An Analytical Review of DDOS Attack in IPV6

Shubham[1], Vishal Bharti[2]

[1] *Masters of Engineering Honours, Information Security, Chandigarh University*

[2] *Prof. and Head of Department, Deptt. Of CSE, Apex Institute of Technology, Chandigarh University*

Abstract **-** The massive growth of the Internet has demonstrated its value to businesses, government, professionals, academics and individuals over the last decade. Industry now relies on a range of benefits from Internet technology and has seen significant productivity gains.IPV6 is considered as a novel version of internet protocol, which is being developed for providing novel services and for supporting the internet growth. The security is the key challenge in the mobile IPv6. This review has reviewed the DDoS attack in IPv6. DDoS is distributed denial of service attack which is considered as a rapidly growing issue.

Keywords **-** IPV6, DDoS, Network, Security

I. INTRODUCTION

The Internet Protocol (IP) is basically a method or protocol by which information is directed from a distinct computer to another over the Internet. Every computer over the internet is known as a host and possesses at least one IP address which helps to identify it uniquely from other computers over the Internet. Internet Protocol mainly designates the technical presentation of packets and the addressing strategy for computers to interconnect over the internet [1]. When you send or retrieve an e-mail or a Web page, the message gets separated into tiny blocks termed as packets. Each packet contains IP address of both the sender and the receiver. A packet is first directed to a gateway computer that comprehends a trivial fragment of the Internet. The gateway computer interprets the target address and redirects the packet to a neighbouring gateway that sequentially interprets the target address and so on; over the Internet till one gateway distinguishes that the packet belongs to a computer within its vicinity or domain. That gateway then passes on the packet immediately to the computer whose address is stated [2].

Most of the networks integrate IP with a higher-level protocol called as Transmission Control Protocol (TCP), which build a simulated connection between a target and origin [3]. IP lets a sender to remit a package and relinquish it within the system, but then again there's not any direct connection between the sender and the recipient. On the other hand, TCP/IP creates a connection among the two host computers and enables to send messages backward and forward over an interval of time.

An IP address is normally the binary numbers yet, can be stored as a text for users. For instance, a 32-bit numeric address (IPv4) is generally inscribed in decimal as four numbers parted by periods. Each number inscribed within the decimals ranges from 0 to 255, such as 218.1.192.16 could be an IP address of an individual computer over the internet [4]. IP is considered as a connection less protocol, i.e. there is no ongoing connection between the endpoints that are communicating with each other over the network. Every packet that crosses over the Internet is rendered as an individual block of information lacking connection to every other block of data. Within the Open Systems Interconnection (OSI) communication model, IP is in layer 3 i.e. the Networking Layer.

1.1 IPv6

Internet Protocol version 6 in short IPv6 is the latest amendment of the Internet Protocol (IP) and the foremost version of the protocol that has been extensively used. It is frequently interpreted as an assortment of designations that are generated by the Internet Engineering Task Force (IETF) as a solution towards the exhaustion of IPv4 [5]. The fundamentals of IPv6 are comparable to those of IPv4. IPv6 incorporates the strengths of IPv4 and each server that carry IPv6 packets can also carry IPv4 packets. Things can adopt IPv6 as the origination and target addresses to transfer packets across the network, and the tools such as ping work for network testing as they do in IPv4, along with some petty modifications.

The success that IPv6 held over IPv4 is that in IPv6, the IP addresses are extended from 32 bits to 128 bits. IPv6 further sponsors auto-configuration, that helps in fixing the utmost shortcomings in version 4 (IPv4), and it has unified security and versatility attributes [6].

The following are the significant circumstances that have performed a major role in the origination of IPv6:

(i) The Internet has evolved rapidly and the space provided by IPv4 for the address is immersing. There is an extreme necessity to develop a protocol that can fulfil the obligations of future Internet addresses which is suspected to rise in an unpredicted form.

(ii) IPv4 does not implement any security feature itself. Data must be encrypted by another security application before broadcasting it over the Internet.

(iii) In IPv4, the prioritization of the information is not up to date. Although IPv4 reserved some bits for Type of Service or Quality of Service, yet IPv4 does not render enough functionality.

(iv) IPv4 requires an address configuration mechanism as it lacks a mechanism that configures a device to possess a globally unique IP address.

1.2 Advantages OF IPV6

IPv6 is a short form used to refer Internet Protocol version 6, which is basically a renewed protocol for the Intrusion Detection systems employed to distinguish computers over the network routing traffic across the Internet [7]. With the introduction of IPv6, almost everything from small devices to vehicles can be connected with other objects on the internet. But, an exaggerated extent of IT addresses is not the exclusive benefit of IPv6 over the IPv4. There are some valid reasons to make certain that your hardware, software, and services must support IPv6 [8].

(i) More Efficient Routing - IPv6 has lessened the extent of routing tables and forms routing more effective and hierarchical. IPv6 permits ISPs to accumulates all their customer's network prefixes within a particular prefix and proclaim that prefix to the IPv6 Internet. Furthermore, in IPv6, disintegration is managed by the source device by adopting a protocol for finding the maximum transmission unit (MTU) of the path.

(ii) More Efficient Packet Processing - The simplified packet header of IPv6 proffers more effective packet processing. IPv6 contains no IP-level checksum in comparison to IPv4, therefore, the checksum does not require to be calculated again at each router hop. As most of the link-layer technologies already hold checksum and failure-control skills, due to which dropping the IP-level checksum becomes feasible. Furthermore, most of the transport layers that manage endways connectivity possesses a checksum which allows detection of errors.

(iii) Directed Data Flows - IPv6 advocates multicast which provides bandwidth-intensive packet streams to be forwarded simultaneously over several targets, preserving network bandwidth. Additionally, the IPv6 header possesses a different field, designated as Flow Label that identifies the packets belonging to the corresponding flow.

(iv) Simplified Network Configuration - IPv6 also incorporates address auto-configuration, i.e. the address assignment. A router will forward the prefix of the local connection in its router broadcasts. A host can create its individual and unique IP address by affixing its link-layer (MAC) address, transformed into Extended Universal Identifier (EUI) 64-bit composition, to 64 bits local connection prefix.

(v) Support for New Services - At the IP layer, a reliable end-to-end connectivity is revived by removing Network Address Translation (NAT), facilitating innovative and valuable services. It is easier to generate and maintain the peer-to-peer networks and the services like VoIP and QoS seems more resilient.

(vi) Security - Internet Protocol Security (IPSec) in IPv6 renders confidentiality, authentication and data integrity. ICMPv4 packets are frequently barred by corporate firewalls due to their tendency to bear malware. But, Internet Control Message Protocol for IPv6, (ICMPv6) packets may be authorized because IPSec can be implemented to the ICMPv6 packets.

Table: 1 Comparison between Advantages of IPv6 and IPv4

Feature	IPv6	IPv4
Easier management of networks	IPv6 systems give auto configuration abilities. They are less complex, compliment and manageable, particularly for extensive establishments.	Networks must be arranged physically or with DHCP. IPv4 had numerous overlays to deal with web development, which request expanding support endeavors.
End-to-end connective Integrity	Direct addressing is conceivable because of huge address space - the requirement for arrange address interpretation gadgets is adequately disposed of.	Across the board utilization of NAT devices implies that a solitary NAT address can cover a large number of non-routable locations, making end-to-end trustworthiness unachievable
Unconstrained address abundance	3.4 x 10^{38} = 340 trillion addresses – around 670 quadrillion addresses for every square millimeter of the Earth's surface.	4.29 x 10^{9} = 4.2 billion locations – far not exactly even a solitary IP address for every individual on the planet.
Platform for innovation and collaboration	Given the number of addresses, versatility and adaptability of IPv6, its potential for activating development and helping joint effort is unbounded.	IPv4 was composed a transport and interchanges medium, and progressively any work on IPv4 is to discover courses around the limitations.
Integrated interoperability and mobility	IPv6 gives interoperability and versatility abilities which are as of now generally implanted in arrange gadgets.	Generally compelled network topologies confine portability and interoperability capacities in the IPv4 Internet.
Improved security features	IPSEC is incorporated with the IPv6 convention, usable with a reasonable key framework.	Security is reliant on applications – Ipv4 was not planned in view of security.

1.3 Disadvantages of IPv6

Although, IPv6 bears a number of benefits and is acknowledged as a most beneficial upgrade to the current Internet, yet there are numerous drawbacks behind this up gradation [9]. Some of the major drawbacks are briefly defined as follows:

(i) Memorizing Addresses - However, most people connect to IP addresses via domain names, more than few people yet connect to addresses via the IP address itself. Connecting without a domain name permits individuals to evade the cost of registering a domain, and it could aid a network remain concealed. IPv6 address are considerably lengthier and encompasses letters along with numbers, so they're far more difficult to memorize.

(ii) More Internet Traffic - Even though IPv6 addresses consumes little space in contrast to the websites and media, it still takes time to request an address from a domain name server. Furthermore, several pages count on peripheral websites, and drawing up these IP addresses take more bandwidth as well. Users might correspondingly run into problems, as writing an IPv6 address consumes quite longer time than writing an IPv4 address, and it's easy to make an error while doing so.

(iii) Cost of the Upgrade - Numerous older networking devices weren't intended for ipv6 implementation, and businesses and other establishments will require to upgrade so as to connect via IPv6 addresses. For units that upgrade networking hardware frequently, there might be not any added cost, but minor businesses that depend on older but consistent software might require to make an expensive upgrade. The hardware cost isn't the alone factor, as various businesses require to bring in advisors to make an upgrade.

(iv) Local Networking Variations - Local networking management frequently comprises handing over particular IP addresses to particular devices, and physically assigning IPv6 addresses can be problematic. Several local networks will continue to depend on IPv4 addressing for inner use, but then again this could lead to misperception. In all, local networking is expected to be a bit more complex when accounting for IPv6.

(v) Dual IP Schemes - Other misperception is expected throughout the conversion from IPv4 to IPv6. Providing that a substantial number of internet service providers and other establishments fail to completely support IPv6, backwards compatibility will be necessary, and juggling between two different protocols can be difficult. Projections of when IPv4 support won't be necessary vary, but experts agree it will be a long transition.

Table: 2 Comparison between disadvantages of IPv4 and IPv6

Subject	IPv6	IPv4
Memorizing Addresses	IPv6 address are considerably lengthier and encompasses letters along with numbers, so they're far more difficult to memorize.	Its easy to memorize the ranges of IPv4. But understanding the high bit order and the calculation give more perspective to it, and makes it even more easier to remember because you now know how to calculate the ranges.
Internet Traffic	IPv6 addresses consumes little space in contrast to the websites and media, it still takes time to request an address from a domain name server. Furthermore, several pages count on peripheral websites, and drawing up these IP addresses take more bandwidth as well.	There are limited number of addresses that’s why internet traffic should be low.
Hardware Cost	For units that upgrade networking hardware frequently, there might be not any added cost, but minor businesses that depend on older but consistent software might require to make an expensive upgrade.	Currently using hardware’s are IPv4 supporting. So there should not be any hardware cost to implement.
Local Networking Variations	Local networking management frequently comprises handing over particular IP addresses to particular devices, and physically assigning IPv6 addresses can be problematic.	Normally there are IPv4 addresses are used in all hardware devices.
Dual IP Schemes	Misperception is expected throughout the conversion from IPv4 to IPv6. Providing that a substantial number of internet service providers and other establishments fail to completely support IPv6	Most of the internet service providers are using IPv4 compatible hardware and providing support to IPv4 only.

II. DENIAL OF SERVICE

A Denial-of-Service attack (DoaS attack) is a cyber-attack where the perpetrator tries to make an appliance or system ability inaccessible to its prearranged clients by concisely or uncertainly upsetting services of a host associated with the Internet. Denial of service is normally practiced by flooding the focused on appliance or asset with worthless demands trying to over-burden frameworks and keep a few or every single authentic demand from being satisfied. In a circulated denial-of-service attack (DDoS attack), the forthcoming movement flooding the subject begins from various sources. This adequately makes it difficult to stop the attack just by obstructing a solitary source.

A DoS or DDoS attack is practically equivalent to a gathering of individuals swarming the section entrance or door to a shop or business, and not giving true blue assemblies a chance to go into the shop or business, disturbing typical activities. Criminal perpetrators of DoS attacks often target destinations or services facilitated on prominent web servers, for example, banks or charge card installment portals. Retaliation, extortion and activism can inspire these attacks.

The disparities amongst DoS and DDoS are substantive and significant. In a DoS assault, a perpetrator utilizes a solitary Internet association with either misuse a product ineffectiveness or surge an objective with counterfeit solicitations—more often than not trying to debilitate server assets (e.g., RAM and CPU). Then again, disseminated disavowal of administration (DDoS) assaults are boosted from numerous associated gadgets that are circulated over the Internet. These multi-individual, multi-gadget blasts are by and large harder to avoid, for the most part because of the sheer volume of gadgets included. Dissimilar to single-source DoS assaults, DDoS strikes tend to focus on the system foundation trying to immerse it with gigantic volumes of activity.

DDoS assaults additionally contrast in the way of their execution. Comprehensively, DoS assaults are propelled utilizing homebrewed contents or DoS contraptions while DDoS assaults are propelled from botnets — extensive bunches of associated gadgets tainted with malware that permits remote control by a provoker.

DoS assaults are propelled by people, organizations and even country expresses, each with their own specific inspiration:

- **Hacktivism** – Hacktivists utilize DoS stabbings as a way to express their feedback of everything from governments and legislators, including "huge business" and contemporary circumstances. In the event that they can't help contradicting you, your site will go down (a.k.a., "tango down").

Less actually judicious than different sorts of aggressors, hactivists tend to utilize premade devices to wage ambushes against their objectives. Unknown is maybe extraordinary compared to other known hacktivist gatherings. They're in charge of the cyber attack in February 2015 against ISIS, following the last's psychological militant assault against the Paris workplaces of Charlie Hebdo, and also the assault against the Brazilian government and World Cup supports in June 2014.

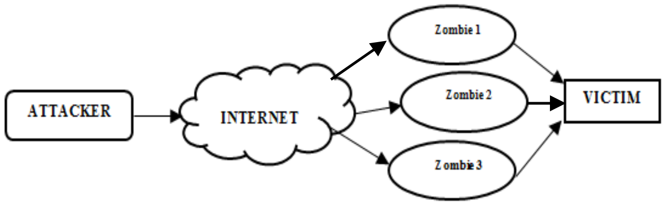

Figure 1: DoS attack Components

III. DISTRIBUTED-DENIAL OF SERVICE (DDOS)

A distributed denial-of-service or simply acknowledged as DDoS is an attack scenario where several computer systems gets compromised and attack a target, for example, a server, website or other resources of the network, and eventually induce a denial of service for the users of the resource that are being targeted [10]. The overwhelming quantity of incoming messages, link requests or abnormal packets to the destination system subdues it to hold back or even crash and power failure, thereby refusing service to authentic users or systems. A number of hackers use DDoS attacks to organized crime rings and government agencies. Certain circumstances associated with inadequate coding, missing pieces or unpredictable systems can even lead the genuine requests towards the destination systems to same results as in DDoS attacks [11]. The following steps are distributed attacks.

- The real attacker will "execute" the message to the controlling host program.
- The program that controls the host then receives the "execute" message and propagates the command to attack the daemon under its control.
- When the attack command is received, the agent machine begins to attack the victim.

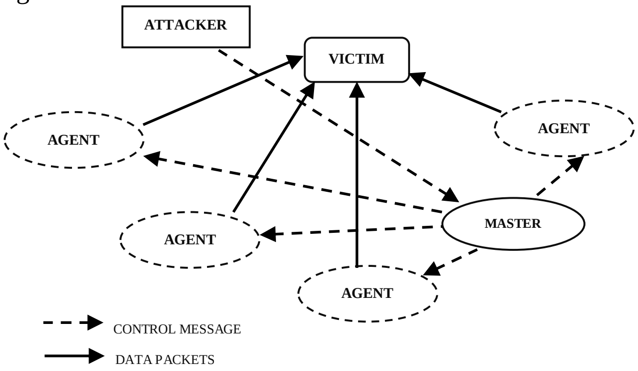

Figure 2: DDoS attack components

An attacker communicates with all of its DDoS agents before a real attacker reaches the victim. Therefore, the control channel must be present between the proxy and attacker machines [12]. The cooperation between the two requires agents to send traffic based on the attackers' orders. Attack network has three components, namely, agents, attackers and control channels. In the attack, the network consists of three types, namely Internet Relay Chat (IRC) based model, proxy handle model and reflector model. Agent Handler The model contains components: handlers, attackers, and agents. Figure depicts the agent handler model architecture. The main attacker finishes the control message over the previously damaged proxy with multiple handlers and directs them to generate unwanted traffic to send to the victim [13].

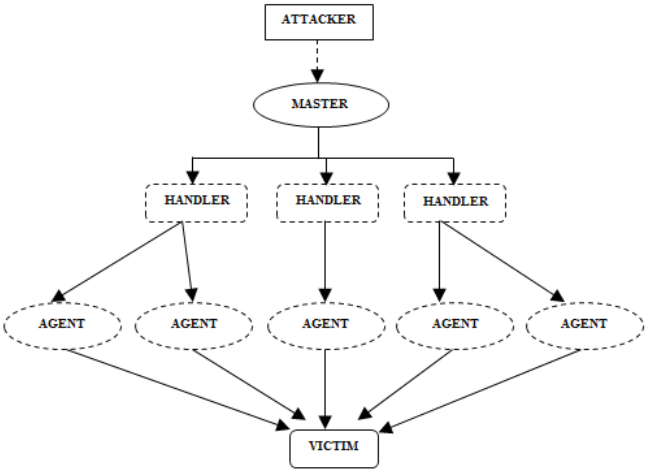

Figure 3: Typical DDoS architecture (the agent handler model)

The difference between the architecture of the IRC-based model and the agent processor model is the former case where the IRC communication channel is used to connect the principal attacker to the proxy machine shown in Figure. In the attack, the reflector model network architecture, reflector layer and DDoS attack architecture shows a major difference. In the request message, the proxy changes the source address field in the IP header to the victim's address, and thus restores the real proxy's address [14]. After that, the reflector will in turn generate the victim's response message. Flood traffic has reached the victim's computer, or the victim network is not from a hundred agents, but from a million reflectors. An exceptionally decentralized reflector-based DDoS attack enhances tracking of real-life attackers by defeating a large number of attackers behind the reflector [15].

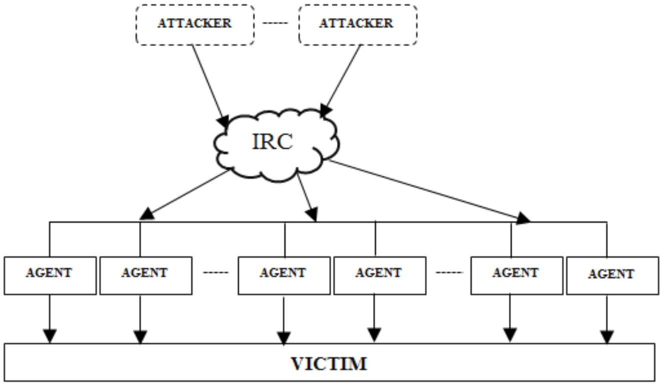

Figure 4: Architecture of IRC based DDoS attack

IV. RELATED WORK

A lot of research has been done in the detection of network in IPv6. Few of the work have been listed below:

Omar E. Elejla et al. developed for studying the DoS and DDoS attacks for IPv6 network utilizing ICMPv6 messages. Moreover, it examines the different related detection and prevents the methods being proposed for tacking ICMPv6 dependent DoS and DDoS attacks. Additionally, it has explained the related tools that may be utilized for executing the attacks.

Luís M. L. Oliveira et al. has proposed a method on the basis of 6 LowPAN protocol of neighbour discovery for the mitigation of DoS attacks taken from the internet with no extra overhead on 6LoWPAN sensor devices. DoS attacks could be described the some third party action with an objective for reducing or eliminating the network ability for performing its required functions. Even there are different general methods in existing computing which eliminates the effect of few of general DoS attacks which are remained is a significant problem for network security community.

T. Winter et al. has utilized IPv6 routing protocol for RPL (low power and lossy network) that gives the scheme and the support has been given to multipoint to point traffic by means of LLN in the central control point and the point to multipoint traffic as of the central control point. The maintenance has also been provided to point to point traffic.

R. Hinden et al. has described the IPv6 addressing framework. The research consist of Ipv6 model for addressing, IPv6 description, IPv6 textual representations, description of IPv6 Types, namely, Multicast address, unicast address and anycast address with the Ipv6 needed addresses for nodes.

G. Montenegro et al. has defined the frame format for IPv6 packets transmission and the technique of producing IPv6 link local address with state-loosely auto configures addresses on IEEE 802.15.4 networks. More specifications have easy header compression mechanism utilizing the collective context and the packet transfer provision in IEEE 802.15.4 meshes.

V. CONCLUSION

IPv6 is the considered to replace the existing IP (Internet protocol) which is IPv4. In spite from various improvements, IPv6 suffers from varied security vulnerabilities and one of that vulnerability is DDoS attack with duplicate address detection mechanism. Comparison between IPv4 & IPv6 is done by detailed study on previous work. Also this paper has dealt with the review of DoS & DDoS attack in IPv6 with advantage and disadvantages along with brief description of IRC Architecture related to DDoS. Work done by number of authors has also been studied and analysed in the same field.

VI. REFERENCES

[1]. Hinden, R. (2017). Internet protocol, version 6 (IPv6) specification.

[2]. Hinden, R. M., & Deering, S. E. (2003). Internet protocol version 6 (IPv6) addressing architecture.

[3]. Montenegro, G., Kushalnagar, N., Hui, J., & Culler, D. (2007). Transmission of IPv6 packets over IEEE 802.15. 4 networks (No. RFC 4944).

[4]. Winter, T. (2012). RPL: IPv6 routing protocol for low-power and lossy networks.

[5]. Lahti, P., & Aalders, M. (2014). U.S. Patent No. 8,869,278. Washington, DC: U.S. Patent and Trademark Office.

[6]. Elejla, O. E., Anbar, M., & Belaton, B. (2017). ICMPv6-based DoS and DDoS attacks and defence mechanisms. IETE Technical Review, 34(4), 390-407.

[7]. Oliveira, L. M., Rodrigues, J. J., Sousa, A. F., & Lloret, J. (2013). Denial of service mitigation approach for IPv6- enabled smart object networks. Concurrency and Computation: Practice and Experience, 25(1), 129-142.

[8]. Elgoarany, K., & Eltoweissy, M. (2007). Security in mobile IPv6: a survey. Information Security Technical Report, 12(1), 32-43.

[9]. Cox, D., & McClanahan, K. (2004). U.S. Patent No. 6,738,814. Washington, DC: U.S. Patent and Trademark Office.

[10]. Lahti, Patrik, and Michael Aalders. "Method for defending against denial-of-service attack on the IPV6 neighbour cache." U.S. Patent 8,869,278, issued October 21, 2014.

[11]. Li, Qing, Ronald Andrew Frederick, and Thomas A. Clare. "System and method for building intelligent and distributed L2-L7 unified threat management infrastructure for IPv4 and IPv6 environments." U.S. Patent 9,553,895, issued January 24, 2017.

[12]. Ren, Kui, Wenjing Lou, Kai Zeng, Feng Bao, Jianying Zhou, and Robert H. Deng. "Routing optimization security in mobile IPv6." Computer Networks 50, no. 13 (2006): 2401-2419.

[13]. Dang, Xuan-Hien, Emil Albright, and Abdullah A. Abonamah. "Performance analysis of probabilistic packet marking in IPv6." Computer Communications 30, no. 16 (2007): 3193-3202.

[14]. Modares, Hero, Amirhossein Moravejosharieh, Jaime Lloret, and Rosli Salleh. "A survey of secure protocols in mobile IPv6." Journal of Network and Computer Applications 39 (2014): 351-368.

[15]. Vilajosana, Xavier, Kris Pister, and Thomas Watteyne. Minimal IPv6 over the TSCH Mode of IEEE 802.15. 4e (6TiSCH) configuration. No. RFC 8180. 2017.

Shubham

Masters of Engineering Honours, Information Security, Chandigarh University

s_kamra@ymail.com

Research Area: IPv6