Denial of Service Attack on Neighbor Discovery Protocol Processes in the Network of IPv6 Link-Local

Ghaith Mousa Hamzah Amlak [1], Firas Qays Kamal [2], and Ahmed K. Al-Ani [3]
[1] General Directorate of Education Babylon, Ministry of Education Iraq, Babylon, Iraq
[2] General Directorate of Education Al Qadisiyah, Ministry of Education Iraq, Al Qadisiyah, Iraq
[3] National Advanced IPv6 Center (Nav6), Universiti Sains Malaysia 11800 USM, Penang, Malaysia
Email: Tammar2009ghaith@gmail.com; faris_qais2001@yahoo.com; ahmedkhallel91@nav6.usm.my

***Abstract*—Most devices are nowadays connected automatically via an IPv6 address. IPv6 was developed in 1998 so that the IPv4 address space issues are solved. Due to rapid technological advancements, i.e., the internet of things (IoT), IPv4 is no more efficiently functioning. Therefore, IPv6 introduced with a novel protocol, i.e., Neighbor Discovery Protocol (NDP). It involves many processes to facilitate the communication operation between nodes (hosts and router) that are located on the same link. NDP does not have any verification mechanism to validate the exchange messages, whether it comes from the legitimate or illegitimate node. Besides, the NDP messages are not secure by its design. Therefore, an attacker may manipulate these messages and perform attacks such as Denial of Service (DoS) attack which is considered a frequent attack that threatens the network of the NDP IPv6 link-local. We have reviewed in this paper the main processes of NDP and the security issues of these processes. In addition, the experiments result shown the NDP processes are completely vulnerable to the DoS attack. Thus, the future direction involves developing a prevention mechanism that aims at securing the NDP processes in the network of IPv6 link-local.**

***Index Terms*—DoS attack, IPv6 link-local network, NDP processes**

I. Introduction

Internet Engineering Task Force (IETF) announced that Internet Protocol version 4 (IPv4) would not be able to satisfy all Internet devices in 2020. Therefore, Internet Protocol version 6 (IPv6) [1] was proposed. IPv6 enjoys numerous features, which were unidentified in IPv4, e.g., it can provide the concept of "plug-and-play" in accordance with neighbour discovery protocol (NDP) [2]. Any novel host is allowed by NDP to create its IPv6 address when connecting to a specific network. It can perform more tasks along with a neighbor, as well as router discovery functions. These tasks are associated with diagnostics, as well as packets sending's error reporting [3].

The novel features work on enhancing the IPv6 network security, e.g., by adding a new security key named IPsec [4]. Nevertheless, IPv6, as a novel technology, remains vulnerable. IPv6 networks currently experience varied types of attacks like Denial-of-Service. DoS foils a specific legitimate node of using the network services, including web and e-mail services, as well as the Internet shopping service. Based on the National Vulnerability Database, most of the IPv6 attacks are the DoS attacks [5].

There are some survey papers discussed the security challenges of some of NDP processes, yet not all NDP processes covered and did not give a clear explanation what are the main requirements to secure NDP processes in IPv6 link-local network. Therefore, this paper reviewed the main process of NDP along with security issues during the attack of DoS in the network of IPv6 link-local and discussed the main requirements for securing NDP processes. In this paper, it is arranged into the following sections: NDP, with its processes, is explained in Section 2. DoS attack on NDP processes is illustrated in Section 3. Related work discussed in Section 4. Section 5 provides the experiment and the results. The conclusion and future directions are provided in Section 6.

II. Neighbor Discovery Protocol (NDP)

NDP comprises a specific messages' group, as well as procedures, which identify relationships among nodes (routers, as well as hosts) with their neighbors on a similar network. Several protocols that are utilized in IPv4 are substituted by NDP, including router discovery, address resolution protocol (ARP), and internet control message protocol (ICMP), as well as ICMP Redirect. Novel applications are provided by NDP, including DAD, as well as neighbor unreachability detection (NUD). In the same way, IPv6 NDP allows nodes to spot neighbors on the same LAN. Also, existence can be publicized to the existing neighbors [1]. One interesting aspect of IPv6 networks involves the nodes' capability of configuring their addresses automatically through stateless address auto-configuration (SLAAC) [2] without the deployment

Manuscript received September 23, 2019; revised November 5, 2019; accepted November 29, 2019.
Corresponding author: Ahmed K. Al-Ani (email: ahmedkhallel91 @nav6.usm.my).

doi: 10.18178/ijeetc.9.4.247-251

of a protocol of stateful configuration, that is, IPv6 dynamic host configuration protocol (DHCPv6). Power to an IPv6 host is provided by SLAAC so that link-local, as well as global addresses without manual intervention, can be generated [3]. There are five messages of ICMPv6, which are used by NDP, as shown in Fig. 1.

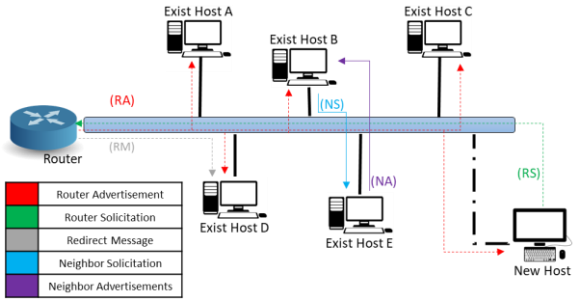

Fig. 1. NDP five messages.

A. Neighbor Discovery Protocol (NDP) Processes

There are many important processes, which are performed by NDP, to facilitate communication between nodes (hosts and routers). The most common processes of NDP are listed below:

1) Address Resolution (AR) process

In this case, a unicast packet is possessed by a specific node to be sent to a certain neighbor. However, it cannot recognize the link-layer address of the neighbor; it carries out address resolution, AR in short. The AR is executed by utilizing two NDP messages; in other words, neighbor solicitation (NS), as well as neighbor advertisement (NA) messages. For example, in case Host_A communicates or sends a packet of data to Host_B, then, Host_A must first inspect if the Media Access Control (MAC) of B exists in the cache or else the AR process must be conducted by Host_A. To this end, Host_A requires multicasting the message of NS to a solicited-node multicast address, i.e., (SNMA), depending on the last 24 bits of Host_B IP address. Host_B is asked to reply via the MAC address. The message of NS is received by all the hosts in the network of the local area, but only Host_B can provide the AR reply via the NA message that comprises its IP, as well as MAC addresses. Accordingly, after the reply is received, Host_A updates its own cache, then a packet of data is sent to Host_B based on the address of MAC in its cache.

2) Router Discovery (RD) process

When a novel host is there to join the network of IPv6 link-local, it needs to obtain some important information from the router such as the network prefix. For example, in case Host_A joins the network of IPv6, the router solicitation (RS) message will be multicast on the link, and the router exists of the link, i.e., Router_A will reply via the router advertisement (RA) message. Host_A will, therefore, use the RS message information to perform its connection to the IPv6 network [4].

3) Redirect process

In this process, when the router finds a better-hop node, which reaches a specific destination, it will send a redirect message (RM) message with the aim of informing the host.

4) Neighbor Unreachability Detection (NUD) process

This process is implemented when a host wants to recognize whether another host is reachable or not. There are two NDP messages that are used to perform this process, i.e., NS, as well as NA messages. For example, if Host_A requests to identify whether Host_B is still on the link or not, it will multicast NS messages on SNMA depending on the last 24-bits of Host_B targeting Host_B. In case Host_B exists and connects to the link, it will reply via NA messages. Receiving the NA message indicates that Host_B is reachable.

5) Duplicate Address Detection (DAD) process

Each host on the link must have an IP address, which is unique, that can be used to establish communication with the existing hosts. After the host generates a new IPv6 address, it should perform the DAD process with the aim of checking the generated IP address's uniqueness. For example, when Host_A aims at joining the network of IPv6 link-local, a novel IP address should be generated. After the IP address is generated, it needs to check whether it is unique. This means that there is not any other existing host, which uses the same generated IP address. This can be done by using the DAD process through multicasting NS messages on the SNMA address. When the IP address, which is generated, is already engaged by another existing host, i.e., Host_B, Host_B should reply via a message of NA and if it is received, this means that the generated address of IP cannot be unique and, therefore, a new IP address should be generated [5].

III. Denial of Service (DoS) Attack on NDP Process

The attack of DoS is characterized as a specific cyber-attack. In this attack, perpetrators seek to make the host or network resource inaccessible for the intended users by disrupting the services of the host temporarily connected to the Internet, or they are indefinitely connected. In general, the DoS attack can disturb the NDP process during the processes as shown in the scenarios below.

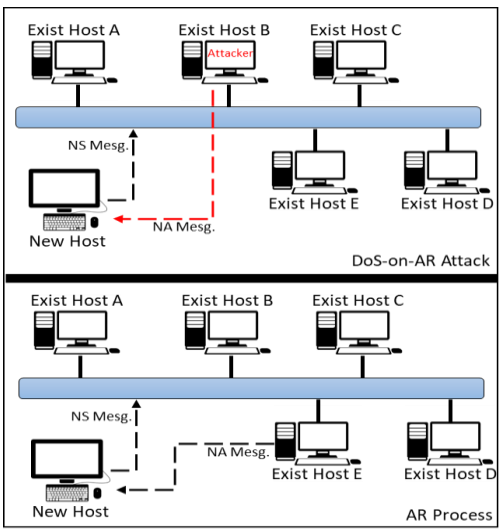

Fig. 2. DoS attack on the process of AR.

1) DoS attack on AR process

The AR is simple, and it is efficient. However, there are potential security risks. First, all the hosts on a similar IPv6 link are capable of joining the process of AR. Therefore, any of the malicious nodes, which are on the link, are capable of disrupting the AR process when a fake NA message is sent. This is because the NDP messages are, by design, unsecured. Second, a specific verification mechanism is lacking in the process of AR [6]. For example, in case the Host_A requires to establish communication with the Host_B, then the former will not be checking if the reply message of NA is a valid or a fake message. The neighbor cache table is updated by Host_A when the messages of NA are established with the address of MAC that is invalid. Such a process, therefore, makes available a convenient situation for the attack of DoS. Fig. 2 shows the attack of DoS on the process of AR in the network of IPv6 link-local.

2) DoS attack on RD process

RFC2461 [7] pointed out that when the Default Router List is empty, then the sender presumes that a destination is on the local link. Accordingly, a spoofed RA can be sent by the attacker with a Router Lifetime that is zero. In case of cheating the victim, it endeavors to send each packet directly instead of using the Router. When a destination is not on-link, then this packet will not be able to reach the real destination [8].

3) DoS attack on redirect process

It is used with the aim of sending packets for a specific destination to any address of the addresses of the link-layer on the link. The existing first-hop router's link-local address is used by attackers with the aim of sending the Redirect message to a host that is legitimate. The host aims to detect the message via the address of the link-local as this message is generated in the first-hop router and, therefore, the Redirect is accepted. During the whole time that the attacker reacts to probes from NUD to the address of the link-layer, then the packet towards a destination can be redirected [9].

4) DoS attack on NUD process

If the node of IPv6 is processing the NUD process, attackers can launch such an attack via sending an NA, which is fabricated. In case the neighbor cannot be reachable, it will cheat the detecting node, presuming that the neighbor can be accessible. A Man-in-the-Middle attack is, therefore, expected [10].

5) DoS attack on DAD process

If the stateless address autoconfiguration is processed, a node of IPv6 (i.e., the victim) makes the DAD process for a given address of IPv6 with the aim of checking whether the generated IP address is unique or not. Meanwhile, the attacker disguises as this address are used by the node (i.e., the IP address that is generated) and respond to the message of detection, which results in that the victim cannot normally obtain the address of IPv6 [11].

IV. Related Work

NDP considers the core of the IPv6 link-local network, which is including all the significant processes occurring in the IPv6 link-local network. Due to its importance, several attacks aimed to threat its processes, as shown in the previous section. Thus, there is a number of mechanisms proposed to secure NDP by utilizing either an agent to monitor the network behavior or add additional options to five NDP messages.

For example, SeND mechanism has been proposed by Arkko in 2005 [12] by adding four new options named cryptographically generated address (CGA) option to verify CGA senders, Rivest–Shamir–Adleman cryptosystem (RSA) signature option, which attaches a public key-based signature and time stamp and the Nonce option, which validates unsolicited advertisements that have been sent as responses to solicited messages to prevent replay attacks. Although SeND recommended by request for comment (RFC), however, SeND mechanism is facing high computational issues that led to consuming processing time, CPU, and memory that may permit the host prone to flooding attack (that cause the host to freeze during processing SeND messages).

Another study proposed a mechanism to monitor the network behavior and notify the admin if there is abnormal behavior, mechanism named is neighbor discovery protocol monitor (NDPmon) [13]. NDPmon is based on Arpwatch (software application) for IPv4 in terms of features but provides additional attack detection capabilities. Although NDPmon prevents the attacks launched by illegal users, the attacks inflicted by legal users are very difficult to detect. In addition, NDPmon can detect the attack but not prevent it.

Furthermore, additional researchers from Tsinghua University have proposed the source address validation architecture [14] addressing the security issues in NDP processes by binging the packet with the source IP address. SAVA is generally deployed at three network levels, namely, the inter-AS level, intra-AS level, and local subnet level. The study by [10] shows that SAVA is an ideal way to stop receiving spoofed packets from many network scopes, but their study did not examine other NDP vulnerabilities.

TABLE I: SUMMARY OF RELATED WORKS

Mechanism Name	Limitations
SeND	• It has a high computational cost, especially for the CGA and RSA options. • Unable to identify the CGA address that is utilised by the legitimate node. • Cannot utilise CGA for static address configuration. • Shows high complexity. • Increases the network overhead and bandwidth consumption.
NDPmon	• Unable to distinguish the normal and abnormal behaviour of <IP, MAC addresses>. • Encounters problems during the training phase. Requires database support to monitor network traffic. • Requires a third-party device to provide additional services. • Increases the deployment cost of the DAD process in an IPv6 network. • It can only detect attacks and not prevent them.
SAVA	• Shows high complexity. • Shows weaknesses against DoS-on-DAD attacks given its design.

Therefore, the most common proposed mechanisms still facing security issues to secure NDP processes. The summarizing of related work is listing in Table I.

V. DoS-on-NDP Experiment

In this section, the DoS attack is launched on each of the processes of NDP, including NUD, RD, DAD, etc. To successfully conduct the experiments, the necessary hardware and the software detailed specifications of the test-bed environment are illustrated in Table II and, as shown in Fig. 3.

Table II: Test-bed Environment

Item Name	CPU	Memory	Operating System
Host 1	Intel(R) Core (TM)2 CPU Q8400 @ 2.66GHz × 4	5.00 Gb	Windows 10 Pro
Host 2	Intel(R) Core (TM) i7-3770M CPU @ 3.40GHz × 8	8Gb	Ubuntu 16.04
Attacker	Intel(R) Core (TM) i7-2640M CPU @ 2. 30GHz × 4	4.00Gb	Ubuntu 16.04

Item Name	Type
Switch (SW)	Cisco Catalyst 2960 Fast Ethernet
Gateway Router (GW)	Cisco Router C7200

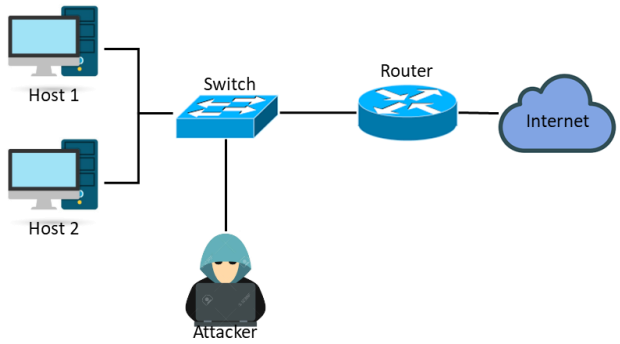

Fig. 3. Test-bed Environment.

The experiments were conducted with the aim of measuring the NDP processes' performance during the DoS attack. The scenarios of the conducted experiments were implemented via two tools: the dos-new-ipv6 attacker tool [15], in addition to the Scapy attacker tool [16]. They were repeated 20 times for each of the NDP processes. The equation (1) below is implemented to measure the ability of the NDP process in preventing the DoS attack [17]:

$$NDPSR = 1 - F/N \quad (1)$$

where NDPSR represents the NDP process success rate, N represents the number of NDP process times, and F signifies the NDP process times failed. According to the NDPSR's definition, it was found that if NDPSR is 1, this means that the attack is not successful. Nevertheless, if *NDPSR* is 0, this indicates that the NDP process can be susceptible to DoS.

Table III illustrates the experimental results of each of the NDP processes, including AR, NUD, RD, Redirect process, and DAD.

Table III: Experimental Results

NDP Process	Number of Experiments (N)	NDP Process Success	NDP Process Failure (F)	NDPSR
AR	20	0	20	0
NUD	20	0	20	0
RD	20	0	20	0
Redirect	20	0	20	0
DAD	20	0	20	0

Based on Table III, the results revealed that the NDP processes are completely vulnerable to the DoS attack. The main problems with the current NDP processes include (i) the five NDP messages are unsecured by design, (ii) all the nodes that are located on a similar link (including the attacker) are capable of joining any NDP process, and (iii) there is no verification mechanism, which can detect the originality of these exchange NDP messages during these processes. A new prevention mechanism is, therefore, necessary to secure NDP messages, which are used during the processes. The proposed mechanism should be able to verify the incoming messages. It should distinguish between legitimate messages and illegitimate ones on both sides, i.e., the sender and the receiver.

VI. Conclusion and Future Direction

IPv6 was introduced to overcome the IPv4 address space issues. It aims to provide better security through a new concept named NDP, which consists of many important processes such as AR, DAD, RD, etc. with the aim of facilitating communication between nodes (hosts and routers). However, all these processes experience security issues and are vulnerable to the DoS attack, which can disturb these processes. Furthermore, the experimental results revealed that the processes of NDP are vulnerable to the DoS attack. Therefore, a new mechanism should be introduced to secure the NDP process through securing the NDP messages and adding security verification to verify the originality of the NDP messages, whether these messages come from the legitimate or the illegitimate node and that is our future direction.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Ghaith Mousa Hamzah Amlak and Firas Qays Kamal conducted the research. Ahmed K. Al-Ani carried out the experiment and analyzed the results. Ghaith Mousa Hamzah Amlak and Firas Qays Kamal wrote the manuscript with support from Ahmed K. Al-Ani. All authors had approved the final version.

References

[1] O. E. Elejla, M. Anbar, and B. Belaton, "ICMPv6-based DoS and DDoS attacks and defense mechanisms," *IETE Technical Review*, vol. 34, no. 4, pp. 390-407, 2017.

[2] T. Narten, R. Draves, and S. Krishnan. (2007). Privacy extensions for stateless address autoconfiguration in IPv6. No. RFC 4941. [Online]. Available: https://tools.ietf.org/html/rfc4941

[3] A. Al-Ani, M. Anbar, I. H. Hasbullah, R. Abdullah, and A. K. Al-Ani, "Authentication and privacy approach for DHCPv6," *IEEE Access*, vol. 7, pp. 73144-73156, 2019.

[4] F. Najjar, M. Kadhum, and H. El-Taj, "Neighbor discovery protocol anomaly detection using finite state machine and strict anomaly detection," in *Proc. 4th Int. Conf. on Internet Applications, Protocols and Services*, 2015, pp. 978-967.

[5] A. K. Al-Ani, M. Anbar, S. Manickam, and A. Al-Ani, "DAD-match; Security technique to prevent denial of service attack on duplicate address detection process In IPv6 link-local network," *PloS one*, vol. 14, no. 4, 2019.

[6] A. K. Al-Ani, M. Anbar, S. Manickam, A. Al-Ani, and Y. B. Leau, "Preventing denial of service attacks on address resolution in IPv6 link-local network: AR-match security technique," in *Computational Science and Technology*, R. Alfred, Y. Lim, A. Ibrahim, and P. Anthony, Ed. Singapore: Springer, 2019, pp. 305-314.

[7] S. Deering and R. Hinden, Internet Protocol, version 6 (IPv6) Specification. Internet Engineering Task Force, No. RFC 2460, 1998.

[8] O. E. Elejla, M. Anbar, and B. Belaton, "ICMPv6-based DoS and DDoS attacks and defense mechanisms," *IETE Technical Review*, vol. 34, no. 4, pp. 390-407, 2017..

[9] A. K. Al-Ani, M. Anbar, S. Manickam, C. Y. Wey, Y. B. Leau, and A. Al-Ani, "Detection and defense mechanisms on duplicate address detection process in IPv6 link-local network: A survey on limitations and requirements," *Arabian Journal for Science and Engineering*, vol. 44, no. 4, pp. 3745–3763, 2018.

[10] S. Praptodiyono, I. H. Hasbullah, M. M. Kadhum, C. Y. Wey, R. K. Murugesan, and A. Osman, "Securing duplicate address detection on IPv6 using distributed trust mechanism," *International Journal of Simulation--Systems, Science & Technology*, vol. 17, no. 26, pp. 3.1-3.9, 2016.

[11] A. El Ksimi and C. Leghris, "Towards a new algorithm to optimize IPv6 neighbor discovery security for small objects networks," *Security and Communication Networks*, 2018.

[12] J. Arkko, J. Kempf, B. Zill, and P. Nikander, Secure Neighbor Discovery (SEND), No. RFC 3971, 2015.

[13] F. Beck, T. Cholez, O. Festor, and I. Chrisment, "Monitoring the neighbor discovery protocol," in *Proc. International Multi-Conference on Computing in the Global Information Technology*, 2007, pp. 57-57.

[14] J. Wu, G. Ren, and X. Li, "Source address validation: Architecture and protocol design," in *Proc. IEEE International Conference on Network Protocols*, 2007, pp. 276-283.

[15] T. H. C. Van Hauser. (2006). Attacking the IPv6 protocol suite. [Online]. Available: https://pacsec.jp/psj05/psj05-vanhauser-en.pdf.

[16] P. Biondi. (2014). Scapy-Packet Manipulation Tool.

[17] G. Song and Z. Ji, "Novel duplicate address detection with hash function," *PloS One*, vol. 11, no. 3, Mar. 2016.

Ghaith Mousa Hamzah Amlak was born in Babel Province, Iraq, in 1984. He received the bachelor's degree in computer science from Babylon university, Iraq, in 2007. and M.Sc. Information Systems from Osmania University, India, in 2016. Currently, he is an assistant lecturer at the Directorate General of Education Babylon, Iraq. His research interests include data mining, big data, Networks and cloud computing.

Firas Qays Kamal was born in Al Qadisiyah Province, Iraq, in 1986. He received the bachelor's degree in computer science from Al Qadisiyah university, Iraq, in 2007. and M.Sc. Information Systems from Osmania University, India, in 2016. Currently, he is an assistant lecturer at the Directorate General of Education AL Qadisiyah, Iraq. His research interests include data mining, big data, Networks and cloud computing.

Ahmed K. Al-Ani is a computer engineer. Received his B.S. degree in Computer Technique Engineering in 2013 from University of Al-Ma'mun and MSc. in information technology from Universiti Utara Malaysia (UUM) in 2016. Currently, he is a Ph.D. candidate at the National Advanced IPv6 Center (NAv6), Universiti Sains Malaysia (USM), 11800 Gelugor, Penang, Malaysia. His research interests include Computer Network Security, Internet Security, Network Communication Protocols (IPv6), and IPv6 Security.