International Journal on Advanced Science Engineering Information Technology

Vol.8 (2018) No. 5
ISSN: 2088-5334

Denial of Service Attack over Secure Neighbor Discovery (SeND)

Amjed Sid Ahmed[#], Rosilah Hassan[*], Nor Effendy Othman[*]

[#]*Faculty of Information and Communication Technology, Limkokwing University of Creative Technology, 63000 Cyberjaya, Malaysia.*
E-mail: amjed.sidahmed@limkokwing.edu.my

[*]*Center for Software Technology and Management, Faculty of Information Science and Technology,*
Universiti Kebangsaan Malaysia, 43600, Bangi, Selangor, Malaysia.
E-mail: rosilah@ukm.edu.my, effendy@ukm.edu.my

***Abstract*—IPv6, the Internet Protocol suite version 6, uses a Neighbor Discovery Protocol (NDP). NDP mainly replaces router discovery and the Address Resolution Protocol (ARP) and after that redirects the functions used in IPv4, i.e. the Internet Protocol suite version 4. The NDP system is a stateless protocol since it does not need the dynamic host's configuration protocol server to enable the various IPv6 nodes for determining the connected hosts along with the IPv6 network routers. To add layers of protection to NDP, the SeND (Secure Neighbor Discovery) extension was developed, which provides router authorization, proof of address ownership, and message protection for the protocol. SeND employs CGAs (Cryptographically Generated Addresses) and X.509 certificates. Despite its many advantages, deploying SeND is not easy, and it is still vulnerable to specific DoS (Denial-of-Service) attacks. The components of SeND and its responses to NDP threats are further elaborated in this paper. Also, an overview of the implementation of SeND, its limitations, existing vulnerabilities, and current deployment challenges are also presented. Furthermore, to test the performance of SeND under a DoS attack, a test bed was implemented, and the results discussed.**

***Keywords*—DoS; IPv6; NDP; SLAAC; Denial of Service; Neighbor Discovery Protocol.**

I. Introduction

In the age of the Internet today, the existing Internet Protocol, IPv4, is faced with issues of scalability and space limitation of IP addresses as well as security. To address these issues, a new protocol was developed to supersede IPv4, called IPv6. The Neighbor Discovery Protocol, NDP, provides IPv6 with a Stateless Address Autoconfiguration (SLAAC) service and is a core protocol of the IPv6 suite [1]-[4]. There are many critical functions of NDP including identifying physical addresses, detecting duplicate addresses, discovering nodes that are found within the same subnet, providing active neighbors with reachability information about paths, and discovering routers. Additionally, NDP enables mobile nodes to join with foreign networks, especially important in mobile IPv6, as it eliminates the need for foreign agents. Despite its many advantages, since it is assumed that every node in a link trusts the other, NDP is greatly susceptible to severe attacks. Nevertheless, there are instances where this assumption does not hold true, such as when wireless networks are utilized [5]. Malicious users can forge NDP messages by pretending to be legitimate nodes with the intention of attacking the protocol [6]. As a solution, a new standard—the RFC 3971, SeND—was developed by the IETF (Internet Engineer Task Force) [7]. An X.509 certification, digital signature, and cryptographically generated address (CGA) are the measures that SeND uses to protect NDP. SeND was designed such that replay attacks and IPv6 address thefts are prevented, message integrity is ensured, and the router authority verified. Despite it being a potential approach for protecting NDP and making IPv6 a safer protocol, SeND is difficult to deploy. This is because network device manufacturers and operating system developers have not yet implemented SeND to the point that it has reached maturity. Besides that, SeND is vulnerable to DoS attacks and consumes high bandwidth, besides being computationally intensive.

II. Material And Method

A. Neighbor Discovery Protocol

ICMP Redirect, Internet Control Message Protocol (ICMP) Router Discovery and ARP are integrated to develop a single protocol—IPv6 NDP. The five ICMPv6 control messages—Router Solicitation, Router Advertisements, Neighbor Solicitation, Neighbor Advertisement, and Redirect—are the

basis for most of the core functionalities of NDP [8]. The definitions of these messages are as follows:

1) Redirect: A message sent from routers to alert hosts of better first-hop destinations.

2) Neighbor Advertisement: A message sent from hosts to assist in link-layer address changes or as a Neighbor Solicitation reply.

3) Neighbour Solicitation: Requests sent from IPv6 hosts *to* verify that a node is still reachable or to determine the link layer address of a neighbor.

4) *Router Advertisements:* Responses or messages, which serve as advertisements for the local link prefix and several other options, sent from routers to Router Solicitation.

5) Router Solicitation: Router Advertisement request sent from hosts.

There are two categories of NDP functionalities, which involve host-to-host and host-to-router functionalities [9]. Host-host functionalities determine direct host reachability, IP destination address of the datagram, Duplicate Address Detection (DAD), and Neighbor Unreachability Detection (NUD) or determination based on the address resolution, if a selected address is already present in the link-local network, as a basis for determining the next hop. Meanwhile, host-router functionalities allow the host to differentiate between the remote networks and link local network and auto-configure their IPv6 address based on the router's provided information, in addition to finding routers on the link-local network and determining the parameters of the neighboring routers and local link network. [10].

There are 5 categories of NDP messages, i.e., Redirect (ICMPv6 number 137); Neighbor Advertisement (NA, ICMPv6 number 136); Neighbor Solicitation (NS, ICMPv6, number 135); Router Advertisement (RA, ICMPv6, number 134); and Router Solicitation (RS, ICMPv6, number 133). All these categories will become operational after the ICMPv6 message structure and format is applied.

1) Router Solicitation: The main idea behind the application of RS messages is to allow the nodes that were present within a specific subset to investigate the presence of the IPv6 routers, which are connected to the subnet. A multicast message, which is transmitted by the hosts, is presented in the link in the form of an immediate response to the RA unicast message.

2) Router Advertisement: When the IPv6 routers pseudo-periodically transmit some unsolicited RA messages (if the link consists of several other advertising routers), synchronization issues that arise are decreased after randomizing the interval present between the unsolicited advertisements. After receiving an RS message, the routers also transmit some solicited Router Advertisement messages. The data, which is required by the hosts, is present in these RA messages and helps them to understand the link prefixes, link MTU, particular routes, a lifetime of the addresses generated after auto-configuration, and also determine whether or not the address auto-configuration system has to be applied.

3) Neighbor Solicitation: For verifying a previously generated physical address or for discovering the physical address of an on-link IPv6 node, the IPv6 nodes transmit the NS messages, which generally include the sender's link-layer address. If the neighboring node's reachability needs to be verified, the general NS messages are unicast; however, for resolving the address-related issues, they are multicast.

4) Neighbor Advertisement: As a response to the transmitted NS messages, the IPv6 nodes transmit an NA message. Different nodes can transmit this unsolicited NA message. In this way, the changes that occur in the link-layer addresses or in the role that the nodes play are relayed to the neighboring nodes. After that, the information needed by the nodes, which includes the transmitter's link-layer address and the role played by the sender within the network, is stored by the nodes.

5) Redirect: The initiating node is notified about the first-hop address for a particular destination once the IPv6 router sends a redirect message. Only the routers can transmit redirect messages as unicast traffic. Furthermore, only the hosts can process the messages, which are unicast for the primary hosts.

The local network security could potentially be broken with the utilization of NDP, which is insecure by default [11]. NDP has vast scope, so although it has basic protection mechanisms to some extent, it still requires additional conditions that must be fulfilled. These include a hop limit of 255, a source address that must be a link-local address, and NDP messages sent from routers should not go beyond the layer in which 2 access networks are directly connected. Even if all these conditions were fulfilled, it will still not be enough to protect the local networks in IPv6 completely. An insecure NDP would be vulnerable to attacks of different kinds such as Rogue routing information attacks, spoofing attacks, or Replay, DoS, and Redirect attacks [12]. These probable attacks are described and categorized in RFC3756. To exacerbate the issue, there is even a toolset that was developed to attack IPv6, called the Hacker's Choice IPv6 (THC-lPv6). The many attacks targeted towards NDP are further described in the following sections:

1) Spoofing Attack: This attack involves an attacking node that gains unauthorized access by making use of the address or identifier of another node [13]. This attack could also give rise to different attacks such as DoS and MITM (Man-In-The-Middle) attacks. In short, if the IPv6 does not have an authentication mechanism in place, it will be open to malicious node attacks, which use spoofed source addresses to generate spoofed IPv6 packets [14].

2) DoS (Denial-of-Service) Attack: When an attacking node prevents a legitimate node from communicating with another node attached to the link by using up computer resources, this is called a Denial-of-Service attack. In this attack, the attacker aims to prevent a network node from acquiring a network address by generating the DoS on DAD (Duplicate Address Detection) [15]. DAD is used to ensure that addresses in the same link do not collide. Also, a legitimate host might be prevented from obtaining a new IPv6 address as a result of a malicious node. The malicious node uses a spoofed message stating that it has the address in answer to every DAD attempt. Consequently, the victim will fail to access the network or configure an IP address because

every attempt to generate a new valid IPv6 will not pass the address collision check successfully [16].

3) Replay Attack: In this type of attack, the victim is given fake replies by malicious nodes that silently capture transmitted messages. The attacker changes a captured message transmitted between two nodes. For instance, this attack could occur when Host B tries to communicate with Host A, where, to obtain the physical address of Host B, Host A transmits a Neighbour Solicitation message [17].

4) Redirect Attack: This attack prevents the legitimate receiver from receiving a packet, by redirecting it to a further away node. The attacker could assume the role of the legitimate router and take charge of the routing as well as generate fake router redirect messages. Because this attack intercepts every message exchanged between two nodes, it could also act as a MITM attack [18].

5) Rogue Router Attack: This attack involves the rerouting of traffic via insertion of rogue information by a malicious node. As a result, the victim would not be able to access the desired network and the routing tables will be infected. In other words, the malicious node acts as a router and transmits a fake address prefix. This attack is very severe because all joined nodes within the same subnet will also be affected [19]. In fact, an expert attacker sometimes mixes between the threats mentioned above—such as DoS and spoofing—in order to strengthen the attack and make it more difficult to detect, in addition to producing packets with a fake source address to conceal his identity.

B. Secure Neighbor Discovery

As a response to defend against NDP attacks, the IETF SeND working group released the first specifications of SeND in 2002. SeND is not a new standalone protocol, but rather agreed upon enhancements for NDP, which include three additional features as an extension to the NDP i.e. a mechanism for router authorization, address ownership proof, and message protection. TABLE I summarizes the actual NDP attacks and corresponding SeND responses to overcome these attacks. Fig. 1 outlines the features and components of SeND including RSA signature, CGA, Timestamp, and Nonce. Also, to secure the process of router authorization, SeND added two new ICMPv messages—Certificate Path Solicitation and Certificate Path Advertisement [20].

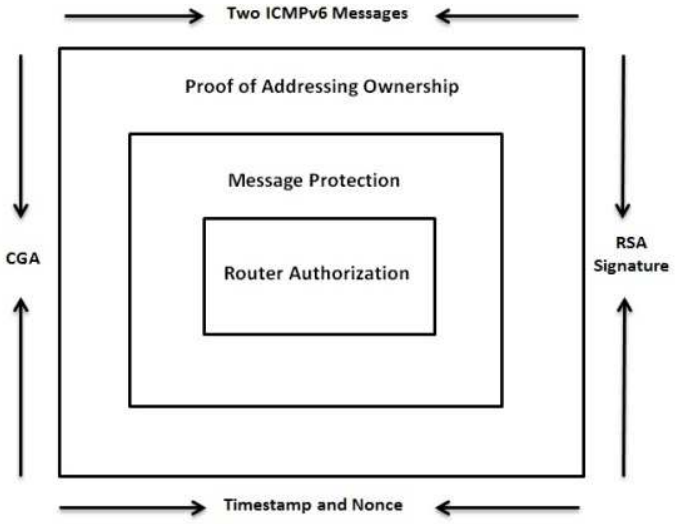

Fig. 1 The Components and Functions of SeND

SeND is based on CGA, which was created to prevent theft of addresses. The main idea behind the application of the CGA system is the use of asymmetric cryptography for authenticating the IPv6 auto-configuration addresses without altering the SLAAC 0-configuration paradigms. IDentifiers (IIDs) that can be generated by the 1-way hashing of public keys of nodes and other such auxiliary parameters are what make up the CGAs, which are also IPv6 addresses. In short, the node's public key is associated with its IPv6 address. This can be verified after recalculating the hash values and comparing them to the IID values of the transmitter's address. The general CGA system estimates two independent 1-way hash values (i.e., Hash1 and Hash2). The estimation of the Hash2 (112-bit) values establishes an input parameter for calculating the Hash1 (64-bit) value. The Hash2 value is seen to increase the costs and computing time for hackers when they attempt to carry out a brute-force attack. However, it does not increase the Hash 2 output value length. The Hash 2 value has been described in the IID section of the IPv6 node's address. Also, a scaling factor, i.e., the Security Parameter (Sec), assists in maintaining the security for each generated address. Sec refers to an unsigned 3-bit integer, which has a value ranging between 0 and 7, wherein a value of 0 indicates the lowest security while a value of 7 refers to the highest security [7]. TABLE II presents the CGA parameters, the data structure, and the CGA generating notations.

SP, K_pub, m, and Sec are the input values that the CGA generation algorithm uses. The CGA address is output by the CGA algorithm. Before obtaining the output, the appropriate Sec value must first be used and the public key of the address owner established. Then, the Final Modifier is assessed and established by the Hash2 computation loop. The value of the 16*Sec-leftmost bits of Hash2 must be 0, a requirement that the Modifier must be able to satisfy.

The concatenation of (64 + 8) 0 bits and combination of m and K_pub values will result in the Hash2 value. The system will terminate the calculation of the Hash2 loop when the address generator finds a suitable match.

TABLE I
RESPONSES OF SEND TO THE NDP THREATS

Neighbor Discovery Protocol Attack	Spoofing of Neighbor Solicitation/Advertisement Messages	Failure of Neighbor Unreachably Detection	Denial of Service for Duplicate Address Detection Procedure	Router Solicitation/Advertisement Messages Attacks	Replay Attacks
Secure Neighbor Discovery Responses	The RSA Signature and CGA options are employed.	RSA Signature option should be included in every Probe of Neighbor Solicitation messages.	Each Neighbor Advertisement message related to a DAD procedure must include an RSA Signature option	Router Advertisement Messages must include an RSA Signature within their messages	Timestamp and nonce option must be used within every single solicitation message.

The Hash1 computation utilizes the saved value of the Final Modifier. The process of generating the CGA is outlined in Fig. 2.

TABLE II
CGA GENERATION NOTATIONS

Notation	Length
SP	64-bit
m	128-bit
CC	8-bit
sec	3-bit
u, g	1-bit each
IID	64-bit
K_pub	Variable
K_priv	Variable
Sign	Variable

The value of Hash1 represents a hash that is generated out of the CGA Parameters Data Structure. Using the Hash1 value, IID was produced. It then truncates the gained value of the Hash to the suitable length (64-bit) and encodes the three leftmost bits of IID into a Sec value. From the leftmost bits of IID, the 7th and 8th (u and g) bits are set aside and are also set to "1" to signify that it represents the CGA address. Then, the CGA Parameters Data Structure's Hash output is spread throughout other 59 bits of the IID (2). The combination of the (64-bit leftmost bits) for SP with the IID part, forms the final complete address of Internet Protocol version 6 (3). Lastly, a DAD process is carried out with the produced address to check against address collision within the same local link. In the event of an address conflict, the CC has to be incremented and the Hash1 procedure has to be performed again until a valid address is obtained or the CC value becomes 2. For validation, the binding between CGA and public key CGA Parameter Data Structure is associated with the CGA option. To affirm the generated address ownership, the owner of the address will make use of a private key to sign messages that are transmitted from that address. For the purpose of authenticating the identity of the sender, SeND utilizes the RSA Signature Option. It can also help prevent spoofing attacks on the CGA addresses.

$$CGA\ parameter = (SP, K\_pub, sec, m) \quad (1)$$

$$IID(64) = hash(CGA\ parameter) \quad (2)$$

$$CGA(128) = SP(64) \| IID(64) \quad (3)$$

The verification of CGA inputs the CGA Parameter Data Structure and IPv6 address. An indicator of a successful verification process is that the verifying node will recognize that the address fits with the public key. Subsequently, messages coming and going from the real address owner can be authenticated once the verifier utilizes the public key. Fig. 3 illustrates this process in more detail.

By utilizing SeND, the solicitation message will also have a Nonce Option. This matching option is required for all advertised messages. In this way, a solicitation message that a node has previously sent could be certified as a new response/replay. In short, this option prevents replay attacks, but it only applies for two-way RS/RA communications involving NS/NA, and not for one-way communication messages. To protect against replay attacks involving advertisements that are unwanted such as periodic Router Advertisements and Redirect messages, SeND utilizes the Timestamp Option. This way, it is assumed that all nodes are equipped with synchronized clocks and can, therefore, implement a Timestamp checking algorithm to avoid Replay attacks.

For IPv6 address authentication, a combination of the CGA and RSA Options are used. The address authentication proves that the person owning the specific address is the true owner of the subsequent pair of asymmetric keys. SeND uses a process known as Authentication Delegation Discovery (ADD) in which some third-party services are utilized for router authorization and for authorizing and validating default gateways for IPv6 routers. ADD can also be applied for specifying the IPv6 prefixes that the specific router is authorized to relay on the whole link. This process can be carried out using 2 new types of ICMPv6 messages, i.e. CPA and CPS.

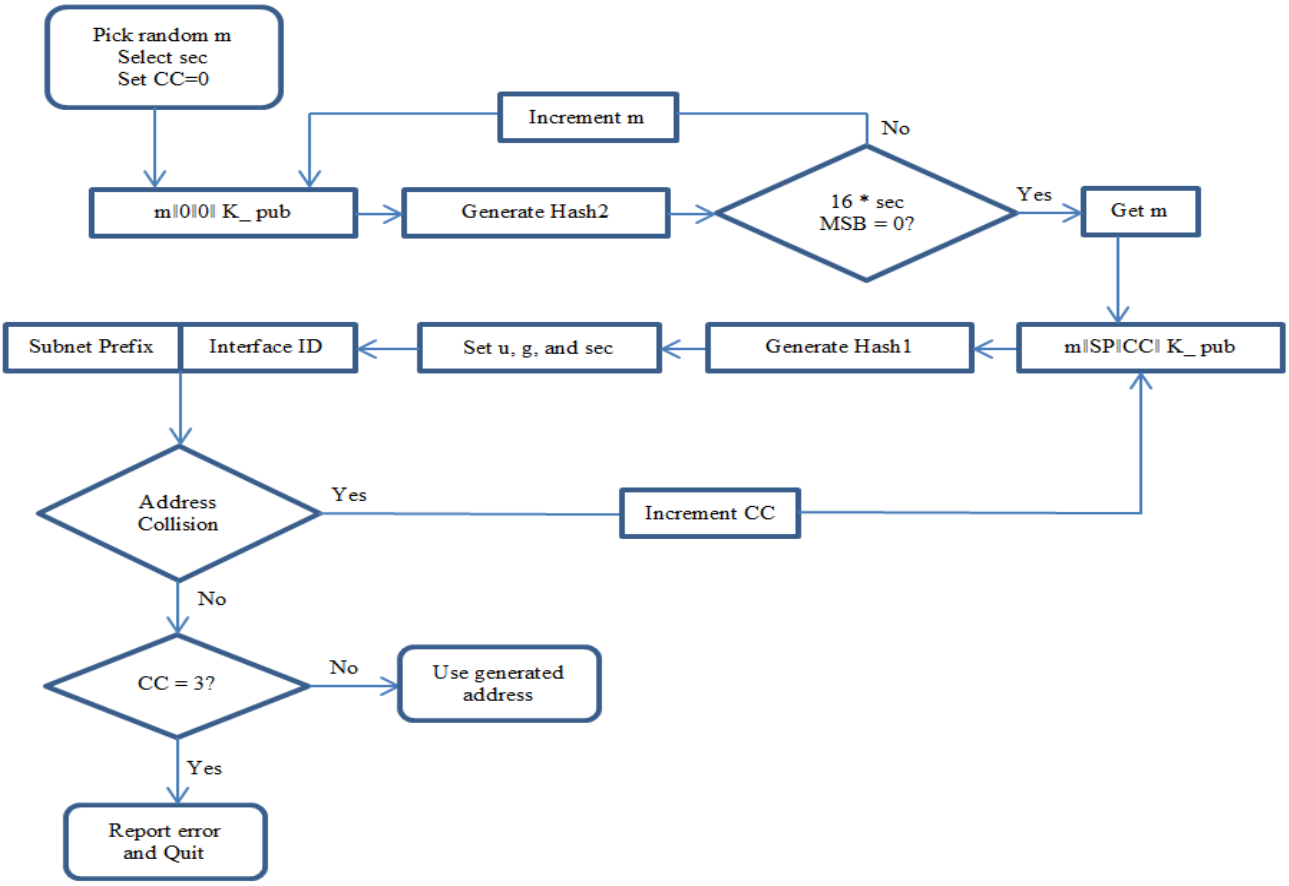

Fig. 2 CGA Generation Flow

```
1   Procedure VerifyCGA (CC, SP, K_pub, IID, CGA)
2   IF CC > 2 orCGA[0:8] ≠ SP:
3   Return False
4   End IF
5    Concat := concatenate (m,SP,CC,K_pub)
6   Digest := SHA1(Concat)
7   Hash1:= Digest [0:8]
8   Hash1[0] := Hash1[0]
9   IID:= CGA [8:16]
10   IID [0] := IID [0]
11  IFHash1 ≠ IID:
12   Return False
13  End IF
```

Fig. 3 The Pseudo Code used in CGA Verification

To request certification between a host's trust anchor and router, nodes send a message during the ADD procedure called CPS. In response to CPS, another message that also contains the router certificate and is ICMPv6 type 149 is transmitted. This message is known as CPA.

Although SeND provides promising security measures for protecting NDP messages, its deployment, computation requirement, and security in systems are still lacking. This could result in increased susceptibility of NDP messages to attacks. Therefore, the researcher described the different challenges and drawbacks of the SeND process in the following section to discuss this issue further.

Although SeND can prevent the theft of node addresses, the real node identity cannot be guaranteed. Furthermore, SeND is unable to confirm whether or not the proper node had used the CGA address. This case of unverified CGA allows hackers to use their public key to generate a novel and valid address as well as initiate the necessary communication process. In this way, an attacker could use a valid public key to mimic a node address; however, since the attacker does not have a private key, he will not be able to assume the address of the existing host. The SeND system is highly vulnerable to DoS attacks. The processes of SeND that are most vulnerable are the DAD check, CGA parameter verification process, and specific steps of the CGA verification process, where the attacker blocks the connection from a new CGA node to the link. The attackers target the hosts by transmitting many pointless certification paths, which force the hosts to use a lot of useless verification resources and memory on the paths. Furthermore, the CGAs can barely withstand TMTO (Time-Memory Trade-Off) attacks [21].

The CGA process requires massive computational complexity, so it could be possible that after the node has developed a suitable CGA process, it could go on applying the process at the subnet. This indicates that the main weak spot of the nodes, which still apply the CGAs, are attacks related to privacy [21].

A technique is known as the hash extension, and considered as the safety constraint Sec, is used in the CGA process. When this factor is applied, the various bits that are linearly incorporated into the hash extension technique will

be stabilized. This affects the average generation time for a CGA address that depends on the Sec-bit setting. In the SeND system, every node must include public keys and similar significant parameters in its message and also attach a signature to each of the generated data packets. This results in the consumption of available bandwidth as a result of increased communication overhead from the addition of more than 1 Kb data to each data packet [7].

Even to this day, there is a lack of awareness regarding the implementation of the SeND technique. The majority of computing systems support NDP; however, they are unable to support the SeND technique. Although the routers developed by major tech giants such as Juniper and Cisco provide some support for the SeND technique, most operating systems are unable to support the SeND process [21]. The researcher has therefore described the current application of this technique and presented the limitations of every process in this paper.

III. Results And Discussion

To launch a DoS attack against SeND, a small test bed with four computers, a switch, and a router were used. The computers contain two victim nodes (Windows 10 Home and Ubuntu 16.04 respectively) and one attacking node (Kali Linux 3.20.2), as per the topology in Fig 4. One computer (Windows 8) is used to monitor the network traffic during the attack. THC-IPv6 attacking tools were used to implement the DoS attack, and the sendpees6 command was used.

A built-in tool and resource monitor bundled with the Windows operating system was used. This allows the users to observe the processor utilization, hard disk, network, and memory usage. For Linux-based systems, the same tool is also available, but under the name system monitor.

To monitor the CPU usage for Ubuntu 16.04 and Windows 10, in the experiment, a system monitor and a resource monitor were used, respectively, for 60 seconds. The role of each node and its software and hardware specifications are outlined in TABLE III.

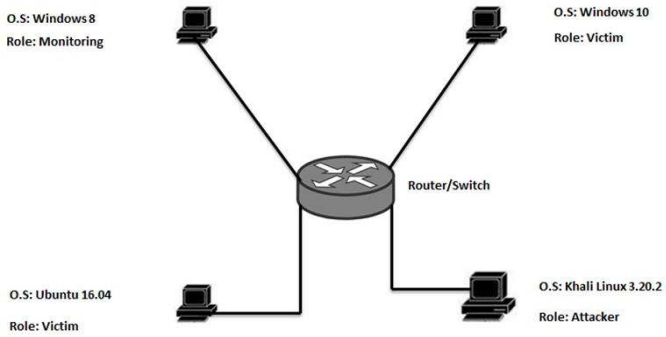

Fig. 4 Test Bed Topology

To evaluate the impact of a DoS attack, two performance metrics, network bandwidth consumption and processor utilization, were used. Previous works indicate that although SeND has been implemented in both Linux and Windows, DoS attacks still occur. Fig. 5 and Fig. 8 show that Windows is more vulnerable to DoS attacks compared to Linux. For both metrics selected, both Figures 5 and 8 show a significant impact on performance.

IV. Conclusions

The use of Internet facilities in Public areas is a matter of growing concern, as many users do not trust Public Internet services. Due to the problems occurring in the current Internet processes, NDPs are susceptible to many network-based attacks. Furthermore, defense mechanisms such as SeND could also give rise to DDoS- or DoS-related attacks. SeND is an industry-level process, which can adequately secure the NDPs. However, the SeND technique, in itself, is susceptible to some DoS attacks. Additionally, higher computational costs and a lack of deployment make the SeND technique quite unreliable. In this paper, the researchers addressed the various SeND functions and components. An experiment for establishing the limitations of the SeND technique was carried out, and the challenges and problems are affecting the implementation of the SeND technique addressed. The results show that the DoS attacks against the SeND technique could significantly affect IPv6 network operations. Finally, it is concluded that further research must be carried out and more solutions must be generated for developing secure NDPs and SeND processes.

TABLE III
Computer Roles, Software, and Hardware Specifications

Node Role	Operating System	IP Address	MAC Address	Hardware
Victim	Windows 10	FE80::1	A4:1F:72:5B:73 :A2	Intel Pentium G645 2.90 GHz processor. 2.00 GB RAM Memory.
Monitoring	Windows 8	FE80::2	74:27:EA:0D:8 9:10	Intel Core i5 3.00 GHz Processor. 4.00 GB RAM Memory.
Victim	Ubuntu 16.04	FE80::3	00:1D:92:01:06 :F4	Intel Core 2 Duo E4500 2.20 GHz processor. 2.00 GB RAM Memory.
Attacker	Kali Linux 3.20.2	FE80::4	00:1E:33:3A:D 3:9D	Intel Pentium Dual T2390 1.86 GHz processor. 2.00 GB RAM Memory.

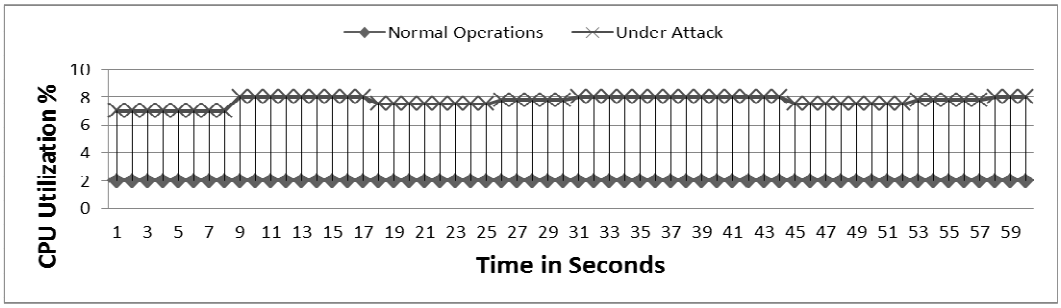

Fig. 5 Windows 10 Home Processor Consumption Before and During DoS Attack on SeND

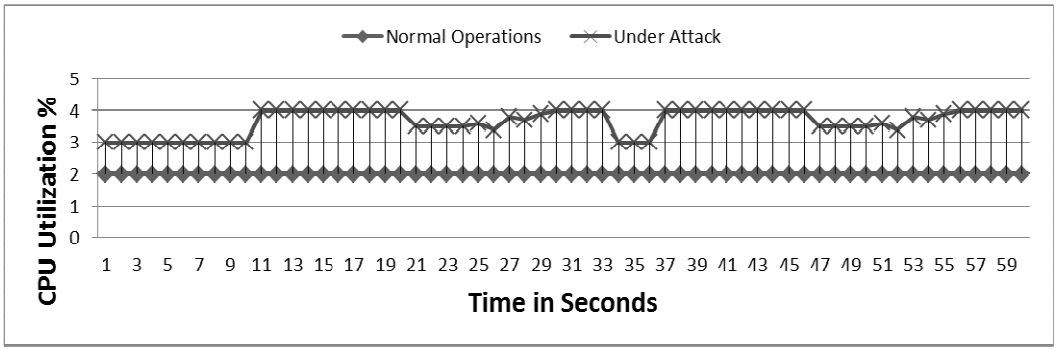

Fig. 6 Ubuntu 16.04 Processor Consumption Before and During DoS Attack on SeND

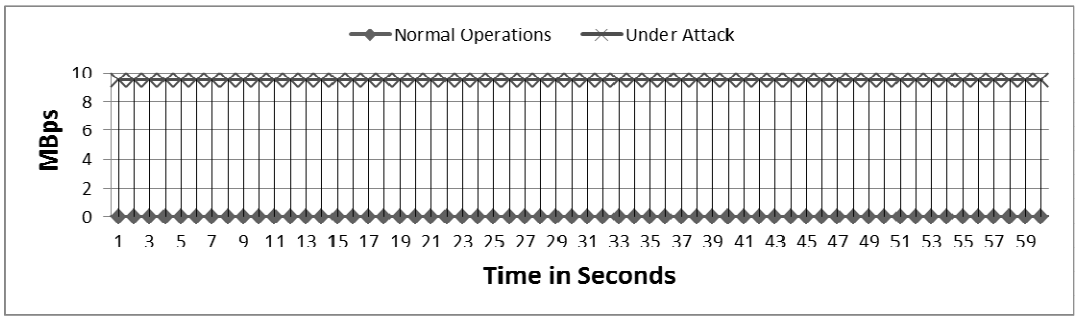

Fig. 7 Windows 10 Home Bandwidth Consumption Before and During DoS Attack on SeND

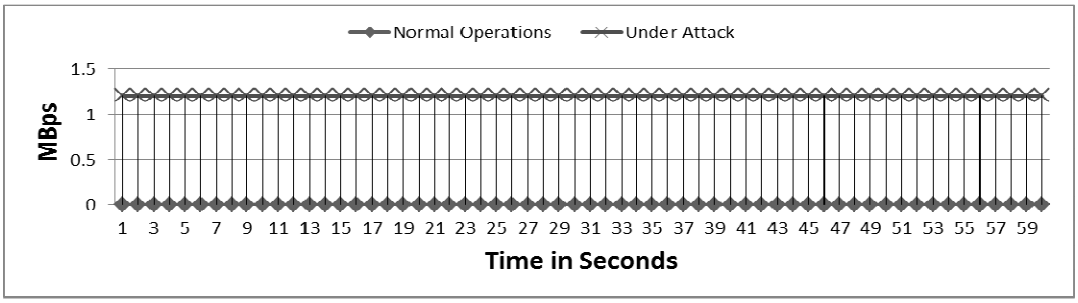

Fig. 8 Ubuntu 16.04 Bandwidth Consumption Before and During DoS Attack on SeND

REFERENCES

[1] G. Song and Z. Ji, "Novel Duplicate Address Detection with Hash Function," *Plos One*, vol. 11, no. 3, 2016.

[2] S. U. Rehman and S. Manickam, "Novel Mechanism to Prevent Denial of Service (DoS) Attacks in IPv6 Duplicate Address Detection Process," *International Journal of Security and Its Applications*, vol. 10, no. 4, pp. 143–154, 2016.

[3] M. Anbar, R. Abdullah, R. M. A. Saad, E. Alomari, and S. Alsaleem, "Review of Security Vulnerabilities in the IPv6 Neighbor Discovery Protocol," *Lecture Notes in Electrical Engineering Information Science and Applications (ICISA) 2016*, pp. 603–612, 2016.

[4] T. Zhang and Z. Wang, “Research on IPv6 Neighbor Discovery Protocol (NDP) security,” *2016 2nd IEEE International Conference on Computer and Communications (ICCC)*, 2016.

[5] Ahmed, A. S., Ismail, N. H. A., Hassan, R., and Othman, N. E, “Balancing performance and security for IPv6 neighbor discovery”. *International Journal of Applied Engineering Research*, 10(19), 40191-40196, 2015.

[6] A. S. Ahmed, R. Hassan, and N. E. Othman, “Improving security for IPv6 neighbor discovery,” *2015 International Conference on Electrical Engineering and Informatics (ICEEI)*, 2015.

[7] Ahmed, Amjed Sid Ahmed Mohamed Sid, Rosilah Hassan, and Nor Effendy Othman. "IPv6 Neighbor Discovery Protocol Specifications, Threats and Countermeasures: A Survey."*IEEE Access* 5 (2017): 18187-18210.

[8] S. Praptodiyono, I. H. Hasbullah, M. Anbar, R. K. Murugesan, and A. Osman, “Improvement of Address Resolution Security in IPv6 Local Network using Trust-ND,” *TELKOMNIKA Indonesian Journal of Electrical Engineering*, vol. 13, no. 1, Jan. 2015.

[9] F. Najjar, M. M. Kadhum, and H. El-Taj, “Detecting Neighbor Discovery Protocol-Based Flooding Attack Using Machine Learning Techniques,” *Lecture Notes in Electrical Engineering Advances in Machine Learning and Signal Processing*, pp. 129–139, 2016.

[10] Y. Lu, M. Wang, and P. Huang, “An SDN-Based Authentication Mechanism for Securing Neighbor Discovery Protocol in IPv6,” *Security and Communication Networks*, vol. 2017, pp. 1–9, 2017.

[11] I. H. Hasbullah, M. M. Kadhum, Y.-W. Chong, K. Alieyan, A. Osman, and S., “Timestamp utilization in Trust-ND mechanism for securing Neighbor Discovery Protocol,” *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, 2016.

[12] R. M. A. Saad, M. Anbar, and S. Manickam, “Rule-based detection technique for ICMPv6 anomalous behavior,” *Neural Computing and Applications*, 2017.

[13] A. S. Ahmed, R. Hassan, and N. E. Othman, “Security threats for IPv6 transition strategies: A review,” *2014 4th International Conference on Engineering Technology and Technopreneuship (ICE2T)*, 2014.

[14] O. E. Elejla, M. Anbar, and B. Belaton, “ICMPv6-Based DoS and DDoS Attacks and Defense Mechanisms: Review,” *IETE Technical Review*, pp. 1–18, Feb. 2016.

[15] Ahmed, Amjed Sid, Rosilah Hassan, and Nor Effendy Othman. "Securing IPv6 Link Local Communication Using IPSec: Obstacles and Challenges." *Advanced Science Letters* 23, no. 11 (2017): 11124-11128.

[16] R. M. A. Saad, M. Anbar, S. Manickam, and E. Alomari, “An Intelligent ICMPv6 DDoS Flooding-Attack Detection Framework (v6IIDS) using Back-Propagation Neural Network,” *IETE Technical Review*, vol. 33, no. 3, pp. 244–255, 2015.

[17] O. E. Elejla, B. Belaton, M. Anbar, and A. Alnajjar, “Intrusion Detection Systems of ICMPv6-based DDoS attacks,” *Neural Computing and Applications*, 2016.

[18] Ahmed, Amjed Sid, Rosilah Hassan, and Nor Effendy Othman. "Secure neighbor discovery (SeND): Attacks and challenges." In *Electrical Engineering and Informatics (ICEEI), 6th International Conference on*, pp. 1-6. IEEE, 2017.

[19] J. L. Shah, “A novel approach for securing IPv6 link local communication,” *Information Security Journal: A Global Perspective*, vol. 25, no. 1-3, pp. 136–150, Apr. 2016.

[20] P. Sumathi, S. Patel, and P., “Secure Neighbor Discovery (SEND) Protocol challenges and approaches,” *2016 10th International Conference on Intelligent Systems and Control (ISCO)*, 2016.

[21] Alsadeh, Ahmad, Hosnieh Rafiee, and Christoph Meinel, "Cryptographically Generated Addresses (CGAs): Possible attacks and proposed mitigation approaches," *Computer and Information Technology (CIT), 2012 IEEE 12th International Conference on*. IEEE, 2012.