IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 12, December 2021

DOI: 10.17148/IJARCCE.2021.101242

DDOS attack detection using machine learning in SDN

Rashmi Parikh, Prof. Pratik Modi

Dept. Of Computer Engineering, LDRP, Gandhinagar, Gujarat, India

ABSTRACT: Software program-described Networking (SDN) is a rising community Standard that has received significant traction from many researchers. Distributed Denial of provider (DDOS) assaults had been a real threat in lots of aspects of computer networks and disbursed applications. The main objective of a DDOS assault is to bring down the services of a target using a couple of sources which are disbursed there are numerous distributed denials of service (DDOS) attack techniques getting used to degrade the performance or availability of focused services at the net This paper presents different type of DDOS attack and Detection of DDOS attack using SDN

Keywords: Overview of SDN, DDOS Attack Type, Famous attack.

1. INTRODUCTION

As technology grow there is so many risk associate with the technology for example cyber security, leack of data, data corrupted etc. As we know cybercrime is one of the major problem now day so we have to ensure that our application or website are secure. To protect our application, software or website from authorized user is called cyber security, cyber security is process of technology which control process, protect process.

2. DISTRIBUTED DENIAL OF SERVICE

Now day there are several type of attacks among theme Distributed denial of service DDOS attack is most popular and most harmful attack DDOS Attack involves many online objects, known as botnet, which are used to cover targeted websites with fake traffic. There are so many reason like anger and criticism, Means to extract money, to disrupt operation of Private or Government Enterprise etc. behind the attack. The main of Attacker is to overwhelm them with more traffic than the server or network can accommodate. The first-ever DDOS attack was executed by David Dennis, a 13-year old student at the University of Illinois High School. [1]

2.1 Evolution of DDOS Attacks [2]

2.1.1 1996: the first known DDOS raid:

1996 attack targeting Panix with SYN flood, the oldest Internet Service Provider (ISP) in New York. This method exploits the TCP with SYN (synchronize) packets coming from a spoofed IP address.It took Panix roughly 36 hours to get back on track

2.1.2 2000: DDOS goes pro, hacktivism kicks in

Amazon, eBay, Yahoo!, Dell, CNN, and FIFA underwent a massive attack launched by Michael Calce, a Canadian teenager going by the online alias “Mafia boy.”

2.1.3 2007: DDOS becomes a threat to nation-states

This Attack is against government

2.1.4 2016: DDOS via IOT botnets makes its debut

2.1.5 2018: ransom DDOS comes into existence and perseveres

This relies on the User Datagram Protocol (UDP) communications that do not support authentication and can be easily exploited.

2.2 Famous DDOS attack [3]

2.2.1 February 2020 attack: AWS DDOS Attack

AWS reported that it reduced the major DDOS attacks by February 2020. At its peak, the attack saw incoming traffic at 2.3 terabits per second (Tbsp.). Responsible attackers have used Connection-less Lightweight Directory Access Protocol (CLDAP) web servers. CLDAP is a user identifier protocol. It is one of the LDAP, an older version of the protocol

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 12, December 2021

DOI: 10.17148/IJARCCE.2021.101242

2.2.2 February 2018: GitHub DDOS Attack

One of the biggest DDOS attacks record on GitHub. This attack was up to 1.3 Tbsp., sending packets at 126.9 million per second .The GitHub attack was a memcached DDOS attack, so there were no botnets involved. Instead attackers have exploited the amplifying effect of the popular data storage system known as memcached. With the influx of memcache servers with deceptive applications, attackers were able to increase their attacks by as much as 50,000x. GitHub used the DDOS security service to be automatically notified within 10 minutes of the attack.

2.2.3 October 2016: Dyn attack

This attacks were damaging too many major sites, including Airbnb, Netflix, PayPal, Visa, Amazon, New York Times, Reddit, and GitHub. This is done using a malware program called Mirai. Mirai creates botnet from obsolete Internet of Things (IoT) devices such as cameras, smart TVsTo create attack traffic, and these damaged devices are all designed to send applications to a single victim. Dyn was able to resolve the attack within one day

2.2.4 2015: GitHub attack

Attack traffic was created by injecting JavaScript code into the browsers of everyone who visited Baidu, China's most popular search engine. Some sites that used Baidu analytics tools also provided malicious code; this code enabled infected browsers to send HTTP requests to targeted GitHub pages. After the attack it was discovered that malicious code was not coming from Baidu, but was added to the arbitrator service.

2.3 Worldwide List Of DDOS Attacks

Table 1: DDOS Attacks [4]

Date of attack	Country	Industry	Downtime	Company Affected
July 27	UK	Media	-	Info security Magazine
July 23	Russia	Media	Few Hours	Vedomosti
July 16	Russia	Government	1 hr	Russian Defense Ministry
July 9	Ukraine	Government	-	Defense Ministry portal
July 8	Gibraltor	Gambling	30 Min	888 Sport
July 5	USA	Cryptocurrency	2 days	Bitcoin.org
July 1	Russia	Telecom	-	Rostelecom

3. SOFTWARE DEFINED NETWORKING

Software-Defined Networking simplifies network management by separating control logic (control plane) from the underlying hardware that forwards the traffic (data plane). With this decoupling of control plane and data plane, network switches become simple forwarding devices whereas control logic and functionality are implemented in logically centralized controller [5].

Software-Defined Networking (SDN) is an approach to networking that uses software-based controllers or application programming interfaces (APIs) to communicate with underlying hardware infrastructure and direct traffic on a network. SDN's origins can be traced to a research collaboration between Stanford University and the University of California at Berkeley that ultimately yielded the Open Flow protocol in the 2008 timeframe

3.1 Summary of popular SDN-based DDOS attack detection techniques

Table 2: DDOS Detection Technique [5]

Techniques	Description
Entropy	Entropy-based methods depend on network feature distributions to detect anomalous network activities. Probability distributions of various network features such as source IP address, destination IP address, and port numbers are

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 12, December 2021

DOI: 10.17148/IJARCCE.2021.101242

	used to calculate the entropy. Predefined thresholds on changes in the entropy values are used to identify the presence of anomolies
Machine learning	Machine learning-based methods employ techniques such as Bayesian networks, SOM, and fuzzy logic to identify the presence of anomolies. These algorithms takes into account various network features and traffic characteristics to detect the presence of anoamlies
Traffic pattern analysis	These techniques work on the assumptions that the infected hosts exhibit similar behavioral patterns which are different from benign hosts. Typically, in case of a botnet attack, infected machines (bots) are usually controlled by single bot master. Similar traffic patterns are observed as a result of command that is sent to many members of same botnet causing the similar behavior (e.g., sending illegitimate packets, starting to scan)
Connection rate	These techniques are classified into two types: 1) connection success ratio and 2) connection rate, where connection rate refers to the number of connections instantiated within a certain window of time
SNORT and Open Flow integrated	These technique use combination of intrusion detection system (such as SNORT) and OpenFlow to detect attacks and reconfigure the network dynamically. An intrusion detection system monitor the traffic to identify malicious activities. OpenFlow switches are then dynamically reconfigured based on the detected attacks in real time

3.2 SDN Architecture

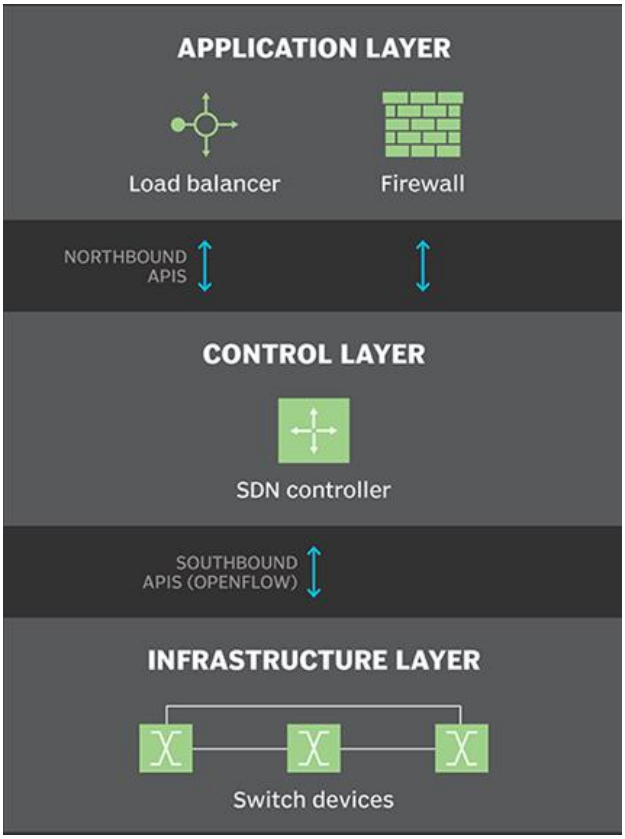

Fig 1. SDN Architecture [6]

\

The SDN Architecture has main three layer: The application layer, Control layer, infrastructure layer

Application Layer: Application layer contains standard network applications or functions used by organizations. This may include system access, upload, or firewalls. Where a normal network will use a special device, such as a firewall or loading balance, a software-defined network replaces an operating system with an application that uses a controller to control the flight behavior of the data.

Control Layer: The control layer represents software for the central SDN controller that acts as the brains of the

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 12, December 2021

DOI: 10.17148/IJARCCE.2021.101242

software defined by the software. This controller stays on the server and manages the policies and flow of traffic across the network.

Infrastructure layer: The infrastructure layer consists of portable switches on the network. These channels transmit network traffic to their locations.

3.2 Classification of DDOS attacks according to OSI layer:

Table 3: Classification of DDOS Attacks [7]

Network or Volume Centric Attack – 64%	
UDP Floods	DDOS flood attacks targeted by User Datagram Protocol (UDP) packets. The goal of the attack is to attack on random ports into a remote host. This causes the host to check several times that the application is listening in that hole
ICMP flood	ICMP floods cover the targeted application with ICMP Echo Request (ping) packets, usually sending packets very quickly without waiting for responses. This type of attack can consume both outgoing and incoming bandwidth
Application Layer Attack – 16 %	
HTTP Flood	**The** attacker uses HTTP GET or POST requests that appear to be legitimate to attack a web server or application. HTTP floods do not use the wrong packets, fraudulent or display strategies, and require less bandwidth than other attacks to slow down the targeted site or server. Attacks work best when it forces the server or application to provide the highest possible resources in response to each request.
Slowloris	Slowloris is a highly targeted attack, which allows one web server to slow down another server, without touching other resources or holes in the target network. Slowloris does this by holding as many connections to the targeted web server as open for as long as possible. It does this by creating a connection to the targeted server, but sending only partial request.
Protocol attack - 20%	
SYN flood	DDOS flood SYN attacks use known vulnerabilities to track TCP connections. In the case of SYN floods, the attacker sends multiple SYN requests, but may not respond to SYN-ACK host responses, or send SYN requests from fake IP. Address.
Ping of Death	Attack involves an attacker sending multiple malicious pings to a computer. The packet length of the IP packet (including header) is 65,535 bytes. The recipient ends up with an IP packet larger than 65,535 bytes when reconnected. This can overload the memory tubes stored in the package, resulting in rejection of the service in the official packaging.

4. LITERATURE REVIEW

Author	Title	DOI	Description
Bawany, Narmeen Zakaria; Shamsi, Jawwad A.; Salah, Khaled (2017).	DDOS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions	10.1007/s13369-017-2414-5	mitigation technique like block port, control bandwidth, Network reconfiguration and topology change, IP address change

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 10, Issue 12, December 2021
DOI: 10.17148/IJARCCE.2021.101242

Saman Taghavi Zargar, Member, IEEE, James Joshi, Member, IEEE, and David Tipper, Senior Member, IEEE	Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks	10.1109/SURV.2013.031413.00127	DEFENSE MECHANISMS AGAINST NETWORK/TRANSPORT-LEVEL DDOS FLOODING ATTACKS BASED ON THEIR DEPLOYMENT LOCATION
Reneilson Santos, Danilo Souza, Walter Santo , Admilson Ribeiro , Edward Moreno	Machine learning algorithms to detect DDoS attacks in SDN	10.1002/cpe.540	four different ML-Algorithms like MLP, SVM, Decision Tree, and Random Forest
Jian Yuan, Mills, K.	Monitoring the Macroscopic Effect of DDoS Flooding Attacks	10.1109/TDSC.2005.50	constant rate, increasing rate, natural-network-congestion-like, pulsing, TCP-targeted, and subgroup attacks
Ismael Amezcua Valdovinos , Jesús ArturoPérez-Díaz, Kim-Kwang RaymondChooc, Juan FelipeBoterod	Emerging DDoS attack detection and mitigation strategies in software-defined networks	10.1016/j.jnca.2021.103093	Detection and mitigation strategies. DoS: Block chain-based, NFV-based, Honey net-based, Network slicing-based, MTD-based

5. CONCLUSION

In this paper, we have discussed Type of DDOS attack, overview of SDN DDOS attack impact in our daily life, major cause of DDOS attack. DDOS attack is more harmful than other attack .DDOS attack is biggest threat nowadays. With the help of SDN we define which type of DDOS attack it is. The increased reliance on cyber physical systems and advancements in networking, we have to more focus on cybercrime

6. REFERENCES

[1] https://www.radware.com/security/ddos-knowledge-center/ddos-chronicles/ddos-attacks-history/
[2] https://www.embeddedcomputing.com/technology/security/network-security/the-history-and-evolution-of-ddos-attacks
[3] https://www.cloudflare.com/en-in/learning/ddos/famous-ddos-attacks/
[4] https://blog.mazebolt.com/list-of-ddos-attacks-july-2021
[5] Bawany, Narmeen Zakaria; Shamsi, Jawwad A.; Salah, Khaled (2017). DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions. Arabian Journal for Science and Engineering, 42(2), 425–441. doi:10.1007/s13369-017-2414-5
[6] https://www.techtarget.com/searchnetworking/definition/software-defined-networking-SDN
[7] https://www.imperva.com/learn/ddos/ddos-attacks/