It is not fool proof, legitimate traffic may sometimes be dropped or delayed and malicious/attack traffic may be allowed. 3. Requiring users to authenticate themselves introduce more delays to legitimate users.
10	Chaitanya Buragohain *et al.* [10]/2016	Can only detect attack specified according to algorithm.
11	Arpita Narayan *et al.* [20]/2016	1. Hop count filtering is not so effective. 2. Does not seems good for practical usage. 3. ISP involvement is high. 4. Bandwidth overhead is extremely high. 5. Until the trace process is completed, attack should remain active.
12	Seung Yeob Nam *et al.* [19]/2014	1. Only for HTTP based web servers. 2 Packet filtering is not effective if flooding attack use legitimate services.

V. CONCLUSION

A foolproof solution to negate DDoS attacks is next to impossible. Best way to keep a check on these attacks is to define metrics which cover more scenarios and have wider scope to detect attacks and then come up with equally robust mitigate techniques which can negate the attack closer to the source so that the collateral damage could be reduced to minimal.

REFERENCES

[1] Ram Charan Baishya, "Ddos attack detection using unique source ip deviaion", *International Journal of Network Security,* Vol. 19, pp. 929–939, 2017.

[2] Narmeen Zakaria Bawany, "Ddos attack detection and mitigation using sdn: Methods, practices and solutions", *Springer Arabian Journal of Science and Engineering,* Vol. 42, pp. 425–441, 2017.

[3] Sunny Behl, "Characterization and comparison of ddos attack tools and traffic generator - a review", *International Journal of Network Security,* Vol. 19, pp. 383–393, 2017.

[4] Sunny Behl, "Detection of ddos attacks and flash events using novel information theory metrics", *Else vier computer networks*, Vol. 116, pp. 96–110, 2017.
[5] Sunny Behl, "Discriminating flash events from ddos attacks: A comprehensive review", *International Journal of Network Security*, Vol. 19, pp. 734–741, 2017.
[6] Sunny Behl, "D-fac: A novel -divergence based dis- tributed ddos defense system", *Journal of King Saud university - Compter and information sciences*, 2018.
[7] Abhinav Bhandari, "performance metrics for defence framework against distributed denial of service at- tacks", *International Journal of Network Security*, 2014.
[8] Abhinav Bhandari, "Destination address entropy based detection and traceback approach against dis- tributed denial of service attacks", *Computer Net-work and Information Security*, Vol. 8, No. 1, pp. 9–20, 2015.
[9] Abhinav Bhandari, "Characterizing flash events and distributed denial of service attacks: An empirical invesigation", *Security and communication networks*, Vol. 9, pp. 2222–2239, 2016.
[10] Chaintanaya Buragohain, "Flowtrapp: An sdn based architecture for ddos attack detection and mitigation in data centers", *IEEE 3rd International Conference on Signal Processing and Integrated Networks*, 2016.
[11] Alberato Compango, "Poseidon: Mitigating interest flooding ddos attacks in named data networking", in *38th IEEE Conference on Local Computer Networks*, 2013.
[12] Christos Douligeris, "Ddos attacks and defense mech- anism: Classification and state of the art", *Elsevier Computer networks*, Vol. 44, pp. 643–666, 2004.
[13] K. Giotis, "Combining openflow and sflow for effec- tive and scalable anomaly detection and mitigation mechanism on sdn environments", *Elsevier Computer Networks*, Vol. 62, pp. 122–136, 2014.
[14] Vincenzo Gulisano, "A streaming ddos defense framework", *Expert Systems with Applications*, Vol. 42, No. 24, pp. 9620–9633, 2015.
[15] B.B. Gupta, "Defending against distributed denial of service attacks:issues and challenges", *Information Security Journal*, Vol. 18, pp. 224–247, 2014.
[16] Manju Khari, "Comprehensive study of web application attacks and classification", *3rd International Conference on computing for sustainable global development*, 2016.
[17] Ashwini Kharke, "Review on mitigation of distributed denial of service (ddos) attacks in cloud computing", *10th International Conference on intelligent system and control*, 2016.
[18] Ahmed Redha Mahlous, "A defense framework against ddos in a multipath network environment", *Communication and Network*, Vol. 7, No. 2, pp. 106– 116, 2015.
[19] Seung Yeob Nam, "Defending http web servers against ddos attacks through busy period-based attack flow detection", *KSII Transactions on Internet and Information Systems*, Vol. 8, No. 7, 2014.
[20] Arpita Narayan, "A defense mechanism: Dns based ddos attack", *International Journal of Computer trends and Technology*, Vol. 33, No. 1, 2016.
[21] Dhruv A Patel, "Detection and mitigation of ddos attack against web server", *International Journal of Engineering Development and Research*, Vol. 2, 2014.
[22] Mohammed A. Saleh, "A novel protective framework for defeating http- based denial of service (dos) and distributed denial of service attacks", *The Scientific World Journal*, Vol. 2015, No. 238230, 2014.
[23] Yang Xiang, "Low-rate ddos attacks detection and traceback by using new information metrics, IEEE transactions on information forensics and security", *IEEE Transactions on Information Forensics and Security*, Vol. 6, 2011.
[24] Gang Xiongi, "Survey of network attacks based on protocol vulnerabilities", *Springer international pub lishing*, pp. 246–257, 2014.