IJCSN - International Journal of Computer Science and Network, Volume 9, Issue 2, April 2020
ISSN (Online) : 2277-5420
www.IJCSN.org
Impact Factor: 1.5

A Survey of DDoS Attacks in Application Layer and SDN Based Environments

[1] Sharan A S; [2] Dr. Radhika K R

[1] Dept. of Information Science and Engineering, B.M.S College of Engineering,
Bengaluru, Karnataka, India

[2] Dept. of Information Science and Engineering, B.M.S College of Engineering,
Bengaluru, Karnataka, India

Abstract - The Internet usage has increased rigorously in the modern scenario; cyber-attack such as DDoS attack is still the most powerful attack that disrupts the genuine users from accessing the essential services. In application layer-based DDoS attack, attacker uses other machine instead of using his own IP address to flood the targeted system and disrupts the services, that leads to server failure. Most of the reputed enterprises are converting their networks to SDN (software defined networks) for cost efficiency and network flexibility, but DDoS is one of the most launched attack on SDN layer. DDoS attack in this type of environment leads to system failure, financial loss, data theft, and performance degradation. In our paper, extensive survey has been made to detect and prevent DDoS based attack in application layer and SDN based environment. Finally, some of the important solutions are outlined. The solutions are providing promising results based on various parameters.

Keywords - *Distributed Denial of Service, Detection, Prevention, SDN, Application Layer.*

1. Introduction

This is the age of modern computing, internet is the basic need and the backbone for distributed applications, software defined networks, internet of things and many more technologies. As internet usage increases the crime rate also increases [2]. These crime causes serious economic damage by flooding internet traffic to a network and stops the essential services.

DDoS attacks are threats to the networks. The DDoS attack process has 4 roles: Attacker, Master, Zombies and Victim. The attacker leads the operation remotely by delivering the commands. The master receives the command from the attacker and manages the zombies. Zombies perform the operations that are commanded by the master and attack the victims. Victims are the targeted system simultaneously attacked by several hosts [3].

The survey report produced by Kaspersky illustrated that the DDoS attack source which has emerged from 86 nations lasted for 329 hours. The DDoS attack size has increased by 73% and increment in HTTP based application layer attacks, from 8.4% to 9.4%. The WISR published in Q1 in 2017 says application layer is the most targeted, where in 80% on HTTP attack and 81% on DNS . Recently, DDoS attack on web servers and web applications has increased. The attackers are targeting the application layer. Application layer DDoS attack will disrupt the services rather than exhausting network resources. These attacks require less network connections for attacking and are difficult to detect because the traffic look like normal benign traffic [20].

Innovative framework such as SDN is used for resource management, monitoring and controlling the traffic in cloud computing environments. SDN is enabled with service function chaining for providing multiple network services to specific network flow. Open flow-based network in SDN are now vulnerable to DDoS attack that causes resource exhaustion [18,32].

DDoS attack will target the victims [1] and cause bandwidth depletion and resource depletion this leads to serious network degradation or suffer from file corruption, system shutdown, framework breakdown. DDoS causes huge financial loss and revenue loss to e-commerce companies these types of attack are not easy to detect [21].

Rest of the paper is organized in following manner. Section 2 outlines various strategies on DDoS attacks in application layer. Section 3 outlines DDoS based attacks in

SDN . Section 4 lists various methods to detect attacks on DDoS. Section 5 provides the solutions to prevention DDoS based attacks in Application Layer and SDN.

Table 1: Top DDoS attack that has been launched in recent years[28,29,32]

Affected Vendor	Year	Implication
Telegram	2019	They experienced "state actor sized" attack which flooded with 200-400Gbps Junk data and made servers offline
GitHub	2018	Massive traffic was clocker at a rate of 1.4Tbps for which GitHub was no prepared. When the traffic was traced it came from 10,000 autonomous systems (bots)
Dream Host	2017	Dream host is a domain name register and web hosting providers. The DDoS attack made DNS infrastructure offline.
Dyn	2016	Dyn is a DNS provider. The attack was done using a malware called Mirai; created botnet out of IOT devices such as camera, radio printers and so on.
GitHub	2015	This is a politically motivated attack targeted to the two projects of GitHub. The attackers injected java script codes to the user browser who ever used the search engine called Baidu. The infected browser tends to send HTTP request to the target.
Cloudflare	2014	Cloudflare is a security provider. It was hit by a large traffic of 400Gb traffic per second. This DDoS attack was created with help of vulnerable network time protocol. NTP is used for synchronization of computer clock, attack affected European servers and was so powerful that affected Cloudflare own network.
Spamhaus	2013	Spamhaus is an anti-spam organization which was attacked by sending 300GB traffic per second which was massively large to down the webserver.
US Bank	2012	Six US banks were attacked by hijacking bank servers and sending 60Gbps peak traffic and overloading server. The banks avoided commenting about the attack for financial reason.
SCO Group	2004	Here the attacker used Mydoom virus for flooding the servers of SCO group.
DNS	2002	Two of DNS servers were offline and seven of the servers did not respond out of thirteen, due to internet traffic.
Six MNC's	2000	A hacker of 15-year-old known as Mafia Boy has created DDoS attack and made a chaos in stock market

2. DDoS Based Attacks in Application Layer

DDoS is a cyber-attack that makes many services to the users completely unavailable or partially available. There is a risk of being attacked by the attacker that is against the principle of integrity, confidentiality and availability [10]. The number of DDoS attacks are increasing, and 8.4 million attacks have been recorded in 2019 alone. Table 1 summarizes the various DDoS attacks that has been affected to victim organizations.

2.1 DDoS attacks in Application Layer

In distributed application server location is not an important factor for users. DDoS attack on web server is growing rapidly and has caused huge economic loss for the victims. Flash crowd resembles the traffic in DDoS. The traffic created by legitimate system which are genuine due to flash events are known as flash crowds. The traffic created by the flash crowd leads to increase in the distribution of source IP address. In flash crowd, the traffic increases gradually as the news spread slowly. In the case of DDoS, the traffic increases suddenly in a small amount of time and it leads to bandwidth depletion[6,26].

A slow HTTP based attack is an application layer-based DDoS attack. In these types of attacks, attacker make use of attributes of HTTP to connect to the server so that they stay connected until the request is completed. The compromised hosts are used by the attacker is known as bots and easily makes the services unavailable by sending incomplete HTTP requests. Either incomplete HTTP header will be present in HTTP GET requests or the length of HTTP headers content field will be very huge compared to the message body of HTTP i.e. HTTP POST.

Eventually servers are filled with incomplete requests that make the web server unavailable [22,25].

DDoS attack can be created using the BOTNET that compromise large number of bots. Bots are controlled by the attacker that has neither firewall nor antivirus and are used for internet relay chat (IRC). The attacker launches DDoS attack on thousands of hosts by commanding the bots to flood by spam requests and creates malicious traffic [3,20].

DDoS attack also lead to resource depletion by following attacks [30,31,14,25]

- **UDP flood attack:** Here the request is directly sent to servers without handshake such as TCP. During this time attacker will take the advantage and send large volume of requests and create the traffic. This traffic source is difficult to detect.

- **SYN flood attack:** TCP protocol connection is made by three level way handshake. Client and Server communicate by exchanging SYN (synchronize), SYN-ACK is sent once connection is established and ACK (acknowledge) packets. The attacker sends lot of SYN packet by IP spoofing and server responds for all of these packets by SYN-ACK to those IP's and in return it waits for ACK by client. This leads to resource depletion [15].

- **Ping of Death:** In POD the attacker continuously sends packets where information can be malicious or of large size than 65,535 bytes. Due to this the operating system doesn't knows what it has received, it leads to system crash.

- **SNMP Reflection attack:** Here the attacker sends lot of SNMP queries using fake IP address to the connected devices, in turn it gets reply the fake address. By this the attacker volume will raise due to reply, until the targeted system is down.

- **LAND attack:** This attack is taken place in transport layer. The attacker will set both Source and Destination with same address in TCP segment. This leads to system failure by sending packets repeatedly to the TCP stack.

- **Authentication attack:** Here the attacker will send the fake signatures and it will be verified by the server. Verifying the signatures take lot of resources rather than creating a new signature. This leads to resource depletion.

- **CGI Attack:** In CGI attack the Perpetrator send CGI request to the target computer that consumes CPU cycles in return it stops taking requests from other sources.

2.2 DDoS Attack Strategies in Application Layer

Server load: The attacker uses bots to flood requests at a constant rate and all other bots send the requests at the same rate, which doesn't change over time. These attacks will mimic the flash event. The requests start from low level and keep rising over a slow rate which is difficult to detect; till the buffer capacity reaches the breaking point of the server. Once the buffer is full, requests of the legitimate users starts overflowing.

Constant: The intruder will decide the request rate that has to be sent to victim's web servers. Same amount of request will be sent by the botnets. This request rate is called constant.

Targeted Webpage: Here the attacker uses the strategies that mimic the legitimated users. The bots access the web pages and confuses the servers such a way the webpage is accessed by the legitimate users. Depending on accessing the webpages single/multiple attack are classified as single URL or multiple URL.

Single web page attack: In single URL attack, bots repeatedly access the single webpage from the collection of web page of a particular website. These types of attacks can be detected in a straight- forward technique. The single web page that is accessed repeatedly is main page.

Multiple Web Page attack: Bots try to access multiple web pages on random basis instead of targeting single web page, irrespective of any category. The web pages are accessed equally irrespective that can be same set of hot pages or not. These attack patterns are close to the patterns of legitimate users.

Main Page Attack: Attacker mainly targets the main page of the website. Attacker uses botnets, by sending requests to server and overloads it. This will affect the legitimate user's access to the main page, while subpages are not affected.

Dominant web page attack: In this attack intruders will figure out the most accessed web pages by the legitimate users. Then attacker will use HTTP based DDoS attack to prevent the users accessing it.

Frequent Change attack: The attacker will send malicious requests to various category of web pages. But this attack will only affect specific category of the Website, whereas other category web pages are accessible.

Web Proxy attack: The attacker uses web proxy as the mediator to send malicious request to the web server and causes traffic. Multiple web proxy will be used to send HTTP requests hence the traffic is not easy to detect.

Session Flood attack: The attacker uses bots to generate new session without terminating the previous session. Multiple session exists and the session rate increases. This leads to create multiple bot server session that creates server overloading.

3. DDoS Based Attacks in SDN

Technologies such as Software Define Networks (SDN), Internet of Things and many more are booming in the industries. One interesting feature of SDN is separation of control plane from data plane[24]. SDN is used to minimize the operations on the network and provides programmability for networks, by centralizing all the decisions of the network from a single point. The decisions to send the packets in SDN are made by the control panel[17]. Data plane will forward the packets by implementing the control plane decision. Open flow is a protocol used to communicate between switches and controller. The incoming and outgoing packets are managed by open flow to match the flow table of switch[23,30]. Based on targets, attack on SDN happens in the following ways as shown in Figure 1.

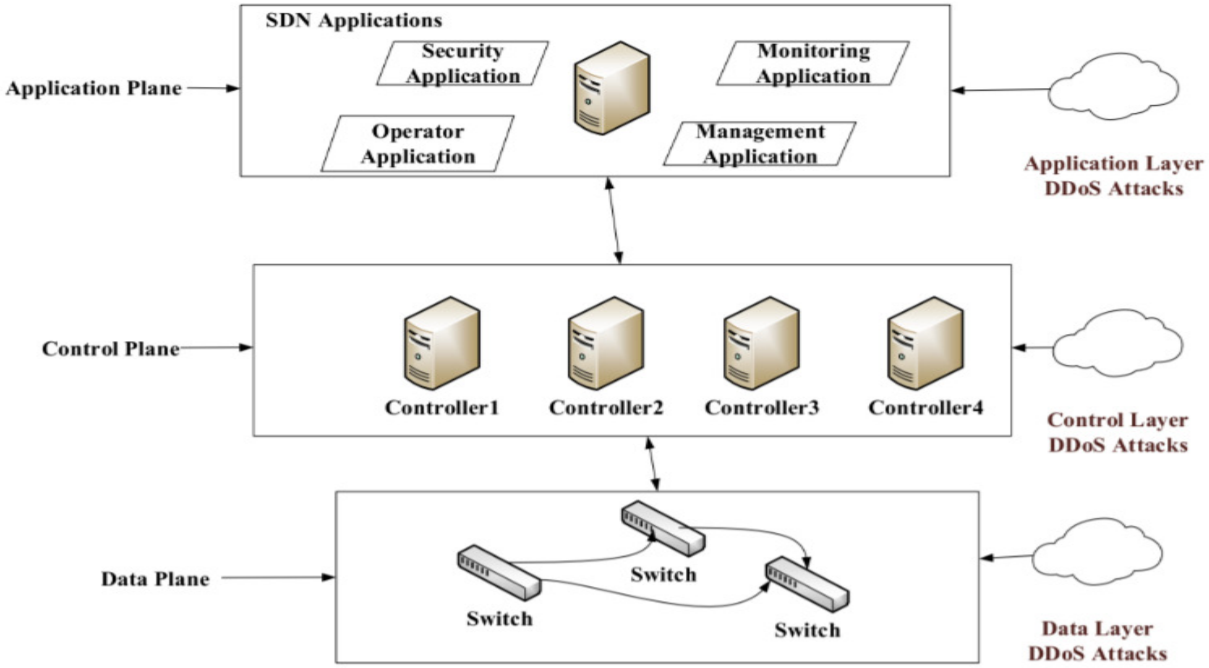

Figure 1: DDoS Based Attacks in SDN

Application Layer DDoS Attack: The attack can be taken place either by application attack or northbound API attack. The attack not only affects the targeted application but also affects the other application on that platform[12].

Control Layer DDoS Attack: Control layer in SDN architecture is more vulnerable to the DDoS attacks because of single point failure. Northbound API and South bound API launches control layer attacks. Each application has distinct flow rules. Since controller will forward the flow of packets according to the flow rules this causes chaos and leads to attack.

Data Layer DDoS Attack: Data layer must not install any malicious application. In data layer the attack happens either on southbound API or routers. For example, if packets header information is sent to controller then packets information is stored in its node until entry of the flow table is returned. The attacker uses this bottleneck to overload router and switch memory.

Open Flow Agent Overloading (OFA): OFA acts as a mediator in between switch and the controller. Whenever a new packet arrives, OFA will check if the packet matches with the flow rules. If none of the rules matches, then OFA forwards the packet to the controller. Then the controller will process the packet and send back new flow rules to the switch via the same path it had received. OFA after receiving it installs new rules to the flow table. OFA can process limited number of packets, using this limitation the attacker will send packets that has no flow rules in high rate and cause OFA overloading.

Packet Buffer Overflow: It is another module of switch which is vulnerable to DDoS attack. Packet buffer is an important factor in terms of the response time and performance. Initially when switches receive the packet, it processes and then forwards the packet to the controller. By the DDoS attack if the packet buffer is full then it tends to send full packet to controller. As a consequence, the packet starts using control channel bandwidth and resources which leads to increase in response time. The impact of the attack is:

- net flow entries cannot be installed
- congestion in control plane
- cannot divert the traffic.

Flow Table Overloading: The limited size packet buffer can be a bottleneck that attracts the attacker. The attacker requires fewer resources to overload the flow table of the switches. This new flow-based DDoS attack exhausts the controller in a network. Due to this, some legitimate entries can be dropped. This leads to network degradation, damage in network resources and services. In this the attacker will be present either inside or outside of the network.

4. Methods for DDoS Attack Detection

Tarun Agarwal et al. [4] has proposed a comber approach to protect from HTTP based DDoS attack by using SOAP message to request. The message is processed with SOAP signatures by hashing the message part. To provide extra protection, double signature is made for few parameters such as number of children, header element and body element. Next we embed SOAP header with client IP address and puzzles. All malicious packets will come to the puzzle resolver. Finally, it finds the malicious message IP address and sends the puzzle to these addresses. If the puzzle is solved correctly, then the request is from a genuine client. By this method we can detect DDoS attack and defend from it.

According to J Zhang et al. [5] they use a metric called Reduction. Using this they detect the DDoS attack. Reduction is a difference between normal data transfer rate and data transfer during attack by normal data transfer. By using fixed length, variable length link delay and hop count, Reduction rate has been observed. This Reduction rate helps to detect the DDoS floods.

K. M Prasad et al. [6] has used internet threat monitor (ITM) system for detecting DDoS attack and its strength. They are divided into 2 phases, in the first phase they detect the DDoS attack using centralized detection, hybrid detection and distributed detection. In centralized detection, threshold is maintained by data centers, if the traffic monitored by ITM exceeds the threshold then alarm will raise. In distributed approach, ITM sets the threshold if traffic exceeds the threshold, then ITM will inform the data centers to block the traffic. In hybrid, threshold is managed by both the ends. Once the threshold has been updated to data centers second phase starts. In the second phase we calculate the strength of attack using entropy. Entropy is calculated using updated threshold value, path flow and local flow.

According to Yan et al.[8] by considering all the abilities of the controller and network we draw an entropy statistic. They use POX [16] controllers and detect the attack. By using a new framework AVANT-GUARD we can provide security between data and control plane. FortNox is an extension of open flow it uses role-based authentication. It uses multiple trust anchor certificates and cryptography across the controllers and data plane.

According to Rakshitha and Ashwini [9], the use of network intrusion detection software is to inspect all the incoming packets and make a deep inspection. Instead of using algorithm they use re-configurable virtual networking approach to prevent the attempts. Initially they use software to capture the traffic and report the same to the control center. The control center will take necessary actions based on the report given by the attack graph model and the attack analyzer.

By combining Shannon entropy method and clustering algorithm [7] of relevant parameters they detect the DDoS attack. In the early stage they detect and inform the network administrator. They use ARPaD (Advanced repetitive pattern detection) algorithm that helps to detect all the patterns that are repeated in sequence. This method uses logs from the network and informs at an early stage about the attack with very less False Positive Rate (FPR) and provides security.

Aqeel Sahi et al.[11] has invented a CS_DDoS system to detect the DDoS based flood attack. Initially they will collect the packets until a time frame of 60 sec. Then on the packets are checked across the blacklist array. If any of the source is blacklisted as an attacker, then the system directly sends the packet to prevention system. If packets source is not listed in array, they are sent to classifier to classify. If a source sends more request to the same destination rather than the fixed threshold then they are subjected as attacker and listed in that array which could help in future to detect the attacker.

Vishali Kansal et al. [13] has come up with a new approach to detect proactive DDoS attack. They use early detection and isolation policy (EDIP) to overcome the attack. They place 2 types of proxies between client and server. Head proxy is used to detect attack and Attack proxy to handles insiders. Initially, head proxy assignment is done, then on load balancing is very important. If proxies are full, they will lead to performance degradation. To find the presence of the insiders, they use head proxy to compare the individual client usage value with maximum usage of client. If any value is greater than the maximum value, then the insiders or the attacker is present.

Myo Myint [19] has proposed Advance support vector machine (AVSM) algorithm to detect DDoS attack. It takes less time for testing than SVM. Whenever the packet arrives, they capture and store the traffic. Then the traffic is initialized, next the features are extracted and normalized. Then using this, they produce SVM model and classify using the testing data to generate results. This method detects DDoS attacks when the traffic is at a high rate.

Wang et al. [20] has proposed defense and detection mechanism against DDoS flooding attack. Without the use of any reverse calculation or malicious host storage we can detect using Sky Shield approach. They record and check the divergence of each packet by sketch. Each packet is inspected along various features, such as source and destination IP address, traffic rate, request time, body size and spots malicious hosts. It can only detect attacks only when the attack rate is low.

Kriti Bhushan et al. [23] has made simulation on various network logs and has provided a novel flow table sharing technique. They provide defense mechanism against the DDoS attack by using the unused flow table in the network when the flow tables are overloaded with less involvement in control plane. This approach has very less communication overhead and excellent defensive approach.

Table 2: Summary of DDoS Detection Methods

REF’s	Parameters Used for Detection	DDoS Detection Level	Dataset	Performance Metrics
[4]	Source and Destination IP, number of header elements, body elements	High rate	Realtime logs	Detection rate
[5]	Hop Count, data transfer rate, link delay, number of zombies, Attack period	Low Rate	Simulation	Reduction
[6]	Flow rate, Transfer rate, Traffic rate, Path flow, local flow	High Rate	Real time logs	Entropy
[7]	K-entropy algorithm, time, type, protocol, Source /Destination IP and port	High Rate	Network logs	Entropy , Detection rate, False Positive rate
[9]	Source Ip, Destination IP, time stamp, traffic rate	High Rate	Real time log	Accuracy
[11]	Source IP, destination IP, packet header, blacklist array, number of packets from same source	High rate	Experimental dataset	Accuracy, sensitivity, specificity

[13]	Number of clients, head proxy, client proxy, request of client per sec, size of request, data processing speed of proxy	High rate	Experimental dataset	Number of clients and request proxy can handle
[19]	SVM algorithm, Source IP, Destination IP, network traffic, HTTP header, filters	High rate	Real time logs	Detection rate, False alarm rate
[20]	Source Ip, Destination IP, time stamp, traffic rate, request time, Body size	Low rate	Datasets from web clusters	Detection rate, FPR, TPR
[23]	Size of flow table , used and vacant flow table, arrival and service rate, number of switches , number of switches flow traverse	High rate	Simulation	Detection rate
[25]	Attack rate, Host, TCP SYN flood , Slowloris and ACK flood data rate	Low rate	Simulation	Accuracy
[31]	Average packet per flow, normal bytes per stream, average duration per flow, percentage of bidirectional flow, growth of single flow and port	High rate	Real time logs	Detection rate

Abimbola Sangodoyin et al. [25] has simulated DDoS attack and detected it using simulation with Mininet. They use throughput occurred from normal distributions confidence interval to detect the attack. This method uses various parameters as listed in Table 2 and provides detection accuracy of 99%.

S. Dong et al. [31] says that application layer attack can be detected using self-organizing model by training the information from Open Flow switch. Control layer attacks can be defended by making use of centralized control in SDN. By adding centralized monitoring sort, we avoid the attack. The data layer flooding can be detected by using entropy-based algorithm to detect the lightweight DDoS attacks by running packets in Open Flow edge switch. This method has less overhead and makes less communications with controller. This method can also detect the incontinency created in the software defined networks.

5. Best Solution to Prevent DDoS Attack

5.1 Prevention of DDoS Attack in SDN

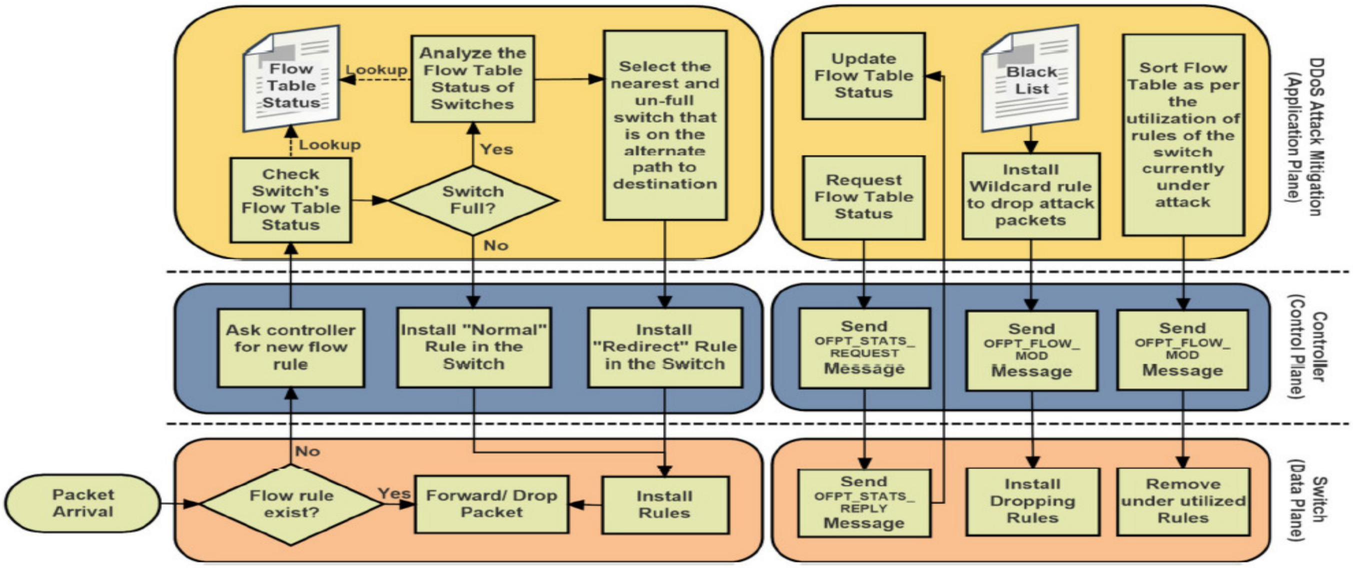
Flow Table Status
Lookup
Analyze the Flow Table Status of Switches
Select the nearest and un-full switch that is on the alternate path to destination
Lookup
Yes
Check Switch's Flow Table Status
Switch Full?
No
Update Flow Table Status
Black List
Sort Flow Table as per the utilization of rules of the switch currently under attack
Request Flow Table Status
Install Wildcard rule to drop attack packets
DDoS Attack Mitigation (Application Plane)
Ask controller for new flow rule
Install "Normal" Rule in the Switch
Install "Redirect" Rule in the Switch
Send OFPT_STATS_REQUEST Message
Send OFPT_FLOW_MOD Message
Send OFPT_FLOW_MOD Message
Controller (Control Plane)
No
Packet Arrival
Flow rule exist?
Yes
Forward/ Drop Packet
Install Rules
Send OFPT_STATS_REPLY Message
Install Dropping Rules
Remove under utilized Rules
Switch (Data Plane)

Figure 2: Architecture to Prevent SDN based DDoS Attack in SDN

As discussed, attack in SDN happens on 3 layers. The main reason behind flow table overloading is limited size of packet buffer[27]. Attacker overloads all the flow table by sending new flow rules in huge numbers. As flow table starts overloading, new flows will be dropped even though they are genuine. According to Kriti Bhushan et al. [23] the important observation is that, all the switches are not targeted for DDoS attack at the same time. Hence, we can make use of unused flow tables of the other switches to resist the attack made on a targeted switch. Further, to increase attack resistance, we need to remove less used flow and attack rules from the flow table.

Kriti Bhushan et al. has proposed an approach to avoid DDoS attack from flow table overloading as shown in the above figure 2. The approach uses 2 databases *status of flow table* that provides status of flow tables of all switches and *blacklist table* that lists all the source IP of the attacker. If any of the flow table is overloaded, then the proposed system uses status of flow table of all switches to identify the suitable switch. The approach uses few parameters such as *distance to new switch* to minimize the delay of forwarding packets to new switch, *flow table consumption status of new switch* that ensures the flow is transferred to the sufficient amount of unused flow table of other switch and *alternative path to switch* that ensures the packets are transferred to the new switch located at alternative path to new destination. Therefore, *redirection rules* are installed to redirect the traffic belonging to a particular flow to the different switch. The advantage of removing less utilized flow rules is to increase the availability of flow tables. The reason behind removing less utilized flow rules is the attacker will send a very large number of new flows with spoofed IP to fill up the table. Hence, whenever there is less utilization in flow rules the possibility of attack is high.

The attack can be avoided by collecting all the attack source IPs and stored in Blacklist database. A new rule will be formed and installed at the victim's end to directly drop the packets that come from the source IPs that are listed in the Blacklist database. The Blacklist will be updated regularly. The process that updates the *status of flow table* parameter will remove less utilized flow rules and hence can avoid DDoS attack in Software defined networks with the available resources.

5.2 DDoS attack prevention in application layer

Aqeel Sahi et al. [11] has proposed a new architecture figure 3 that can avoid the flood attacks. Each incoming packet is inspected in a detailed manner and few parameters are collected such as source and destination IP. Few parameters are set to the framework such as *threshold* that ensures how many packets can come from the same source to the same destination, *time frame* that ensures number of packets received from same source to same destination in 60 seconds, *flag* indicates normal packet when it is set to 0 and -1 for malicious packet. They make use of a database called *Blacklist Table* that has all the attackers source IP. This system works in 3 scenarios. First when a normal request packet arrives, and it is delivered in a normal manner. Second scenario when the source IP of the packet is not blacklisted but the number of packets that arrive from same source to destination exceeds the threshold. During this time the packets are treated as DDoS attack and the source is listed in blacklisted database. Third scenario, where the packets source IP is already listed in Blacklisted database. In these types of situations, the packets will be dropped and notified to the network admin. Using this way, we can prevent Application Layer based DDoS Attacks.

6. Conclusion

In this paper, initially we discuss about the DDoS attack and its effects. Then we have explored the famous DDoS attacks that has taken place till date. At this point we outline various types and strategies used by the attacker to create application layer and SDN based DDoS attack. In addition, we make an extensive survey on DDoS detection using various methods in application layer and software defined networking environment. We summaries all the algorithms in a single table with parameters used to detect, DDoS detection level and performance metrics used by those algorithms. At last, we investigate the real time problems created by attacker and try to prevent those problems with proposed architecture. The proposed architecture will avoid flow table overloading approach by flow table sharing method in SDN. In application layer, we detect the packet is genuine or not. If it is malicious and from attacker, then we will terminate those packets. These approaches will help us to resist the attacks.

Future Work

In spite of bottomless research in this area, there are still some problem that could not be solved till date. And many new problems occur in different scenarios that has to be addressed and provide solutions in future research. There is an urgent need to design a common framework, that can be suitable for detecting DDoS attack in all environments.

Acknowledgments

The authors would like to thank the anonymous reviewers and editors for their valuable comments and suggestions which has substantially improved the quality of the paper.

References

[1] B. B. Gupta, S. Jain and P. Agrawal, "Svm based scheme for predicting number of zombies in a ddos attack," Proceedings - 2011 European Intelligence and Security Informatics Conference, EISIC Oct 2011, pp. 178– 182, Oct 2011.

[2] S.-H. Kim, J.-H. Jun and H. Oh, "Ddos flooding attack detection through a step-by-step investigation," Proceedings of the 2nd IEEE International Conference on Networked Embedded Systems for Enterprise Applications, pp. 1–5, 12 2011.

[3] L. Jia, "The research on ddos attack based on botnet," Advances in FCCS, Springer, pp. 325–330, Jan 2012.

[4] T. Karnwal, T. Sivakumar, and G. Aghila, "A comber approach to protect cloud computing against xml ddos and http ddos attack," IEEE, pp. 1–5, March 2012.

[5] L. Capretz, M. Mahmoud and A. Ouda, , "Cloud-based ddos attacks and defenses," International Conference on Information Society, i-Society 2013, pp. 67–71, Jan 2013.

[6] K. V. Rao and K. M. Prasad, "Discriminating ddos attack traffic from flash crowd on internet threat monitor using entropy variation," African journal of computing and ICT, IEEE, pp. 53–62, June 2013.

[7] M. Rajarajan, S. Veluru, A. Healing and A. Olabelurin, "Entropy clus- tering approach for improving forecasting in ddos attacks," ICNSC 2015- 2015 IEEE 12th International Conference on Networking, Sensing and Control, 04 2015.

[8] Q. Yan, J. Li, F. R. Yu and Q. Gong, "Software-defined networking (sdn) and distributed denial of service (ddos) attacks in cloud computing environments: A survey, some research issues, and challenges," IEEE Communications Surveys Tutorials, vol. 18, pp. 602–622, Jan 2016.

[9] Rakshitha. M and Ashwini. B P, "A survey on detection and mitigation of zombie attacks in cloud environment," 2016, 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), Bangalore, pp. 764–769, Jan 2016.

[10] T. Gairola and K. Singh, "A review on dos and ddos attacks in cloud environment and security solutions," International Journal of Computer Science and Mobile Computing, vol. 5, pp. 136–141, July 2016.

[11] A. Sahi, D. Lai, Y. Li, and M. Diykh, "An efficient ddos tcp flood attack detection and prevention system in a cloud environment," IEEE Access, vol. 5, pp. 6036 – 6048, March 2017.

[12] Q. Wang, Z. Zhao, and H. Zhang, "Ddos defense mechanism based on software defined network," 9th IEEE International Conference on Com- munication Software and Networks, pp. 1122–1127, May 2017.

[13] V. Kansal and M. Dave, "Proactive ddos attack detection and isolation," 2017 International Conference on Computer, Communications and Elec- tronics, pp. 334–338, July 2017.

[14] D. Gautam and V. Tokekar, "An approach to analyze the impact of ddos attack on mobile cloud computing," IEEE, International Conference on information communication, Instumentation and control, pp. 1–6, Aug 2017.

[15] J. Jiao, Y. Benjun, Y. Zhao, R. Stones, G. Wang, X. Liu, S. Wang, and G. Xie, "Detecting tcp-based ddos attacks in baidu cloud computing data centers," IEEE 36th Symposium on Reliable Distributed System, pp. 256–258, Sept 2017.

[16] M. Haque, S. Ali, S. Tan, Z. Yusoff, C. Lee, I. Kaspin, and S. Ziri, "Mo- tivation of ddos attack-aware in software defined networking controller placement," International Conference on Computer and Applications, pp. 36–42, Sept 2017.

[17] D. Hyun, J. Kim, D. Hong, and J. Jeong, "Sdn-based network security functions for effective ddos attack mitigation," 2017 International Conference on Information and Communication Technology Convergence (ICTC), pp. 834–839, Oct 2017.

[18] L. Zhou and H. Guo, "Applying nfv/sdn in mitigating ddos attacks," IEEE Region 10 Conference (TENCON), Malaysia, pp. 2061–2066, Nov 2017.

[19] M. Myint Oo, S. Kamolphiwong, and T. Kamolphiwong, "The design of sdn based detection for distributed denial of service (ddos) attack," pp. 258–263, Nov 2017.

[20] C. Wang, T. Miu, X. Luo, and J. Wang, "Skyshield: A sketch-based defense system against application layer ddos attacks," IEEE Transactions on Information Forensics and Security, vol. 13, pp. 1–1, March 2018.

[21] Arivudainambi D, Varun K A, and S. Chakkaravarthy, "Lion ids: A meta-heuristics approach to detect ddos attacks against software-defined networks," Neural Computing and Applications, Springer, March 2018.

[22] K. Hong, Y. Kim, H. Choi, and J. Park, "Sdn-assisted slow http ddos attack defense method," IEEE Communications Letters, vol. PP, pp. 1–1, April 2018.

[23] K. Bhushan and B. B. Gupta, "Distributed denial of service (ddos) attack mitigation in software defined network (sdn)-based cloud computing en- vironment," Journal of Ambient Intelligence and Humanized Computing, Springer, vol. 10, April 2018.

[24] Y. Yu, L. Guo, Y. Liu, J. Zheng, and Y. Zong, "An efficient sdn-based ddos attack detection and rapid response platform in vehicular networks," IEEE Access, vol. 6, pp. 44 570–44 579, July 2018.

[25] T. V. Phan and M. Park, "Efficient distributed denial-of-service attack defense in sdn-based cloud," IEEE Access, vol. 7, pp. 18 701–18 714, Sept 2019.

[26] A. Sangodoyin, B. Modu, I. Awan, and J. Pagna Disso, "An approach to detecting distributed denial of service attacks in software defined networks," 2018 IEEE 6th

International Conference on Future Internet of Things and Cloud (FiCloud), pp. 436–443, Aug 2018.

[27] G. Jaideep and B. Battula, "Detection of spoofed and non-spoofed ddos attacks and discriminating them from flash crowds," EURASIP Journal on Information Security, Springer, vol. 2018, Dec 2018.

[28] H. Maziku, S. Shetty, and D. Nicol, "Security risk assessment for sdn- enabled smart grids, elsevier," Computer Communications, vol. 133, Dec 2018.

[29] A. Bhardwaj, A. Sharma, V. Mangat, K. Saluja, and R. Vig, "Experimental analysis of ddos attacks on openstack cloud platform," Lecture Notes in Networks and Systems, pp. 3–13, jan 2019.

[30] A. Serrano, Z. Pervez, Q. Wang, and J. Alcaraz-Calero, "Towards the detection of mobile ddos attacks in 5g multi-tenant networks," IEEE 2019 European Conference on Networks and Communications (EuCNC), pp. 273–277, june 2019.

[31] S. Dong, R. Jain, and K. Abbas, "A survey on distributed denial of service (ddos) attacks in sdn and cloud computing environments," IEEE Access, vol. PP, pp. 80 813–80 828, june 2019.

[32] A. Alsirhani, S. Sampalli, and P. Bodorik, "Ddos detection system: Using a set of classification algorithms controlled by fuzzy logic system in apache spark," IEEE Transactions on Network and Service Management, pp. 936– 949, July 2019.

Authors' Biographies

Sharan A S is currently pursuing master's at B.M.S College of Engineering, Banglore in Information Science department. I have received my bachelor's degree in Computer Science and Engineering in 2018. Got best paper award from international conference of AICDMB, Mysuru in 2020. My research interests lies in Artificial Intelligence, Machine learning, Image/Video Processing and Network Security.

Radhika K R is a professor in B.M.S College of Engineering. She has an experience of 23 years in teaching a wide area of subjects in Information Science Department at BMSCE. She has 40+ publications in various reputed journal. She is a senior member of IEEE. Her area of interests is network security, data mining, cloud security and Biometrics