International Journal of Security and Its Applications
Vol. 10, No. 4 (2016), pp.143-154
http://dx.doi.org/10.14257/ijsia.2016.10.4.15

Novel Mechanism to Prevent Denial of Service (DoS) Attacks in IPv6 Duplicate Address Detection Process

Shafiq Ul Rehman[1] and Selvakumar Manickam[1]

[1]*National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia*
[1]*shafiq@nav6.usm.my,*[1]*selva@usm.my*

Abstract

Most IPv6 security issues are still the same as IPv4; IPv6 has its own unique design characteristics that have additional impact to system and network security, as well as the potential impact on policies and procedures. Address autoconfiguration is a key feature of the IPv6 protocol stack that allow hosts to generate own addresses using a confluence of information from other hosts and information from router advertisement. Duplicate Address Detection (DAD) is a process that is part of address autoconfiguration that is used to check if the addresses generated has already been configured. Nevertheless, the design of DAD process is vulnerable to Denial of Service (DoS) attack leaving hosts unconfigured. For example, any host can reply to Neighbor Solicitations (NS) for a temporary address, causing the other host to consider it as a duplicate and eventually reject the address. Various mechanisms such as SeND and SAVI has been introduced to address such attacks, but these techniques were not very effective as there were still possibilities of DoS attacks to be carried out. As such, a new mechanism is needed to more effectively prevent DoS attacks on DAD process. In this paper, we present a detailed design and development of a novel mechanism that can address the shortfalls of existing prevention techniques.

Keywords*: Address autoconfiguration, DAD, DoS, Intrusion Prevention, IPv6 Security, Neighbor Discovery*

1. Introduction

The address autoconfiguration [1] is one of the main features of Internet protocol version 6 (IPv6) [2, 3]. This feature allows IPv6 hosts to configure IP addresses automatically without any intervention such as; DHCPv6. Nevertheless, generated IP address has to be unique on the local link so that to prevent the conflict of IP addresses among hosts in IPv6 network. In order to resolve this issue IPv6 has a mechanism known as duplicate address detection (DAD) [1,4,5] process which ensures that there is no duplicate IP address among hosts on same link by verifying the uniqueness of self-generated IP address.

During DAD process, hosts use two types of Internet control message protocol version 6 (ICMPv6) [6] message such as; neighbor solicitation (NS) and neighbor advertisement (NA) messages to communicate with each other. New host use neighbor solicitation (NS) message to send a query to existing hosts on the same link and neighbor advertisement (NA) message is used in responding back. For example, when a new host performs DAD process, it sends NS message to verify whether the self-generated IP address is already configured by any existing host or not. In case existing host(s) has obtained that IP address it replies back with a NA message that IP address is already configured else if no reply is received it means generated IP is unique. Figure 1 [7] depicts the duplicate address detection process.

ISSN: 1738-9976 IJSIA

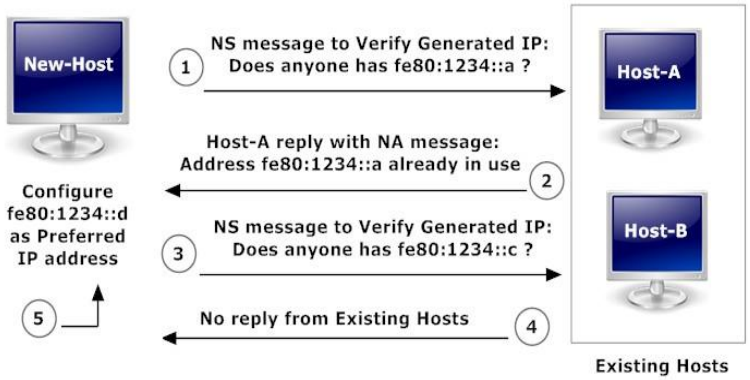

Figure 1. Duplicate Address Detection Process

In IPv6 network, existing hosts are considered as a reliable; hence any host can participate in DAD process. Thus, any intruding host can exploit this process. Therefore, when a new host attempts DAD process an attacker can disrupt the verification process by sending bogus messages in reply. Studies [8-10] have proven that DAD process is susceptible to denial of service attacks.

During DoS attack on DAD process, victim host is unable to obtain a valid IP address since on each attempt an attacker is claiming the generated IP address via sending fake NA messages in response to its NS messages. Figure 2 [7] illustrates the DoS on DAD attack.

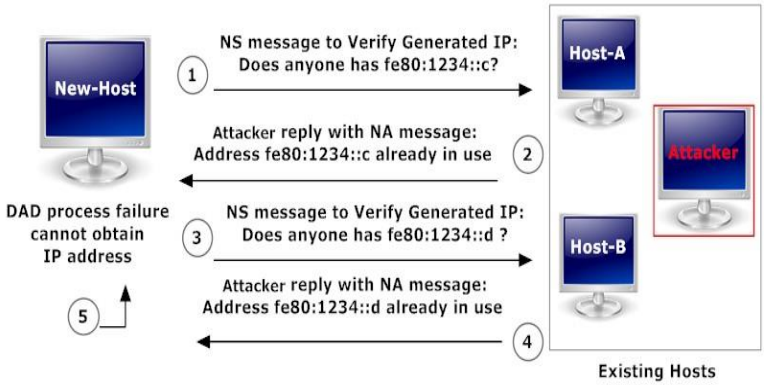

Figure 2. DoS Attack During DAD Process

2. Related Works

Considering the security issues in IPv6 DAD process, as already discussed in section 1. Several security mechanisms have been proposed by the researchers to address this problem. Such as; Secure neighbor discovery protocol (SeND) [11, 12], was defined to address the security problem with neighbor discovery protocol (NDP) [13]. Since DAD is an integral part of the NDP, hence can address the IPv6 DAD issues as well. However, studies [14, 15] have shown that main issue with SeND mechanism is high complexity and also it lacks confidentiality. Thus, during address verification an attacker can exploit SeND message by sending a large number of fabricated packets to the victim host. Since it consumes a lot of processing time, which eventually leads to DoS Attack. Another mechanism known as source address validation improvement (SAVI) [16], was proposed to prevent the source address spoofing attacks. However, the study [14] has shown that SAVI is susceptible to various attacks which can lead to DoS attacks.

Other mechanism such as; optimistic duplicate address detection (DAD) RFC 4429 [5] was proposed to reduce delay in IPv6 DAD process. Nevertheless, it cannot prevent DoS

attacks on DAD process. Moreover, Enhanced Duplicate Address Detection RFC 7527 [17] was defined to enhance the DAD mechanism; in order to address the loop backed issue in DAD process. However, the mechanism does not define any prevention from DoS attacks on DAD process.

In a recent attempt, an integrated framework has been proposed to detect and mitigate DoS attacks on DAD process in IPv6 link local communication [7]. A proposed framework claims to detect and mitigate DoS attacks at the same time. Therefore, can enhance the security in IPv6 DAD process.

Thus, from the existing mechanisms it is clear that there have been attempts from the researchers to enhance the security in IPv6 DAD mechanism. However, studies have also proven that there is no such mechanism which can prevent DoS attacks on DAD process in IPv6 network. Even though, some schemes claims to improve the security in DAD mechanism while others enhance DAD algorithm itself. However, currently there is no such security mechanism which can effectively prevent the DoS attacks in IPv6 DAD process. Therefore, a new mechanism is required to address this issue.

3. Proposed Mechanism Approach

A novel mechanism has been proposed to effectively prevent the denial of service (DoS) attacks in IPv6 duplicate address detection Process. Beginning with the assumptions, this section also describes the threat model, and the design goals of this mechanism in order to secure DAD process during host address autoconfiguration in IPv6 local network.

3.1. Assumptions

A proposed mechanism depends on the following assumptions to design a new security mechanism for DAD process is as follows:

1) IPv6 local network comprises of at least one gateway router, an ethernet switch, a new host, an existing host and an attacker.
2) IPv6 address in the local network is obtained from SLAAC mechanism instead of using DHCPv6 server.
3) The gateway router is secure which sends out various parameters required by hosts on the local link for autoconfiguration purpose.
4) Every new host in IPv6 local network has its own node controller installed.
5) Network monitoring PC which can be used to monitor and analyze (NS/NA messages) packets captured during DAD process in IPv6 local network.

Test-bed scenario has been set up for this purpose as shown in Figure 3.

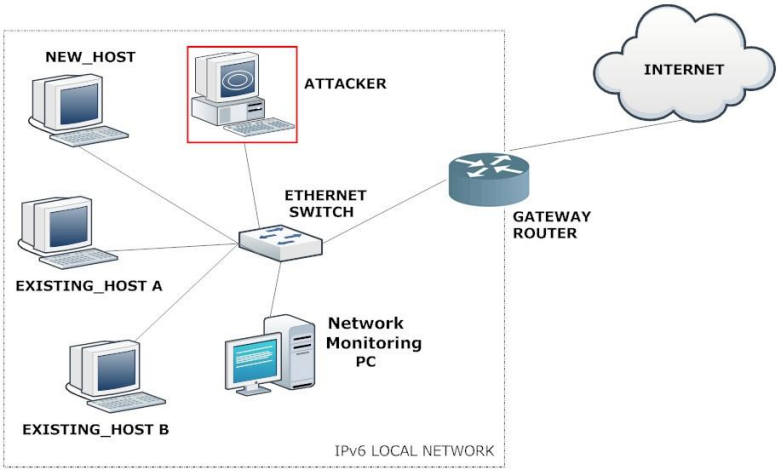

Figure 3. Test-Bed Environment

3.2. Threat Model

Based on the assumptions, threat model could be provided in order to find out a new security mechanism that satisfies the security requirements.

1) The attacker can perform spoofing for neighbor discovery messages such as; NA and NS. Since the NDP messages are insecure by nature, an attacker could modify any field in NS/NA message to launch a DoS attack.
2) The attacker is also able to spoof any IP source address to send malicious messages. This will cause the receiving node to create false entries in its neighbor cache table and thus can disrupt the link local communication.
3) The attacker can read any message sent to existing hosts in IPv6 local network. As the new host uses all node multicast address groups (FF02::1) to perform DAD process. Therefore, all nodes in local network can receive this message including an attacker. Thus an attacker can launch DoS attack by sending fake NA message in reply.

3.3. Design Goals

There are two requirements to design a new security mechanism for DAD process to protect NS and NA messages exploitation namely integrated and controlled DAD operation which can be achieved as follows:

1) To prevent any exploitation of NS and NA messages, since NS/NA messages are possible to be exploited by attackers to launch DoS attacks. Thus, preventing the exploitations of NS/NA messages would satisfy the integrated requirement.
2) To provide a controlled scheme in IPv6 local network in order to perform DAD process between a new host and existing hosts would reduce the chances of DoS attack. Since it avoids the participation of unauthorized nodes in DAD process including an attacker. Thus, would satisfy the successful DAD operation requirement.

4. Node Controller Model

In order to fulfill the security requirements for DAD process a novel mechanism known as Node Controller Model has been designed. This section describes the framework of the designed model, its components and their operations.

4.1. Node Controller Framework

Over the years, the concept of Rule-based system [18, 19] has been used in artificial intelligence related applications and research. Recently, Rule-based system has been applied to design detection and mitigation techniques such as; [7, 20]. Similarly, the same approach can be used to design a node controller framework which can prevent DoS attacks in IPv6 DAD process. Figure 4 presents the node controller framework.

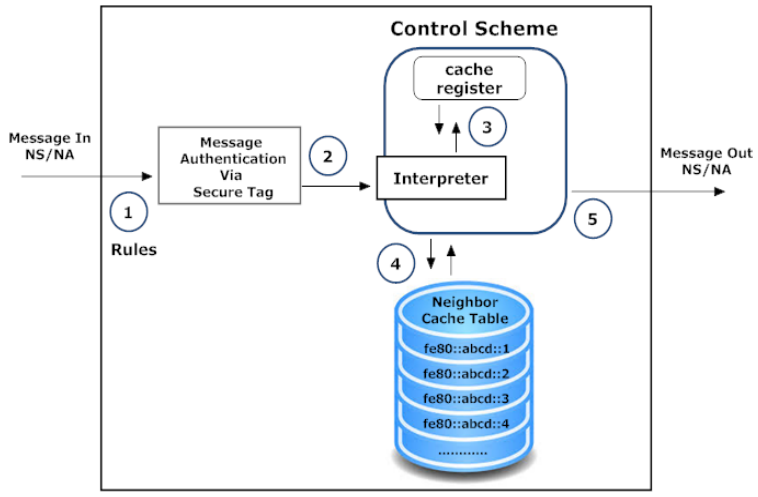

Figure 4. Node Controller Framework

4.2. Components of Node Controller Model

The node controller model has four main elements such as; Message authentication, Control scheme, Neighbor cache table and set of Rules.

1) *Message Authentication* would be used to satisfy the authentication and verification of incoming and outgoing (NS/NA) messages via *secure tag*.
2) *Control scheme* is the core component of this mechanism as it performs the verification of the IP address. It has two subsections such as; *cache registry* and *interpreter*. *Cache registry is* temporary memory to hold incoming NS/NA message and the *interpreter* performs the matching of incoming IP address with its obtained IP address.
3) *Neighbor cache table* is the repository of existing IP addresses currently allocated to the existing hosts on the same link. After the verification of DAD process for unique IP is done. Later, its information is stored in the existing database to keep records updated.
4) *Rules*, a list of rules (knowledge base) which specifies the type of operation to perform.

5. Message Authentication Model

In order to secure NS and NA message exchange between the nodes in IPv6 local network the use of message authentication is recommended to authenticate the message content. In this manner, the integrity of NDP messages especially NA and NS messages will be maintained which is the main purpose of this security mechanism. In case of IPv6 DAD process, authentication is required to protect NS and NA messages from several types of attacks such as; masquerade, content modification sequence modification and timing modification which are the main causes of launching a DoS attack.

Therefore, to authenticate the NDP messages study [21] have shown the use of a hash function is suitable as it has less computation and faster than encryption mechanism. Thus, the most suitable and available hash function algorithm has to be selected which can satisfy this requirement. Studies [21,22] have proven that Universal Hashing approach can be used for message authentication, search operations *etc*. on contemporary machines.

Moreover, the study [22] has shown that UMAC is faster than current practice hashing function HMAC-SHA1 [23], as a practical algorithm for next-generation message authentication. For instance, UMAC achieves peak performance of 5.6 Gbits/sec (0.51 cycles/byte) as compared to SHA-1 implementation runs at 12.6 cycles/byte [22].

According to the study [22] UMAC is parallelizable and will have ever-faster implementation speeds as machines offer up increasing amounts of parallelism. It could provide data integrity to detect a changing of NS and NA message content as the security requirement.

In addition to provide availability, filtering mechanism for receiving message is required. Considering most of NDP messages is in the form of request and response, the use of sequence number or nonce is appropriate to make sure a reply message is only for the corresponding solicitation message.

However, to limit the receiving responses, there is a need to store message generation time in the sender as well Therefore, pre-defined time starting from the generation time could be used to prevent DoS attack on DAD process. This authentication model is the main consideration for formatting new security option known as *Secure Tag*. Figure 5 depicts the designed message authentication model.

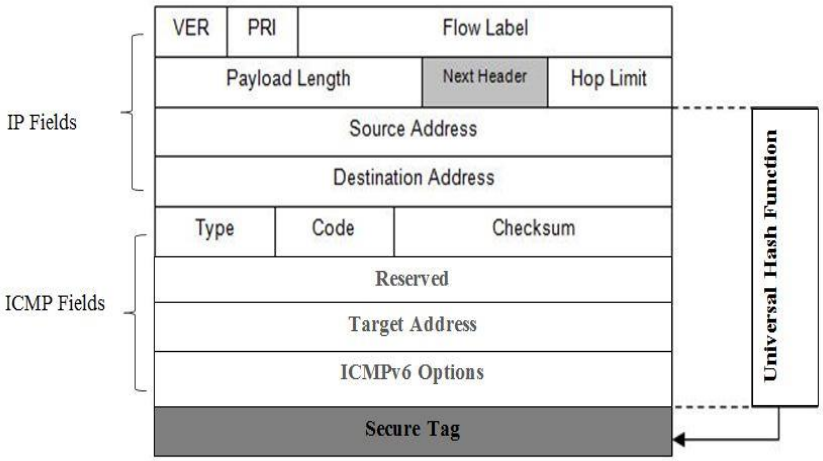

Figure 5. Message Authentication Model

5.1. Secure Tag

The default standard NDP messages such as NS and NA messages consider that all neighboring nodes are trustworthy. However, the increasing cases of insider attack could become evidence that one or more neighboring node may be a malicious node that could launch a DoS attack on other nodes. Therefore, to distinguish the valid nodes from malicious ones can be determined by applying some security mechanism on NDP messages during neighbor discovery process particularly on DAD process. In order to fulfill such security requirement a "*Secure tag*" can be applied on NS and NA messages to ensure that only nodes which possess *secure tag* are able to communicate in IPv6 local network. *Secure tag* is an option which comprises of message authentication algorithm to distinguish the valid messages from the bogus ones.

Thus, when a new host performs DAD process it will generate a *secure tag* appends it on NS message and send it to multicast address upon receiving NS message existing host(s) will match it with its own *secure tag*. If the s*ecure tag* matches, then it will perform DAD process and can reply via NA message appended with *secure tag*. Similarly, upon receiving the NA message new host does the same matching of *secure tags* else if no match of secure tags is found new host can discard the message. Hence a new host can perform DAD process successfully Thus, in this manner new host can obtain a unique IP address. Secure tag generation and matching process is shown in Figure 6.

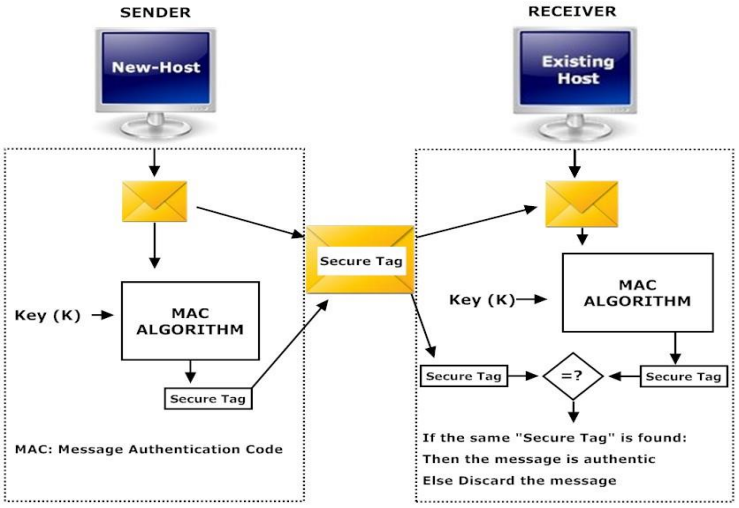

Figure 6. Secure Tag Generation and Matching Process

5.2. Secure Tag Format

In order to ensure only valid nodes can communicate in an IPv6 local network, *Secure Tag* can be appended to carry the message authentication data that could be used to authenticate the NS/NA messages. As required in the message authentication model, a new security option has been introduced, namely s*ecure tag* as already mentioned would be attached to NA/NS messages. The *secure tag* contains at least three requirements discussed in the model including the message authentication data itself, nonce and message generation time. After the addition of the secure tag, the NDP messages such as NS and NA are then named as Secure-NA and Secure-NS. As depicted in Figure 7.

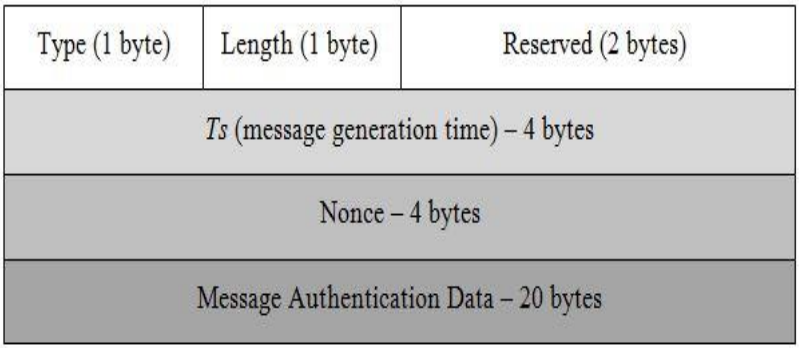

Figure 7. Secure Tag Format

The format of the *secure tag* option as shown in Figure 7 follows the option format of RFC 4861 [13]; all NDP options should include type and length. The length of NDP option should be minimum 8 bytes (64 bit); otherwise the option must be padded. Further, the secure tag consists of 32 bytes size divided into six fields as follows:

Type: 8 bit size identifier that indicates the option type carrying by the NDP message. The secure tag type defined is 253 since this option is under experimentation.

Length: 1 byte field to indicate the total length of the secure tag option including the type and length fields in unit of 8 bytes. The total length of the secure tag option is 32 bytes and thus the value of the Length field is 4.

Reserved: 16 bit unused field that is purported for future improvement of the secure tag. RFC 4861 mandates the minimum NDP option is 64 bits and its length is multiple 8 bytes. Thus, reserved field is padded to meet the minimum size of NDP option.

Ts: 4 bytes size is the message generation time that indicates when the NDP messages with secure tag are generated by the sender. This field contains the hex format of the date time format, including: hour, min, second and millisecond.

Nonce: 4 bytes field that is intended to provide uniqueness of NS/NA messages on IPv6 DAD process in order to prevent replay attack. This field contains a random number generated by sender of solicitation message or unsolicited advertisement.

MAD: 20 byte size is the message authentication data as the output of the universal hash function operation used for hashing of sender information. This field is the main field of the secure tag in providing key information to the receiver. This will examine whether the message contains any alteration.

6. Secure Duplicate Address Detection Mechanism

A new DAD mechanism has been proposed to protect NS/NA messages from any kind of exploitation attempting to attack against data integrity as well as availability. Therefore, to consider the IPv6 local network as a secure network. However, before implementing the new proposed mechanism, an explanation on how the security mechanism works is required. The main process in IPv6 address autoconfiguration is DAD process. This section provides explanation how the proposed DAD mechanism could secure the link local communication between nodes during DAD process in IPv6 local network.

Secure-DAD mechanism proposes to attach S*ecure Tag* option into NS and NA messages. This would be used by receiver to distinguish the secure NS/NA message from insecure one. This is message integrity protection and also DoS prevention for both sender and receiver. While nonce appeared in every NS/NA message would prevent replay attack. The security services for each DAD process could be explained as follows:

The DAD process is vulnerable to DAD DoS attack that could send rogue NA to make the DAD fail. In Secure-DAD mechanism, the NA must carry S*ecure Tag* Option to make sure the NA message is valid and trusted. This validation is important to distinguish the valid NA and the rogue one. If the New Host receives a rogue NA based on the verification result, it will ignore the message. Otherwise, perform a new DAD process on the local network.

In order to perform a secure DAD process, the new DAD mechanism has been defined based on rules as:

1) When a New Host generates a tentative IP address, before sending the NS message, it would generate a *Secure Tag*.
2) The generated *Secure Tag* will be appended to NS message.
3) New host sends the secure NS message to multicast address ff02::7 instead of all nodes solicited multicast group ff02::1. In order to make sure only existing host, who belongs to ff02::7 will receive the NS message rather than all nodes including an attacker in IPv6 local network.
4) Existing host(s) will verify the received NS message by matching its generated *Secure Tag* with sender's *Secure Tag*.

5) If the sender and a receiver *Secure Tag*s match, then the verification of the IP address will take place. Otherwise, if no match of *Secure Tag* is found the receiver will discard the NS message.
6) Upon successful matching of *Secure Tags*, the receiver will verify its obtained address with the new host target address.
7) If the match of duplicate IP address found, receiving node will reply with NA message appended with *Secure Tag* to sender. However, if the target address is found unique it creates an entry in its neighbor cache table in order to maintain and update the table for future communication.
8) Upon receiving the NA message, New Host will verify the NS message by matching the *Secure Tags*. If the match of *Secure Tag*s is found then it will extract the NS message and create an entry in neighbor cache table for future communication and perform new DAD process. However, if the mismatch of *Secure Tag*s is found, it will simply discard the message.

The whole process is illustrated in Figure 8, where a New-Host (Sender) and Existing-Host (Receiver) performs DAD process.

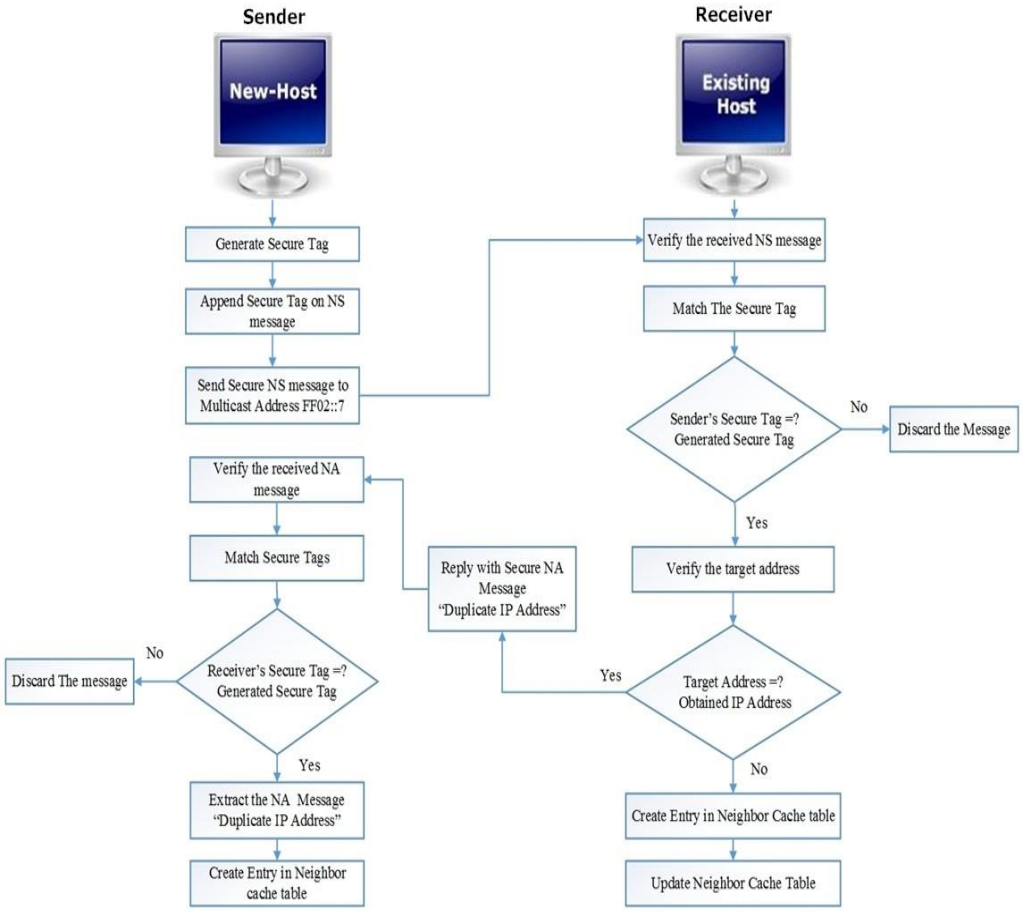

Figure 8. Secure Duplicate Address detection Process

7. Conclusion and Future Work

In this paper, the design of a new mechanism to prevent DoS attacks in DAD detection process was presented. This mechanism is expected to address the shortfalls of existing techniques and further improve DoS attacks on DAD process. This novel mechanism uses a secure tag option appended to NDP messages to maintain integrity between the sender and receiver during DAD process. The proposed DAD mechanism allows the hosts to verify the uniqueness of self-generated IP address while preventing malicious hosts to disrupt the verification process. Hence, new hosts are able to join the IPv6 network in the event of DoS attack. In order to test and evaluate the proposed mechanism in terms of effectiveness and performance, such as time and computation, the next step is to implement the proposed mechanism in a closed IPv6 network test-bed.

Acknowledgment

This research was supported by the Ministry of Higher Education Malaysia, in collaboration with the National Advanced IPv6 Centre, Universiti Sains Malaysia.

References

[1] S. U. Rehman and S. manickam, "Significance of Duplicate Address Detection Mechanism in Ipv6 and its Security Issues: A Survey", Indian Journal of Science and Technology, vol. 8, no. 30 **(2015)**, pp. 1-8.
[2] S. E. Deering, "Internet protocol version 6 (IPv6) specification", **(1998)**.
[3] S. Hagen, "IPv6 Essentials, O'Reilly: Second Edition", **(2006)**.
[4] N. Moore,"Optimistic duplicate address detection (DAD) for IPv6", **(2006)**.
[5] T. Narten, W.A. Simpson, E. Nordmark, and H. Soliman,"Neighbor discovery for IP version 6 (IPv6)", **(2007)**.
[6] A. Conta, and M. Gupta, "Internet control message protocol (icmpv6) for the internet protocol version 6 (ipv6) specification", **(2006)**.
[7] S.U. Rehman, and S.Manickam, "Integrated Framework to Detect and Mitigate Denial of Service (DoS) Attacks on Duplicate Address Detection Process in IPv6 Link Local Communication", International Journal of Security and Its Applications, vol.9, no.11 **(2015)**, pp.77-86.
[8] X.Yang, T. Ma, and Y. Shi,"Typical dos/ddos threats under ipv6 ",IEEE, **(2007)**, pp. 55-55.
[9] Supriyanto, I. H. Hasbullah, R. K. Murugesan, and S. Ramadass, "Survey of internet protocol version 6 link local communication security vulnerability and mitigation methods", IETE Technical Review, vol. 30, no. 1, **(2013)**, pp. 64-71.
[10] A. AlSa'deh, H. Rafiee, and C. Meinel, "IPv6 stateless address autoconfiguration: balancing between security, privacy and usability", Foundations and Practice of Security, Springer, **(2013)**, pp. 149-161.
[11] J. Arkko, J. Kempf, B. Zill, and P. Nikander, "Secure neighbor discovery (SEND)", (RFC 3971), March, **(2005)**.
[12] S. Chiu, and E. Gamess, "Easy-SEND: A Didactic Implementation of the Secure Neighbor Discovery Protocol for IPv6", **(2009)**.
[13] T. Narten, W.A. Simpson, E. Nordmark, and H. Soliman,"Neighbor discovery for IP version 6 (IPv6)", **(2007)**.
[14] R. K. Murugesan, and S. Ramadass, "REVIEW ON IPV6 SECURITY VULNERABILITY ISSUES AND MITIGATION METHODS", International Journal of Network Security & Its Applications, vol. 4, no. 6 **(2012)**.
[15] A. AlSa'deh, and C. Meinel, "Secure neighbor discovery: Review, challenges, perspectives, and recommendations", Security & Privacy, IEEE, vol.10, no. 4, **(2012)**, pp. 26-34.
[16] E. Nordmark, M. Bagnulo, and E. Abegnoli. "FCFS SAVI: First-Come, first-served source address validation improvement for locally assigned IPv6 addresses", (RFC 6620), **(2012)**.
[17] W. George, and T.W. Cable, "Enhanced Duplicate Address Detection", **(2015)**.
[18] B.G. Buchanan, and E.H Shortliffe, "Rule-based expert systems", Addison-Wesley Reading, MA, **(1984)**.
[19] J.A. Bernard, "Use of a rule-based system for process control", International Society for Optics and Photonics, **(1987)**, pp. 835-849.
[20] S. U. Rehman, and S. Manickam, "Rule-Based Mechanism to Detect Denial of Service (DoS) Attacks on Duplicate Address Detection Process in IPv6 Link Local Communication." 4th IEEE International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), IEEE **(2015)**, pp.1-6.

[21] V. Shoup, "On fast and provably secure message authentication based on universal hashing", in Advances in Cryptology—CRYPTO'96, Springer Berlin Heidelberg, January **(1996)**, pp. 313-328.
[22] T. Krovetz, "UMAC: Message authentication code using universal hashing", (RFC 4418), March, **(2006)**.
[23] Krawczyk, Hugo, Ran Canetti, and Mihir Bellare. "HMAC: Keyed-hashing for message authentication." (RFC 2104), January **(1997)**.

Authors

Shafiq Ul Rehman, He has B.Sc. degree in Computer Science and has received his M.Sc. degree in Network Technology & Management from Amity University (India) in 2012. He has worked on various research projects related to Network Security and Internet Technologies. Currently, he is a PhD research fellow in National Advanced IPv6 Centre (NAV6), Universiti Sains Malaysia (USM). His research interest includes: Networking, IPv6, Internet Security, Open Source Technology, Internet of Things (IoT), Ubiquitous Computing and Cloud Computing.

Selvakumar Manickam, He is the senior lecturer at National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia. He received his Bachelor of Computer Science and Master of Computer Science in 1999 and 2002, respectively. He obtained his Ph.D. from Universiti Sains Malaysia (USM) in 2013. His research interests are Internet security, cloud computing, Android and open source technology. He is an Executive Council member of Internet Society (ISOC), Malaysian Chapter and also the Head of Internet Security Working Group under Malaysian Research and Education Network (MyREN).