Denial of Service and Distributed Denial of Service Attack on the IPV6: A Review

Shweta Paliwal
Research Scholar of Computer Science and Engineering, DIT University, Dehradun (State Private University through State Legislature Act No. 10 of 2013 of Uttarakhand and approved by UGC)

***Abstract*- With the Internet doubling in Size rapidly, the Internet Engineering Task Force has developed new and major web operators and service providers activate robust version of Internet Protocol IPV6.Today IPV6. Since every new technology has some point of vulnerabilities, so applied to IPV6. DOS and DDOS are among the severe security attacks on the internet today. Web servers using the HTTP protocol are more exposed to the DOS attack and its more advanced version DDOS. Data centers are becoming faster, larger hence becoming more difficult to protect. Therefore enhancing the security capabilities with machine learning is becoming necessary today in the field of networking.**

Index Terms- IPV6, IPSEC, DOS, DDOS, Machine Learning

1. INTRODUCTION

The roots of the Internet have evolved from ARPANET, which was initially used for connecting the military networks in the early 1980s.Since, then the internet has experienced an accelerated growth, which has automatically increased the need of Internet Protocol (IP) and IP Addresses. We have observed an amount of around 4.32 billion users of IPV6 in 2017 that are expected to be projected around 8.4 billion in the 2021 and hence the requirement of IP addresses becomes much larger. As the number of Wireless Ad-Hoc Networks, Home Area networks along with the normal users are increasing day by day. The present day 32 bit IPV4 can only support 4 billion network devices on the internet. Later on Internet Engineering Task Force (IETF) proposed a next generation Internet Protocol known as IPV6 [2].Presently the IPV6 protocol is supported by all Google services and an approximate of 22.96% percentage of Internet Users access Google using IPV6[3].According to the IOT Agenda, IPV6 address is a128 bit alphanumeric string which helps in the identification of end point devices in the IPV6 addressing scheme. It is divided into 8 groups consisting 16 bits in each group. IPV6 has been introduced with updated features such as Large Address Spacing, Simplified Header, Auto Configuration, Smooth Transitions and IPSEC. With the adoption of the IPV6, here come the new and advanced security challenges and more powerful volumetric DDOS and DOS attacks. The DDOS attacks were previously focused on network layer but with the advancement in web technology, the attackers find it easier to launch the attack using the application layer.

2. COMPARISON BETWEEN IPV4 AND IPV6

Premise of Comparison	IPV4	IPV6
Address Length	32 bit Address Length	128 bit Address Length
Address Representation	In decimals	In Hexadecimals
Address Configuration	Provide support to Manual and DHCP	Provide support to Auto Configuration and Renumbering
Fragmentation	Router to Fragment	End to end
Header Length	20 Bytes	40 Bytes
Checksum Field	Available	Not Available
Message Transmission	Broadcasting	Multicast and Anycast
Security	Depends on Application	IPSEC is embedded within IPv6

Fig.1: Comparison between IPV4 and IPV6

3. IPSEC (IP SECURITY): AN INBUILT FEATURE IN IPV6

In today's world of Internet, verifying information over the system is a hard and complicated issue. While the risk of information modification and information interference is rising, the objective of network security is to provide confidentiality, integrity and authentication. With the recent development of the security tools so many protocols and powerful tools have been proposed but the most famous secure and widely deployed is IPSEC [9].According to Cisco, IPSEC is a framework of open standards that provides confidentiality, integrity and authentication of data between participating peers [10].IPSEC is used to protect the tunnels against false data traffic and provides encryption to the packets against unwanted active and passive intruders. The segment technologies implemented in IPSEC includes encryption algorithms as DES (Data Encryption Standards) and 3-DES for encrypting the data packets, CBC (Cipher Block Chaining) for generating an initiation vector to start the encryption.

3.1 COMPARISON BETWEEN SSL AND IPSEC:

Basis of Comparison	SSL	IPSEC
Installation	Included in the web browsers	Requires client software for installation
Network Layer	Operates at socket layer(transport)	Operates at Network Layer
Design	Simple and well-designed protocol	Complex in design
Security Layer	Implemented at application layer so that browser traffic can be encrypted	Implemented at IP layer so all traffic is encrypted.
Gateway location	Gateways are deployed behind the firewall	Gateways are usually implemented on the firewall
Security Concerns	Client Authentication is often not used	Both the client and server are authenticated
Endpoints	Requires host based clients	Browser based
Encryption	Moderate to Strong	Strong
Authentication	One way or Two Way	2 way using digital certificates
Connecting options	Any device can connect	Only specific devices
Encryption key length	40bits-256 bits	56 bits to 256 bits
IP Header Authentication	No	Yes
Applications	Web enabled Applications	All IP Based Devices

Fig. 2: Comparison between IPSEC and SSL

3.2 IPSEC AUTHENTICATION HEADER (AH): IPSEC consists of two security protocols namely IPSEC- AH and IPSEC-ESP. IPSEC-AH authenticates the origin of the IP datagrams and provides connectionless and anti-replay integrity. It provides integrity of data using checksum which is generated by an Authentication Code similar to MD5.There exist a shared secret key in the algorithm which is used for data origin authentication. In transport mode, the IP header of a datagram is the outermost IP header, followed by the AH header and the datagram .The "Next Header" is a field of 8 bits which identifies the type of the transport layer used in the upper layer. The value of this field is chosen from the set of IP Protocol numbers that are defined by the Internet Assigned Number Authority (IANA). The "Payload Length "isan 8 bit field and specifies the Length of the AH in 32 bit words by not including the first 8 octets or 2 units of first 4 octet. The "Reserved" is a 16 bit field reserved for future purpose and is always initialized to zero for transmission. "Security Parameter Index" (SPI) is a 32 bit field which is used in combination with destination IP address and security protocol to identify the security association of a datagram(packet)."Sequence Number" is a counter value, which increases uniformly and has a bit size of 32 bits. "Authentication Data" is a field with variable length that contains the Integrity Check Value (ICV) for the packet

4. IPSEC ENCAPSULATING SECURITY PAYLOAD

Encapsulating Security Payload is primarily designed to provide Authentication, Encryption and protection services to the payload that is being transferred over the IP Network. ESP does not provide support to the Header, but during the Tunnel mode if the packet is

encapsulated within a packet it can encrypt the entire packet

5. SECURITY CONCERNS WITH IPV6:

IPV6 approach to security is marginally better than IPV4 as it provides Larger Address Spaces and IPSEC but continues to be vulnerable. Not using IPSEC exposes a network to both old IP attacks as well as IPV6 specific feature based attacks. During the transition from IPV4 to IPV6 both the networks are likely to coexist, hence IPV6 networks too can face Dual Stack, Header Manipulation and Flooding issues. Figure 4 depicting Point of security concerns in IPV6 and Major IPV6 attacks.

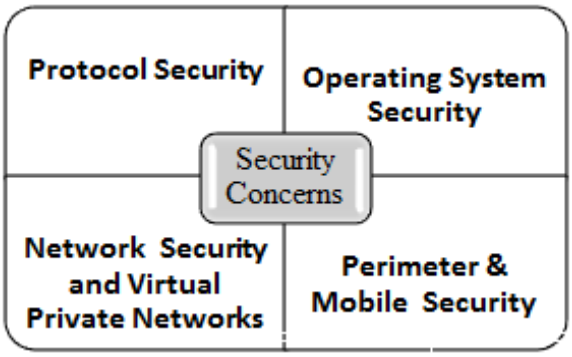

Fig. 3: Security Concerns with IPV6

6. ATTACKS ON IPV6 NETWORKS

There are certain issues that are emerging as the hacking community has already targeted the IPV6 Networks. These are as follows:

- Reconnaissance and Scanning Worms
- Attacks against Internet Control Message Protocol(ICMP) for IPV6
- Auto configuration and extension Header Attacks.
- Attacks on Dual Stack Implementation during migration from IPV4 to IPV6
- Mobile IPV6 Attacks

6.1 RECONNAISSANCE ATTACK:

Here the Intruder engages with the information system to gain information about the point of Vulnerabilities. The attacker often uses Host Probing and port scanning to discover the vulnerable ports. The attacker may also identify the hosts connected to the network and can use port scanning to detect the open ports.IPV6 multiple address structure allows the attacker to identify group of routers or DHCP servers over a network , hence providing an opportunity to scan for these devices open ports.

6.2 AUTO CONFIGURATION ATTACKS:

Auto Configuration is a feature of IPV6 that allows a node to automatically generates and address for each of its network interfaces. Node can configure addresses either through the stateful or stateless auto configurations.ICMPV6 messages sometimes open up the door for attacks including Flooding and Denial of Service when not secured with IPSEC. In a DOS Attack the attacker makes an organizations network services unavailable to its legitimate users. It is implemented on an IPV6 network by exploiting vulnerabilities in DAD Procedure. In DAD the node sends a neighbor solicitation (NS) packet with its tentative IP Address inside the packet waits to seek a response from any node with new generated address, if there is no reply to the message, then the node with new generated address assumes it to be unique and use it

6.3 MAN IN THE MIDDLE ATTACK:

When a node A requires the MAC address of another node B, it sends an NS message to the all-nodes multicast address. An attacker on the same link when see the NS message replies to it with the corresponding NA message, thereby taking over the intended traffic flow between A and B.

7. POTENTIAL ATTACKS OCCURRING IN IPV6

IPV6 has been launched with certain features, which includes Auto Configuration, Large Space Addresses and the extension headers. These features at the same time has given rise to certain points of vulnerabilities as now all hosts are capable to process the routing headers and end to end connection may lead to the misuse of ICMPv6.

8. DENIAL OF SERVICE ATTACK (DOS)

Every new technology when released has some point of vulnerabilities, so with the next generation IP Protocol. DOS is a major security threat to IPV6. It is a situation where the intruder prevents the legitimate users from accessing certain computer system, devices and other IT resources which results in

flooding of servers and networks with the traffic that overwhelms the victim's resources thus making it difficult for the users to access them

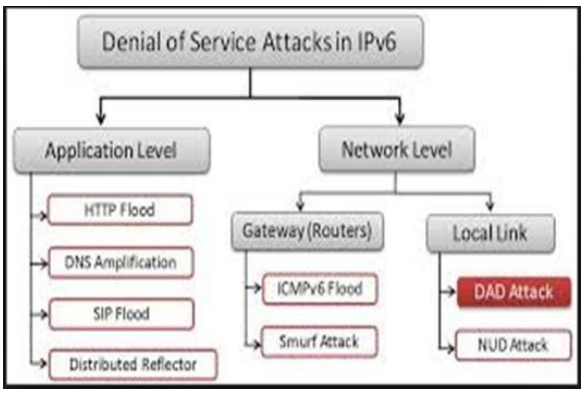

Fig. 4: Types of DOS Attack

Studies have shown that during the process of auto configuration of IPV6 link local network, ICMPv6 messages are more vulnerable to the security attacks, especially during the Duplicate Address Detection Process. The attacker performs fabrication of the ICMpv6 messages and thereafter exploits these messages in order to perform the DOS Attack. Flooding the servers or crashing the servers is two general methods through which DOS can be initiated. Figure5 describes the type of DOS attacks that occurs over the network.

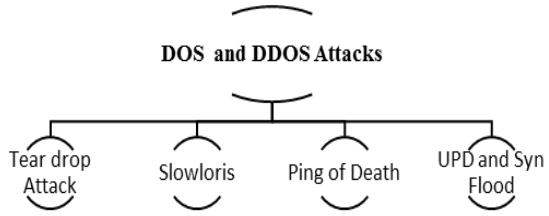

Fig.5: DOS and DDOS Attacks

9. DISTRIBUTED DENIAL OF SERVICE ATTACK (DDOS)

DDOS is a coordinated attack on the services of single or multiple systems through many compromised secondary victims. It attempts to disrupt the normal traffic of a target sever by over flooding the target or surrounded infrastructure with the Internet traffic. The DDOS attack normally requires an intruder to gain control of online machines inorder to carry out an attack. The systems are infected with Malware converting them to Bot and hence gains the control over these groups of bots which is also known as a botnet. The intruder is able to direct the machines by sending updated instructions to each bot using the remote access. DDOS attacks are classified into bandwidth depletion attack and resource depletion attack. In bandwidth depletion, attack large traffic is used by the attacker to flood the victim thus preventing the legitimate traffic and amplifying the attack by sending messages to broadcast IP addresses. In a resource depletion attack the attackers attempt to tie up the critical resources making the victim unable to process the service. DDOS attacks launched at the application layer requires lower bandwidth to prevent the legitimate users from accessing web servers. Studies have classified the DDOS attacks on application layer into the following categories. The table below shows some of the prominent DDOS attacks at the application layer [16].

Name of the attack	Layer of OSI Model	Description
HTTP Flood Attack	Application Layer	Targeted server is overwhelmed with HTTP requests and operates in 2 varieties namely HTTP Get and HTTP Post
Fragmented HTTP Flood	Application Layer	Here BOT with a valid IP establishes a HTTP connection with the web server and the packet are spit by bot into tiny fragments and is sent over slowly keeping the action active for a long time.
SYN-ACK Flood	Application Layer	The listening host generates an ACK packet to acknowledge an incoming SYN packet and the attack exhausts the server resources.
Spoofed Session Flood	Application Layer	This sort of attack bypasses the defense mechanism that monitors the incoming traffic on the network
Session Attack	Application Layer	The attack uses IP addresses of the BOTS to bypass the defense mechanism

Fig. 8: DDOS Attacks

10. WORLD FAMOUS DDOS ATTACKS

According to Cloud fare, the biggest DDOS attack took place in February 2018. The attack was targeted on one of the popular coding management platform, Github. The incoming traffic was sent at a speed of 1.3 terabytes per second and sending packets rate was 126.9 million per second. Luckily DDOS prevention was used by github which alerted them 10 minutes

prior of the starting of the attack. Some of the other famous attacks were as follows:

- 2016 DYN Attack: DYN ,a major DNS provider suffered from the DDOS attack in October 2016.The attack was carried out with the help of malware who created a botnet out of the IOT devices. The attack created disruption for AirBnB, Netflix, PayPal, Visa, Amazon, The New York Times, Reddit, and GitHub.
- 2013 Spamhaus Attack: Spamhaus is responsible for combatting the spam emails. The rate of the traffic was about 300gbps.
- 2007 Estonia Attack: The DDOS attack was targeted on the government services, financial institutions and media outlets of Estonia.

11. APPLICATION OF MACHINE LEARNING TO AVOID SECURITY ATTACKS IN IPV6

Machine Learning has emerged as an application of Artificial intelligence that provides the system an ability to learn automatically and improves from the experiences without being programmed explicitly without human intervention. In the field of networking machine learning has provided improved security services and analytics. Several tools equipped with machine learning have provided better traffic management with longer range capacity planning. In real time, analyzing massive amounts of network data has created a need of improved network analytic tools. Machine learning is based on algorithms that detect anomalies on the network, correlates baseline performance, matches patterns of behavior. Machine learning has also improved the threats analytic space as well as DDOS attack, and remediation. Technological advances in networking as if Software Defined Networking has promoted the applications of ML in networking. Machine learning techniques used for threat detection are classification, anomaly detection and risk scoring. Below points provides the DDOS detection techniques developed using ML.

- The DDOS attacks can be detected with the help of neural classifiers which is one of the machine learning technique.Support Vector Machine (SVM) and Principal Component Analysis helped in detecting Router based flooding attacks in IPV6
- If we talk about the network discovery protocol of IPV6,using Decision tree and Random Forest Algorithm of Machine Learning a model based on Flow representation have been developed that detects the NDP-DDOS Attacks.
- The use of Artificial Neural Networks (ANNs) for misuse detection has been one of the most analyzed data mining approaches for Network Intrusion detection System (NIDS).
- Apart from this, DAD match technique relies on strong cryptographic hash function that will hide the tentative IP Addresses which help to secure DAD protocol of IPV6
- A Hadoop based framework has been developed to detect the high-level DDOS attacks at the application and network layer. The detection phase begins by capturing the server where the incoming traffic occurs and is transferred over the detection server for processing. The detection calculates the traffic to detect an attack if the threshold values increases [18].
- Another approach based on machine learning was designed to detect HTTPs DDOS attack by distinguishing the botnet from the authorized users in detecting attack traffic.
- A machine learning approach with the bio inspired bat algorithm was developed to allow fast and early detection of DDOS attack. They include time intervals instead of user sessions to develop the detection algorithm. The time interval uses machine learning matrix by assigning a value to the maximum sessions for one time interval and number of session in one time interval are computed to detect DDOS at the application layer [21].

12. FUTURE WORK AND CONCLUSION

The approach of Machine learning is used to identify how a normal looks like and what are the possible anomalies within a network. It helps in analyzing the information, identifying the patterns. Machine learning in the field of security means processing of massive amount of security data and distilling it into something more readable for security teams. Researches are more focused on DDOS at application layer The challenges need to be identified for DOS and DDOS attacks on network and emphasis must be

on to produce a significant approach for the prediction and detection purpose using Machine Learning and how to use ML correctly and draw the right conclusion from it. Machine learning has brought several significant security trends with predictive analytics to ensure security. Machine Learning has set off its journey into the field of networking, what comes next will be worth watching

REFERENCES:

[1] Udeagha, C., Martin, R., Peck, D., Youton, A., Marshall, A., & Clarke, J. (2018, April). Migrating from IPV4 to IPV6 in Jamaica. In SoutheastCon 2018 (pp. 1-8). IEEE.

[2] Siddika, F., Hossen, M. A., & Saha, S. (2017, January). Transition from IPv4 to IPv6 in Bangladesh: The competent and enhanced way to follow. In 2017 International Conference on Networking, Systems and Security (NSysS) (pp. 174-179). IEEE.

[3] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., & Carney, M. (2003). Dynamic host configuration protocol for IPv6 (DHCPv6) (No. RFC 3315).

[4] Alshamsi, A., & Saito, T. (2005, March). A technical comparison of IPSec and SSL. In 19th International Conference on Advanced Information Networking and Applications (AINA'05) Volume 1 (AINA papers) (Vol. 2, pp. 395-398). IEEE.

[5] Rescorla, E. (2001). SSL and TLS: designing and building secure systems (Vol. 1). Reading: Addison-Wesley.

[6] Alshamsi, A., & Saito, T. (2005, March). A technical comparison of IPSec and SSL. In 19th International Conference on Advanced Information Networking and Applications (AINA'05) Volume 1 (AINA papers) (Vol. 2, pp. 395-398). IEEE.

[7] Atkinson, R. (1998). IP Authentication Header. IETF RFC 2402, November.

[8] Elkeelany, O., Matalgah, M. M., Sheikh, K. P., Thaker, M., Chaudhry, G., Medhi, D., & Qaddour, J. (2002). Performance analysis of IPSec protocol: encryption and authentication. In 2002 IEEE International Conference on Communications. Conference Proceedings. ICC 2002 (Cat. No. 02CH37333)(Vol. 2, pp. 1164-1168). IEEE

[9] Wu, P., Cui, Y., Wu, J., Liu, J., & Metz, C. (2013). Transition from IPv4 to IPv6: A state-of-the-art survey. IEEE Communications Surveys & Tutorials, 15(3), 1407-1424.

[10] Soumyalatha, N., Ambhati, R. K., & Kounte, M. R. (2013). IPv6-Based Network Performance Metrics Using Active Measurements. In Proceedings of International Conference on VLSI, Communication, Advanced Devices, Signals & Systems and Networking (VCASAN-2013) (pp. 451-460). Springer, India.

[11] Caicedo, C. E., Joshi, J. B., & Tuladhar, S. R. (2009). IPv6 security challenges. Computer, 42(2), 36-42

[12] Anbar, M., Abdullah, R., Al-Tamimi, B. N., & Hussain, A. (2018). A machine learning approach to detect router advertisement flooding attacks in next-generation IPv6 networks. Cognitive Computation, 10(2), 201-214.

[13] Alsadhan, A. A., Hussain, A., & Alani, M. M. (2018, September). Detecting NDP Distributed Denial of Service Attacks Using Machine Learning Algorithm Based on Flow-Based Representation. In 2018 11th International Conference on Developments in eSystems Engineering (DeSE) (pp. 134-140). IEEE.

[14] Jaafar, G. A., Abdullah, S. M., & Ismail, S. (2019). Review of Recent Detection Methods for HTTP DDoS Attack. Journal of Computer Networks and Communications, 2019.

[15] Hameed, S., & Ali, U. (2018). HADEC: hadoop-based live DDoS detection framework. EURASIP Journal on Information Security, 2018(1), 11.

[16] Singh, K., Singh, P., & Kumar, K. (2018). User behavior analytics-based classification of application layer HTTP-GET flood attacks. Journal of Network and Computer Applications, 112, 97-114.

[17] Beitollahi, H., & Deconinck, G. (2012). Analyzing well-known countermeasures against distributed denial of service attacks. Computer Communications, 35(11), 1312-1332.

[18] Sreeram, I., & Vuppala, V. P. K. (2017). HTTP flood attack detection in application layer using machine learning metrics and bio inspired bat algorithm. Applied computing and informatics.

[19] Sabhnani, M., & Serpen, G. (2003, June). Application of Machine Learning Algorithms to KDD Intrusion Detection Dataset within Misuse Detection Context. In MLMTA (pp. 209-215).

[20] Mukkamala, S., Janoski, G., & Sung, A. (2002). Intrusion detection using neural networks and support vector machines. In Proceedings of the 2002 International Joint Conference on Neural Networks. IJCNN'02 (Cat. No. 02CH37290) (Vol. 2, pp. 1702-1707). IEEE.