A NOVEL APPROACH FOR PREVENTING DOS ATTACK IN DUPLICATE ADDRESS DETECTION OF IPV6

B.Bharathi[1], Dr.R.Gunasundari [2], G.Manivasagam[3]

ABSTRACT

IPv6 is the hottest version of the Internet Protocol (IP) that provides an identity and addressing scheme for computers on networks and routes traffic across the Internet. This protocol was introduced to resolve the addressing issues of the previous version. It also provides new services and features such as auto-configuring of the host. This aspect allows the host to configure themselves without any additional utilities. The design aspects of IPv6 have also brought some security issues. The important of them is Denial of service attack that occurs in DAD (Duplicate Address Detection) which does not allows the auto-configuration feature. The Mechanism like SeND (Secure Neighbor Discovery), SSAS (Simple Secure Addressing Scheme) are developed to solve this issues. The side effects of these mechanisms are its complex nature and deterioration of its performance. This paper reviews the moral weakness of these mechanisms and proposes a novel method, Safe Addressing Scheme (SAS), which addresses them.

Keyword: Safe Addressing Scheme, DAD Attack, Denial of Service, Self-Configuration, Auto-configuration problem

[1]Assistant Professor, Department of CS, CA & IT, Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India

[2]Assosciate Professor, Department of CS, CA & IT, Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India

[3]Assistant Professor, Department of CS, CA & IT, Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India

I. INTRODUCTION

Internet Protocol version 6 (IPv6) is the most popular version of the Internet Protocol (IP) and the first version to be deployed broadly. IPv6 is developed by Internet Engineering Task Force (IETF) originally to handle the long-term problem of IPv4 addressing scheme. Along with its contribution of a mammoth amount of logical address space, this protocol has sufficient features to which address the inadequacy of IPv4.

The major features are Reduced Header Size, Auto-Configuration, Quick Forwarding/Routing, No Broadcast, Any-cast Support, Even Transition, Resilience and Enhanced priority Support.

A. Reduced Header size

IPv6's header has been streamline by moving all preventable information and options (which are present in IPv4 header) to the end of the IPv6 header. IPv6 header is just double the size than IPv4 provided the fact that IPv6 address is four times longer.

B. Auto-configuration

IPv6 supports auto configuration mode for its host devices that is of stateful and stateless [11]. This provides an alternative for DHCP in inter segment communication.

C. Quick Forwarding/Routing

The header has been streamlined by placing all

preventable information at the end of the header. The first part in header information is adequate for a Router to make decisions on routing, thus making routing decision as quickly as looking at the mandatory header.

D. No Broadcast

Though Ethernet/Token Ring is considered as broadcast network because they support Broadcasting, IPv6 does not have any broadcast support any more. It uses multicast to communicate with multiple hosts

E. Any-cast Support

The most important feature of IPv6 is Any-cast support. This feature assigns the same IP address for multiple interfaces over the internet. Routers, when routing, send the packets to the nearest host. This helps to service providers to provide region oriented services. For example www.yahoo.in and yahoo.com are assigned same IP address but routed to former when connected in India and later when routed in America.

F. Even Transition

The address spaces in IPv6 are huge, so numerous devices are allocated with unique IP address globally. This option saves the IP addresses and it also avoids NAT which help the devices to send and receive data within themselves. For example, streaming media along with VoIP can be used much competently. The other fact is, since the header is loaded lightly, the routers can take forwarding decisions and forward them as quickly as they arrive.

G. Enhanced Priority Support

Differential Service Code Point (DSCP) of IPv4 used 6 bits and Explicit Congestion Notification (ECN) uses 2 bits to provide Quality of Service but it could used only with end to end devices if then support it, i.e., the source host and destination host and primary network must support it. In IPv6, Traffic class and Flow Label guides the underlying router to efficiently process the packet and route it.

H. Resilience

The main feature of IPv6 is Resilience that allows appending more information in option part of it. The difference with the previous version is that IPv4 provides only 40 bytes space for option where as IpV6 allows as much size as its Packet itself.

II NEIGHBOR DISCOVERY PROTOCOL

The host in IPv6 network has the capability of auto-configuring themselves with a distinctive link-local address. When host gets an IPv6 address, it immediately ties a number to the multicast groups. Generally Auto-configured numbers differ from others [6]. It may start with fe80: Every part of the communication that is related to this sector take place on these multicasts addresses only. A host goes through a series of states in IPv6:

Neighbor Solicitation: The Host sends a Neighbor Solicitation message out to FF02::1/16 multicast address for all its IPv6 addresses in order to know if any host occupies the same IP addresses after configuring. The Configuration may be auto or through DHCP server or it may be manual.

DAD (Duplicate Address Detection): When the host does not receive any NR message from any host in their network regarding Neighbor Solicitation message, it assumes that no duplicate IP address exists on the sector.

Neighbor Advertisement: After assigning the address to the interface and making them up and running the host once again broadcast the Neighbor Advertisement message telling all other hosts on the sector, that it has assigned those IPv6 addresses to its interfaces. After this process the host is done with the configuration of its IPv6 addresses and it does the following things:

Router Solicitation: After successful configuration of IP Address, the host sends Router Solicitation multicast message (FF02::2/16) to its sector to know the presence of its router on that segment. This procedure helps the device to configure the router to its default gateway. Unfortunately if the defaults router fails, the device can look for a new router and configure it as default gateway

Router Advertisement: After receiving the Router Solicitation message, the router replies back its response to the device by advertising its occurrence on that connection [1, 5, 15].

Redirect: When router receives the Router Solicitation request and it knows that its current scenario is not best for the default gateway, it replies with a Redirect message, informing the host that to find a new "Next-Hop" router availability. The next hop is the succession of routers that are interconnected mutually in a network and it's the next possible destination for a data packet. In fact, next hop is an IP address entered in a routing table, which specifies the next best possible router in the specified route[1, 5, 15].Every individual router have an entry in its routing table with a next hop address, which is derived based on the protocol used for routing and its related metric.

III DAD PROCESS SECURITY ISSUES

In the final stages of auto-configuring, the host(s) checks its auto-generated IP for its uniqueness in order to have communication within the network [1, 5, 10]. The authentication mechanism is done exclusively through Duplicate Address Detection procedure as described above. If the auto-configured address exists in the network, the host with that IP will respond with Neighbor Advertisement (NA). Now the DAD process is performed again with the new host. If no proper response for the NS broadcasted from the network, the generated IP address is distinct [1, 5, 15].

The Figure.1 describes the Duplicate Address Detection Procedure of IPv6 network. In IPv6 local link communication, the host with IPv6 configured IP's can take part in DAD process. The design of NS or NA messages (i.e., ND Messages) is insecure by nature. So, the intruder can effortlessly make the most of the DAD process by constructing Network Advertisement message and respond it to every Network Solicitation message received, which can rattle duplicate detection process and route to failure. Thus, auto-configuring host will never attain a valid IP address. This leads to a problem that, a host trying for auto-configuring will never-ever have communication in the home network. This effort to accomplish the denial of service (DOS) attack is named as Denial of Service-on-DAD attack.

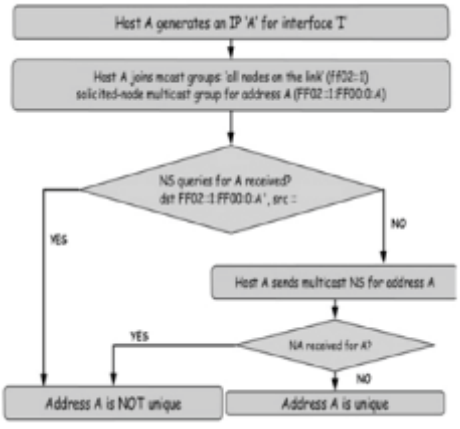

Figure.1.Duplicate Address Detection Process

IV RELATED WORKS

The DoS Attack on DAD is prevented already with SeND (Secure Neighbor Discovery), SSAS (Simple Secure Addressing Scheme) mechanism. The other possible mechanism that was proposed to figure out this problem in IPv6 is Trust-ND. Yet, these procedures have a few design issues which controls their execution on DAD process in local network [9]. The following part characterizes the problems and boundaries of the offered mechanisms as in breif

A. Secure Neighbor Discovery (SeND)

SeND is introduced in IPV6 to handle the issues relevant to security with Network Discovery protocol messages [7]. This mechanism proposes 4 distinct options; Nonce option, CGA option , Timestamp option, and RSA signature option along with two Internet Control message protocol messages;[8] namely Certificate Path Solicitation (CPS) and Certificate Path Advertisement (CPA) stated in RFC 3971 [10]. Secure Network Discovery mechanism prevents DoS - DAD attacks on NDP, but research has confirmed [11, 12] that this mechanism has a downside similar to elevated computation to produce the Certificate Path Advertisement option and RSA signature. Hence, this approach employs high processing time. As by result of the investigation, this approach adds considerable computation time and it uses 367.59 ms to execute the message verification operation [12].

Hence, if this mechanism is implemented, its authentication and validation of certificates can create delay and add to difficulty during duplicate detection process as represented by the researches [7]. So, any wicked user can utilize this approach and can source the attack against this procedure by enticing the victim user during the process of message verification.

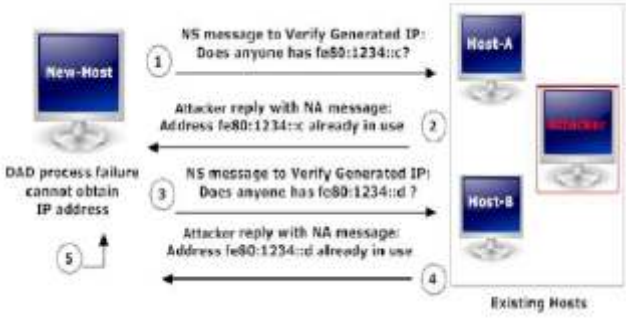

Figure.2. DOS Attack during DAD Process

B. Simple Secure Addressing Scheme (SSAS)

In handling the problems with previous approach (SeND), a new mechanism is designed and it's known as Simple Secure Addressing Scheme (SSAS). It was projected to be an enhanced edition of SeND mechanism. It addresses the protection of ND messages during duplication detection process in version 6 network [11]. Simple Secure proposes another methodology by implementing elliptic curve cryptography (ECC) algorithm instead of RSA which is used by Secure ND mechanism for handling process of configuration. In other terms, simple secure mechanism is trivial version of SeND mechanism. SSAS uses timestamp options and signature as appended information to protect ND messages from spoofing attack during DAD process. This mechanism uses signatures and Key-exchange algorithm for DAD processing attack, but still the complexity issues exist [12]. When compared with the SeNd the complexity and message processing time has been cut-down dramatically. The research conducted earlier by Praptodiyono et al. in 2015 [12] indicates that this approach takes 223.1 ms to create an interface identifier which is a reasonable time for processing. The

complexity arises with the cryptography algorithm used with it. The delay time of this mechanism for verifying the message after address auto-generation in IpV6 local link again paves a way for DAD attack in the network.

C. Trust-ND

In recent time, researches have claimed a light-weighted approach for duplicate detection process in version 6 network known as Trust-ND [12]. The important factor with the approach has been the complex nature of the Neighbor Discovery message computation. When compared with previous mechanisms like SeND and SSAS this approach has significantly cut-down the computing time of ND messages all over the process of address duplicate detection. In this mechanism, authentication of message is an effect of SHA-1 operation and it acts as a message integrity check. Thus, this mechanism depends on SHA-1 hash function to convince the security measures. Trust-ND's protection is based on SHA-1 hash [13] function, thus any wicked host can utilize this limitation to produce hash collision attack next to this approach and that this may lead to DoS attack on duplicate detection process in network. Hence, due to this defense susceptibility of Trust-ND, it cannot be the appropriate approach for duplicate detection process in this version of Internet protocol.

Owing to the setting possessed by existing security approaches as abovementioned, the execution of the security mechanisms for duplicate detection process has been restricted.

As an effect, this duplicate verification process is still open to attack and prone to be exploited by wicked machines. Therefore, this paper projects a new mechanism namely Safe Addressing Scheme (SAS) to secure Neighbor discovery messages during DAD process. The Design of SAS method can defend both solicitation and advertisement messages from any kind of utilization attacks like, replay attack, spoofing, MITM (man-in-the-middle attack) which are liable to route the DoS attack during duplicate detection process in IP network. The following Section explains the design and implementation processes of Safe Addressing Scheme (SAS).

V PROPOSED METHOD: SAFE ADDRESS SCHEME (SAS)

In IPv6 duplicate detection Process, the protection of solicitation and advertisement messages from diverse types of attacks like masquerade, content modification, sequence modification and timing modification are to be handled or it guides to service denial attack [16]. The DoS attack commonly represents lack of the services i.e. in this scenario not allowing for self-configuring of the new host with distinct IP addresses.

The Proposed method includes an additional field SAS-AuthCode in the NS and NA message format as shown in figure.3 and figure.4. This method uses Blowfish algorithm along with CCMA for security and better performnance.

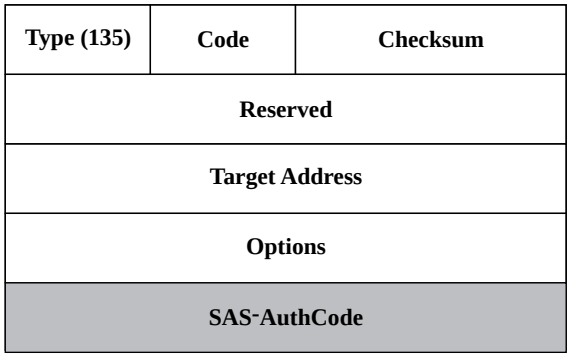

Figure.3. Modified NS Message for Safe Addressing Scheme Packet Format

Type (136)			Code	Checksum
R	S	O	Reserved	
Target Address				
Options				
SAS-AuthCode				

Figure.4. Modified NA Message for Safe Addressing Scheme Packet Format

In these formats the value 135 of Type field represents NS message and 136 represents NA message. Code 0 with Type 135 represents that source address of the IPv6 Packet is encapsulating the NS with Unspecified address ::/0 (All Zeros) if the NS is sent for Duplicate Address Detection and the destination address of NS is the solicited-Node Multicast Address corresponding to the target address. Checksum generally holds the functional value for error detection coverage for the entire message. The SAS-AuthCode field has the Secret key generated by CMAC (Cipher based Message Authentication Code) algorithm[19,20]. This Code is appended to the NS message and is send to multicast address group for verification. After receiving the message of NS all the host will check for its SAS-Authcode with the received code and replies with NA if it matched. Figure.5. represents the SAS mechanism along with the generation of SAS-Authcode.

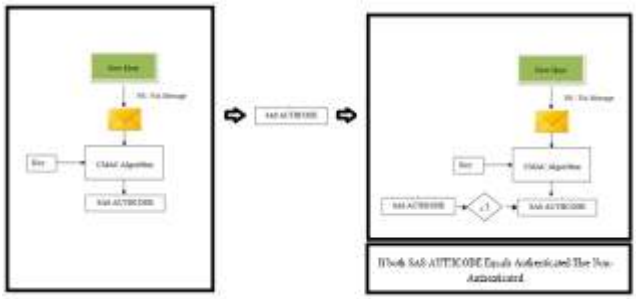

Figure.5. Proposed SAS Method

A. Test-Model

In performing the above mechanism the following test model was created. The test model consists of two existing systems connected with Ethernet Switch in a network. The Ethernet switch in effect connected to the Router or default gateway that acts as an identity of the whole network to the outside world. The Ethernet is also connected to the network monitoring system that generally acts as a server. The attacker who could be a host of own network is also connected to this network. The packet tracing is done by packet tracer tool.

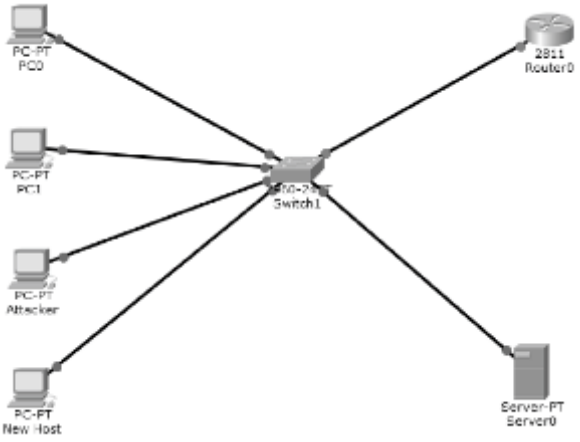

Figure.6. Test Model

B. Result and Discussion

This part provides the result of the test model with SAS mechanism. The processing time of the NS and NA has been used as a metrics for evaluating the performance.

The Standard in figure.7 refers to the plain NS message without SAS field. The Trusted-NS used basic Mac and SAS uses CMAC. The Comparison graph states clearly that mean of the SAS (Safe Address Scheme) is better in processing time than Trusted -NS.

Existing Machine	Standard NS	Trusted NS	SAS
Overhead	Base Line	14.2	8.72
Mean	1.146	15.35	9.2

Figure.7.NS Message Processing Time

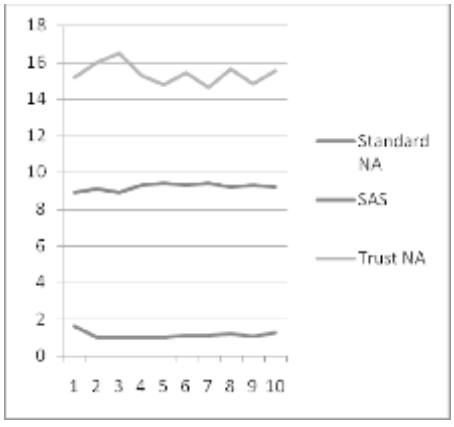

Figure.8. Process Time Comparison NS Message

The researches have already stated that the Trusted-SA is better in security and in performance when compared to previous mechanism. But the proposed NA Performance time is calculated with the above setup and found that the SAS NA is better than the Trusted-NA. The following figures (9 and 10) point the value for better reference.

New Host	Standard NA	Trusted NA	SAS NA
Overhead	Base Line	14.2	8.72
Mean	1.17	8.98	15.4

Figure.9. NA Message Processing Time

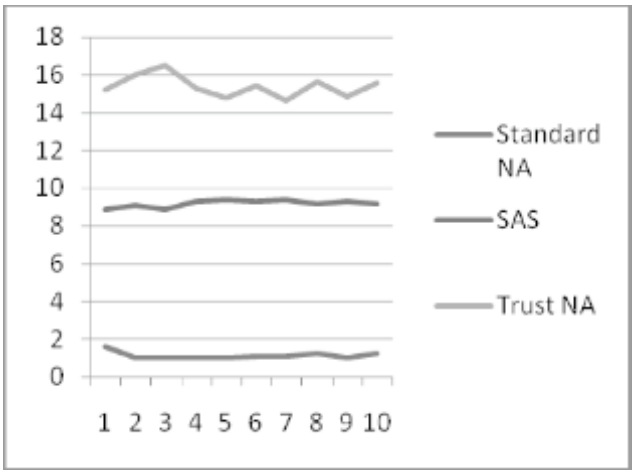

Figure.10. Process Time Comparison NA Message

V CONCLUSION

This paper finally proposes a better mechanism (SAS) which uses Blowfish algorithm for encryption and CMAC as authentication protocol that performs at the faster rate in DAD Process of IPv6 with greater security. The Test model has been tested only on Trusted-NS and SAS. The results clearly states that the mechanism represented is better when compared to previous approaches. The Complexity of the previous approaches is higher than the proposed methods. In addition, experiments results shows that the SAS mechanism is challenging to various types of attacks which can lead to DoS attacks directly or indirectly in DAD process of IPv6 link local network. The future work in this mechanism is to develop a new cryptographic algorithm with even a better authentication protocol. The mechanism must also be optimized even for better results.

References

[1] Thomson S, Narten T, Jinmei T. IPv6 Stateless Address Auto-configuration. Internet RFC 4862, 2007.

[2] V. Ndatinya, Z. Xiao, V. R. Manepalli, K. Meng, and Y. Xiao, ?Network forensics analysis using Wireshark,? International Journal of Security and Networks, vol. 10(2), pp. 91-106, 2015.

[3] Shoup V, fast and provably secure message authentication based on universal hashing. In Advances in Cryptology-CRYPTO'96, pp. 313-328, 1996.

[4] Botta, A., de Donato, W., Persico, V., & Pescapé, A. Integration of cloud computing and internet of things: a survey. Future Generation Computer Systems, Elsevier, 56, pp.684-700, 2016.

[5] Rehman SU, Manickam S. Significance of duplicate address detection mechanism in Ipv6 and its security issues: A survey. Indian Journal of Science and Technology, vol. (8)30, 2015.

[6] Narten T, Simpson, WA, Nordmark E, Soliman H., Neighbor discovery for IP version 6 (IPv6), 2007.

[7] AlSa'deh A, Meinel C. Secure neighbor discovery: Review, challenges, perspectives, and recommendations. IEEE Security & Privacy, vol. 10, pp. 26-34, 2012.

[8] Conta A, Gupta M. Internet control message protocol (ICMPv6) specification. Internet RFC 4443, 2006.

[9] Dawood, H. IPv6 Security Vulnerabilities. International Journal of Information Security Science, vol. 1(4), pp.100-105, 2012.

[10] Arkko J, Kemp f J, Zill B, Nikander P. Secure neighbor discovery (SEND). Internet RFC 3971, 2005.

[11] Rafiee H, Meinel C. SSAS: A simple secure addressing scheme for IPv6 autoconfiguration. Eleventh Annual IEEE International Conference on Privacy, Security and Trust (PST), pp. 275-282, 2013.

[12] Praptodiyono S, Murugesan R K, Hasbullah IH., Wey CY, Kadhum MM, Osman A. Security mechanism for IPv6 stateless address autoconfiguration. 2015 IEEE International Conference on Automation, Cognitive Science, Optics, Micro Electro-Mechanical System, and Information Technology (ICACOMIT), pp. 31-36, 2015.

[13] Andreeva E, Mennink B, Preneel B. Open problems in hash function security. Designs, Codes and Cryptography, vol. 77, pp. 611-631, 2015.

[14] Bhargavan K, Leurent G. Transcript collision attacks: Breaking authentication in TLS, IKE, and SSH. NDSS, 2016.

[15] Rehman SU, Manickam S. Denial of Service Attack in IPv6 Duplicate Address Detection Process. International Journal of Advanced Computer Science & Applications, vol. 7, pp. 232-238, 2016.

[16] Moore D, Shannon C, Brown D J, Voelker GM, Savage S. Inferring Internet denial-of-service activity. ACM Transactions on Computer Systems (TOCS), vol. 24. Pp. 115-139, 2006.

[17] Li, S., Da Xu, L., & Zhao, S. The internet of things: a survey. Information Systems Frontiers, Springer, Science & Business Media, vol. 17(2), pp. 243-259, 2015.

[18] Krovetz T. UMAC: Message authentication code using universal hashing. Internet RFC 4418, 2006.

[19] M Anand Kumar, M Hemalatha, P Nagaraj, S Karthikeyan. A new way towards security in TCP/IP protocol suite. Proceedings of the 14th WSEAS international conference on Computers: part of the 14th WSEAS CSCC multi conference

[20] Mr.B.Bharathi, Mr.G.Manivasagam, Dr.M.Anand Kumar. Metrics for Performance Evaluation of Encryption Algorithms. International journal of Advance Research in science and Engineering, vol 6(3) pp. 62-72

[21] Deering S, Hinden R. Internet protocol version 6 (IPv6) specifications. Internet RFC 2460, 1998.