Indonesian Journal of Electrical Engineering and Computer Science
Vol. 12, No. 1, October 2018, pp. 137~146
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v12.i1.pp137-146

Prevention of Denial-of-service in Next Generation Internet Protocol Mobility

Maanasaa Sethuraman, Senthilkumar Mathi
Dept. of Computer Science and Engineering, Amrita University,
India

Article Info

Article history:

Received Apr 4, 2018
Revised Apr 22, 2018
Accepted Jun 14, 2018

Keywords:

IPv6 security
Denial-of-service
Router discovery
Duplicate address detection
Neighbor discovery

ABSTRACT

Internet Protocol version 6 (IPv6) is a next-generation internet protocol that is devised to replace its predecessor, the IPv4. With the benefit of ample address space, flexible header extensions and its many specific features, IPv6 is the future of the Internet. A significant advantage of IPv6 is its capabilities in the domain of security and mobility, where it scores in comparison with its predecessor. One of the features specific to IPv6, such as the mandatory IPsec messaging or address auto-configuration, is the Neighbor Discovery Protocol (NDP). Even though the concept of security is more pronounced in the IPv6 protocols, there still exist loopholes. The extensive applications of NDP make it even more necessary to identify and address these issues to ensure security. Hence, this paper investigates loopholes in the applications of NDP and analyzes the process of the denial-of-service attacks that endanger the security. Also, the paper proposes a new method to mitigate Denial-of-Service (DoS) in IPv6 based network mobility. This proposed approach is a hybrid of existing solutions and is capable of overcoming the significant disadvantages of these solutions. Also, the paper discusses the comparative analysis among the existing solutions and illustrates the effect of the proposed method.

Corresponding Author:

Senthilkumar Mathi,
Dept. of Computer Science and Engineering,
Amrita University, India.
Email: m_senthil@cb.amrita.edu

1. INTRODUCTION

IPv6 is a network layer protocol that is developed to replace its predecessor the IPv4 owing to the exhausted address space available in IPv4 [1]. The IPv6 provides more extensive address spaces, almost in the range of 340 undecillion addresses to satisfy the ever-growing demand for addresses in tune with the increasing number of devices connecting to the Internet. It coexists with the already familiar IPv4 protocol. A specific feature of IPv6 is the NDP that seeks to replace the Address Resolution Protocol (ARP) of IPv4, the router discovery and the redirect applications. Security threats are rampant on the Internet and overcoming these or preventing them is more relevant in the language of IPv6 than the IPv4 [2]. The mandatory implementation of IP security in IPv6 seeks to make the protocol more secure.

The introduction of IPv6 is advantageous not just to the everyday user, but also to the savvy cybercriminals who continuously seek more system vulnerabilities and exploit them. Despite this feature, the NDP remains an easy target for intercepting and spoofing the messages with a duplicate Media Access Control (MAC) address, thus leading to attacks such as Denial-of-service, Man-in-the-Middle (MITM), ARP poisoning, fragmentation etc. The many applications of NDP include router discovery, Neighbor Unreachability Discovery (NUD), Neighbor Discovery (ND), address resolution, and Duplicate Address Detection (DAD) [3].

NDP is a supporting protocol in IPv6 that operates in the link layer of the network model [4]. Its functionalities include the automatically configuring address, neighbour node discovery on the link, duplicate address detection, detecting domain name servers and available routers, determining the link layer address of the communicating nodes. Exchanging ICMPv6 messages on top of the IPv6 protocol is crucial for IPv6 communication as it is the minimum security prescribed by the IPsec standards Table 1. However, this can be affected, and hence the security can be breached by sending fake response messages to initiate DoS, traffic re-routing and various other attacks [5-7]. The numerous studies have reinstated their stature by suggesting mitigation strategies for these attacks in a wired LAN, MAN or WAN setup. What remains to be discovered through this paper is the effect of these vulnerabilities in the mobility model of the IPv6 wireless networks. Hence, the present paper investigates the possible attacks on these applications when performed on IPv6 network mobility through an exploration of the survey and proposes a mechanism to mitigate the DoS attacks in the network mobility.

Table 1. ICMPv6 packet types and description

ICMPv6 message	Description
RS – Router Solicitation	Here, the routers are located by hosts in an attached link by using the RS messages.
RA – Router Advertisement	These messages are used by routers to advertise their presence together with various other links.
NS – Neighbor Solicitation	NS messages are used by nodes to determine the link-layer address of a neighbour node.
NA – Neighbor Advertisement	NAs are standard response messages to the NS messages sent by hosts.
Redirect	Using this message, the routers can inform hosts of a better first-hop router and a suitable path for a destination, through which the packets can be redirected.

Of the significant improvements in IPv6 are the changes in the length and the format of the IP addresses assigned to nodes and a significantly smaller header size. The mandatory use of IPsec, the primary endways security method, ensures the enhancement of security features in IPv6. The extension header that is introduced in this format is a distinctive feature of this protocol version and the IPsec [8]. The two extension headers introduced in IPv6 are the authentication header and encapsulation security payload. These serve the task of data integrity and confidentiality. As NDP helps for many significant purposes in the IPv6 protocol suite, the protocol finds applications in not just the dedicated wired networks but also in the Mobile IPv6 (MIPv6) network domain. The demands of NDP also include the maintenance of IPv6 mobility networks, and motivating mobile devices to join the visited network links [9].

The host initializations to join the IPv6 network and address auto-configuration are the two useful features offered by the NDP and IPv6 protocol suite. The host initialization is done with the help of the RS messages. The IPsec takes care of the security of transmitted packets, but it is prone to various censorious attacks.

The message headers in the NDP and ICMPv6 messages are embedded with various options, which is another specific feature of the IPv6 protocol suite. The protocol options are prefix information, the source and target link layer addresses, redirected header, route information and the maximum transmission unit for the packet. These options are regularly used to perform the various functions or applications of NDP. The many features of the NDP pave the way for severe vulnerabilities in its applications. The vulnerabilities of NDP are of three types: 1) redirect attack - malicious nodes redirect the packet from the actual destination which cannot be traced from the last hop router, 2) DoS - to pass packets between nodes is included in this category, and 3) flooding DoS - flooding the victim node with packets, above its capacity to disable communication with the network. It is also successful in sending malicious packets as one among the multitude of traffic sent to the victim, by which way the attacker breaches the security of the victim node [10].

The most common threats are the MITM and DoS attacks in the IPv6 networks. For the MITM attack, the access gaining phase is one where the invader places himself between two communicating parties transferring data [11], and further attacks are possible in this position. The MITM attack occurs during ARP cache poisoning or DHCP spoofing in IPv4. In IPv6 link layer network, the communication between nodes happens using the NS and NA messages. These messages are used to bind the MAC address to the IPv6 address of the nodes on the network. Unfortunately, these interactions are unsecured and vulnerable to various attacks. Considering a network with two nodes node A and node B, the usual MAC lookup is done by node A by sending an NS message to the multicast address (FF02::1) indicated by the target address. If the node B is active in the network, it would be anticipated to be listening to the multicast address. After

receiving the message, it responses with an NA message to node A with the solicited (S) flag. Once node A receives the advertisement, it recognizes that IPv6 address of node B is on the node B's MAC address [12]. This information is cached by node A.

In the scenario where the attacker joins the same IPv6 network, it is automatically agreed with an IPv6 address and begins snooping to the multicast group (FF02::1). In such a situation, the attacker node and the victim node A are on the identical LAN. When node A publishes an NS to FF02::1 for a MAC lookup of node B, both the node B and the attacker receives this NS message from node A. While node B responds with NA to node A with the S flag, the attacker returns with an NA with the S and the override (O) flags. The node A receives both the advertisement messages from node B and the attacker. Since the attacker has enabled the O flag, it overwrites and generates an entry for node A wherein it binds the MAC address of the attacker to the IP address of the node B Figure 1. Consequently, all the traffic between the nodes A and B undergo the attacker node since the routing table of node A contains the same MAC address for both the node B and the attacker.

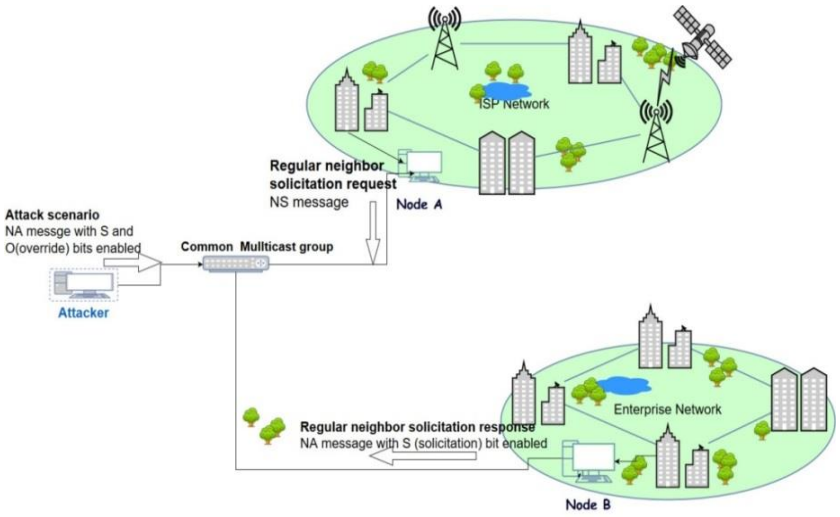

Figure 1. Spoofed ICMPv6 NA message for MITM

A similar process occurs in spoofed ICMPv6 RA also. The attacker (rouge router) pretends to be a router and sends the intermittent RA message to the node A connected to its multicast group. The node A is deceived and routes its packets with the address of the rogue router as the default gateway thus giving access to all the packets to the rogue router [13]. A replay attack is a continuous replay of any previous ND or RD message to gain network access. The invader can capture the message and replay it back after some time to the target node. It is most destructive for a new node if the attacker obtains the commands and passwords and uses them to gain access to applications in node A.

Address auto-configuration is one of the significant features of the IPv6 technology. Through this feature, the address assignment of the link-local addresses is simplified as they are automatically assigned to the hosts. Though an advantage, a significant flaw in this task is its vulnerability to being attached with incorrect addresses, leading to more serious security breaches. Of the many types of attacks that are possible, the DoS attack is the most harmful and the most frequent during auto-configuration of address. The usual impact of a DoS attack on the victim or target host is that the resources allotted to the host are wasted, and the communication link of the host with other nodes in the network is breached. A DoS attack initiated by an extensive system or network is termed as a distributed DoS attack. For this purpose, the attacker uses various nodes, over a distributed area along with the Internet services, called botnets [14]. The NDP and IPv6 protocol suite offer an attacker numerous opportunities to launch a DoS attack.

A unique feature of the IPv6 is the address auto-configuration for link layer address of nodes. Any new node joining a network undergoes many operations to configure an Interface Identifier (IID) for itself. When the node connects to an IPv6 local link, an RS message is sent by the node to a local link router to obtain its network prefix, after which the host can generate its own IID, It then has to combine the subnet prefix and the IID to make its unique IPv6 link-local address. The DAD process verifies the uniqueness of this address. Since the communication is done among nodes in a common link, a link layer address starting with fe80 and 64 bits long. It can be carried out by two methods - EUI-64 and extension mechanism.

To ensure the uniqueness of the address generated or owned by every node in a network, it is mandatory that they go through the DAD process of verification. Once the target node configures a tentative IID, an NS message is published to all the nodes in the same link, through the multicast address (FF02::1). In the case that the tentative IID is not unique, the host holding this address replies with the NA message implying the same and the target node reconfigures its IID and the process is repeated. If the target node does not receive a reply, it assumes that the tentative IID is unique.

A DoS attack in the DAD process Figure 2 happens when the NS message of the target node is repeatedly replied with an NA message. It is achieved by the attacker with the solicited bit (to note that it is in reply to the corresponding NS message) and override bit (to indicate that this NA has to replace any other NA sent by a neighbouring node) enabled, implying that the IIDs requested by the node is never unique. Thus, denying service to the target node as a node without an IPv6 address cannot communicate with another IPv6 node. A mechanism to secure the DAD process with a lower overhead has to be developed [15].

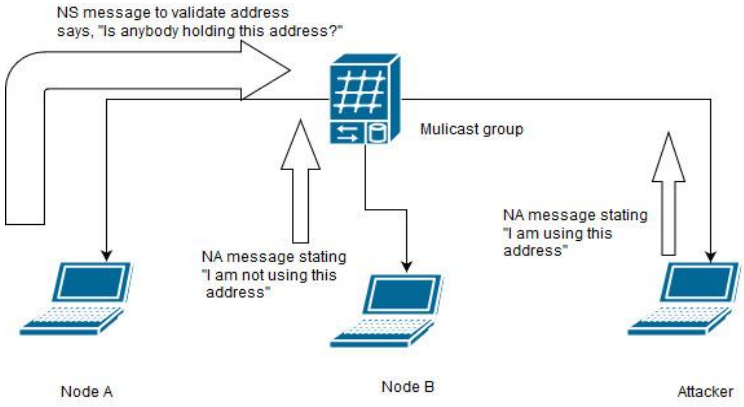

Figure 2. DoS attack in DAD process

Given the multifaceted role of NDP, it is essential to ensure security in its applications. Since the IPsec functions do not solely achieve this purpose, Secure ND protocol (SEND) was defined. This purpose still stands defeated for mobility IPv6 as it is always incompatible with the concept of proxy ND function employed [16]. Following the SEND, a new Improved Secure Neighbor Discovery (ISEND) protocol that overcomes these limitations by adapting the SEND to the concept of mobility was defined.

In SEND protocol, the node prompting ND proves its Cryptographically Generated Addresses (CGA) address ownership by signing its messages with a private key. Also, SEND protocol thwarts functions where a third party node is required to alter an NDP message. The proxy ND, a feature specific to IPv6, is one where a proxy node is allowed to produce messages in support of the mobile node (MN).

The SEND protocol ensures message freshness, authentication and integrity and provides address ownership. It guards the node against address spoofing and gives a mechanism to authenticate the access router. Along with CGA, the SEND protocol introduces three other modes of enhancement - RSA signature, nonce, and timestamp. Even though the SEND protocol remained sufficient to ensure the security of wired networks, it still poses many challenges such as the incompatibility between anycast address and SEND protocol [17].

Having noted that SEND lacks in security despite its many features, many extensions were proposed to give a robust protocol. One of the many suggested extensions was to discriminate between the proxy's role and the address ownership in a wireless network and define the tasks appropriately. The Proxy Signature (PS) is an option in the ICMPv6 message header that includes the digital signature of the message generated using the private key of the proxy node, in addition to the proxy's hashed public key; this certificate is extended to support a new Extended Key Usage (EKU) field. The primary function of this field is to indicate whether the router assumes a proxy role. Then, whenever it issues or modifies ND messages, it signs these messages with its public key.

The ISEND concentrates on improving the SEND protocol to resolve the mismatches between the SEND protocol and the proxy node. When an MN sends an NS message to another neighbour node in the same network, the receiver responds with an NA message. The ultimate challenge arises when the MN leaves its home network, which is addressed by the ISEND protocol [18]. This process is threefold, the first phase is router delegation, and the subsequent steps are delegation checking and revocation.

In the context of mobility, when the MN leaves its home network (regardless of whether it is still transmitting or not), it gives its responsibilities and services to the Home Agent (HA). After this delegation, the HA is allowed to act as a proxy and can sign messages and send them on behalf of the MN. Hence, the HA can now send a secured NA message in the place of the MN. It is achieved using a modified binding and acknowledgement messages.

Once the HA receives a modified binding update from MN1, it registers the delegation in the database. Now, the HA becomes the proxy for MN1, and it gets an NS message on behalf of MN1 from another node (MN2) for a MAC address lookup (the destination of the NS message from MN2 is MN1). HA consults its database to check for a delegation by the MN1 to allow the HA the permission to act on behalf of MN1. If it finds an appropriate delegation, the NA message is generated and signed by the HA instead of MN1. This message is then sent to the MN2. If it does not find an appropriate registration, it drops the NS packet or treats it as it would treat any secure packet. In the case that the router delegation verification is successful, the neighbour cache should be updated promptly. With these options, the router proves that it is delegated by MN1 to act in its stead as a proxy and it can answer all NS messages through the modified NA message. Effectively, this covers the phase of router delegation checking.

The procedure of router delegation is necessary when the MN1 returns to its home network. It is done to revoke the authority given to the HA to act in its place. The MN1 sends an NA message to all nodes in its network with the flag configurations where R and S flags are not set and O flag is set (to override any existing neighbour cache entry and update the link layer address). While the incompatibility between the SEND protocol and the proxy MN is efficiently resolved through ISEND, the interest lies in highlighting the other vulnerabilities in SEND such as the incompatibility between anycast address and SEND protocol as well as the problems related to CGA verification [19]. As seen earlier, the primary shortcoming in the NDP is the lack of integrity. The victim node is almost always incapable of telling the fake message from a legitimate message. The necessary ICMPv6 integrity checking feature of checksum is proved inefficient. Since the protocols as mentioned earlier involve cryptographic algorithms for address generation, they induce computational overhead.

Since the SEND protocol mandates the use of the RSA signature, CGA, timestamp and nonce for every message sent by the node or router. In turn, it increases the complexity for both the sender and receiver and overhead for the DAD process as any message without these options is assumed unsecured and is discarded. Also, the SEND messages are capable of preventing DoS attack only in the DAD process, while it is incapable of handling the IPv6 flooding attacks that also cause the DoS. Hence, the protocol is not a recommended option to secure the mobility network against the DoS attacks. Another proposed solution was the Source Address Validation Improvement (SAVI) by the Tsinghua University, China. This mechanism was successful in preventing source address spoofing by nodes in the same subnet of a network where NDP messages were exchanged.

In the SAVI mechanism, trusted information like the port number and MAC address of the target host is contained in an anchor, which creates a binding between the source IP address and the anchor information. Also, the filtering mechanism of SAVI helps in discarding packets that do not conform to the constraints of the filter while those packets that match the filter are forwarded. While it is a useful method to filter packets, SAVI is also vulnerable to many attacks [20]. The major drawback of this mechanism is that it creates vulnerabilities in the dynamic address auto-configuration process, both StateLess Address Auto-configuration (SLAAC) and DHCPv6 as the constantly changing IP address increases the difficulty in binding the anchor information with it. Another significant disadvantage of the SAVI protocol is its inability in binding when devices with multiple IP addresses are connected to a LAN. Hence, each SAVI must work independently from those devices vulnerable to traffic spoofing [21].

Since the SEND and the SAVI protocols are lacking, a new trust-ND protocol was suggested [22]. It was recommended that to reduce the complexity of generating RSA signature, the concept of soft security based on the distributed trust management be used. Since hard security involves cryptography, with proven higher complexity, the idea of soft security, based on social interactions implementing trust management was suggested. The suggested trust-ND combines both hard and soft security. The protocol uses cryptographically generated hash function and trust management mechanism for trust calculation and data integrity. The SHA-1 hash function is used for data integrity [23]. The protocol also incorporates the best of the SEND, IPsec and SAVI protocols. As a result, a new NDP option called the trust option (32 bytes) is embedded in the NDP message headers. The messages thus exchanged are the trust-NS and trust-NA messages. Also, each node calculates the trust value of its neighbour through this option. The messages without this feature are considered unsecured and are discarded. It makes the verification process faster when compared to SEND, and the smaller size of the options field helps in saving the bandwidth. This feature, though effective in a shorter network is untested and ineffective for a more extensive network.

The rule-based mechanism [24] was proposed to prevent the DoS attack on DAD process. In this process, when a query is sent by the target node, instead of relying on the reply from the neighbouring nodes, the target node verifies the tentative address with the confirmation received from the controller scheme machine. The rules are typical queries to check the uniqueness of the tentative IID. While the applicability of the proposed method was tested for the LAN networks and link local communication, the scalability and implementation of the approach in the mobility model remain untested and unverified.

The regular CGA data structure contains the elements similar to the IPv6 addresses, the subnet prefix, and the IID. When the IID is generated using the public key cryptography, by exploiting the CGA algorithm, verification of the message, by the receiver proceeds without the use of any public key. Since this procedure is vulnerable and produces large overhead, an efficient CGA procedure was proposed that computes the IID efficiently by including the modifier, subnet prefix, public key, collision count and extensions.

Table 2. Compilation of motivations for the proposed method

ICMPv6 message	Description
SEND	CGA verification, anycast add incompatibility, proxy ND incompatibility
SAVI	Causes problems in SLAAC and DHCPv6 anchor information binding
ISEND	Solves only proxy ND incompatibility. Other incompatibilities in SEND remain in ISEND
trust-ND	Effective in smaller LAN network, untested for larger LAN and Wireless networks
Efficient CGA	Lightweight and efficient but CGA efficiency problem

The SHA-1 hash function is used to generate the address and proved to have lower time complexity and hence gives a faster CGA. It eliminates the possibility of the DAD process in CGA as the way to trigger the DoS attacks. It is based on a timer that sets a threshold to control the said attack and is applicable in the MIPv6 networks as well. It is noted that this proposed method is a stand-alone solution for the CGA process alone, and must be used in conjugation with one of the discussed methods against DoS attacks [25]. The motivation for the proposed solution is illustrated Table 2. Even though the domain of securing the MIPv6 networks has given rise to many protocols as mentioned earlier, there still exist areas that are unexplored or unmitigated in the scenario of mobility.

2. RESEARCH METHOD

Since a secure MIPv6 protocol that works to prevent DoS attacks on the applications of NDP (especially DAD process) is necessitated, this paper proposes a hybrid model that serves this purpose. The proposed method is divided into various modules. The first module of the hybrid protocol works on generating a public and private for the MN. The next step is the generation of a Care-of address (CoA) or a tentative IID using the efficient CGA. It is concatenated with the subnet prefix to produce the 128-bit IPv6 address. The block diagram of the proposed method is depicted Figure 3.

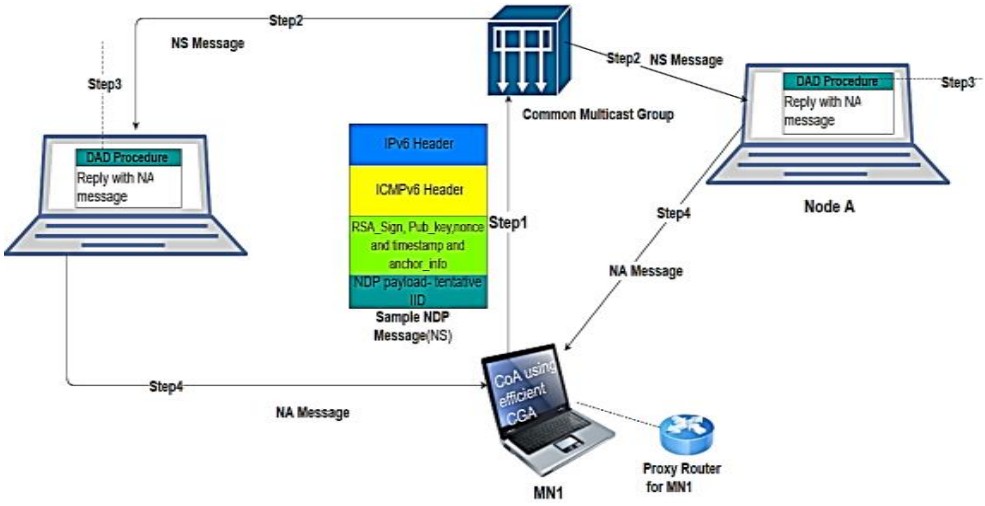

Figure 3. Block diagram of the proposed method

```
Generate public and private key
temp_IID ← efficient_CGA (private key)
SEND_options ← temp_IID, RSA_signature, public key, nonce, timestamp
// encapsulate SEND options in NDP or ICMPv6 message options field
        set DAD_timer ← threshold value
        set IID_ttl ← value                    // where value > DAD_timer
        set time_before_DAD ← value
        set time_after_DAD ← value
                if (IID_ttl > DAD_timer && ((IID_ttl-DAD_timer) > 0.5 * DAD_timer))
                anchor_info (tentative_IID, targetIP, targetMAC )
                  send_ICMPv6_msg(SEND_options, anchor_info)
                else
        Result ← DuplicateAddressDetection (NS_msg from MN)
                                                // result = 0 if duplicate, 1 otherwise
        If (Result = = 1)
                CoA = temp_IID
                                // proceed with regular services
                If (moving_out_of_home_network)
                        Generate Proxy_public_key, Proxy_private_key
                        Security_Certificate (EKU, PS, Proxy_public_key)
                                // EKU=1 when router can act as proxy, PS-proxy sign
                        Authorization_Delegation ()
                Check ← MN.Router_Delegation ( )
                                // Check = 1 if delegation successful, 0 otherwise
                If (Check = = 1 and received NS message from another MN)
                                Router_Delegation_Checking ()
                          Else if (returning_to_home_network)
                                Router_Delegation_Revocation ( )
                        Else
                                Continue_services ()
                If (Done_with_services)
                        Exit ( )
Else
                If (collisionCount < 3)
                Reconfigure_IID ( )
                Else
                Exit ( )
```

Figure 4. Modified version of ISEND

It is achieved by increasing the TTL of the tentative IID and setting it to a value higher than the threshold value for the timer monitoring the DAD procedure. By this, the SAVI is forced to assume the IID as permanent, hence capable of binding it to the anchor information. The time gap between the generation of IID after linking it to the anchor information and the initiation of the DAD procedure is significantly increased. As a result, it increases the time for which the MN holds the said IID. The next phase constitutes the DAD procedure wherein the timer monitors the time consumed to initiate a round of the DAD procedure. The parameter collisionCount is set initially to zero and incremented in the case that the tentative IID is the duplicate. A threshold value of three collisions is permitted wherein, after each collision, the MN generates a new IID. If the threshold is crossed, the attempt to connect to the network by making a SLAAC IID is aborted, and the address is manually configured. If the DAD procedure is successful and the address is found to be unique, the IID is assigned as the new IP address or the CoA for the MN. When the MN leaves the home network, the ISEND implementation of the process of router delegation is carried out Figure 4. Once a router is assigned as the proxy node in place of the MN, any NS messages received to the CoA of the MN is replied by the proxy node. The flow of the proposed method is depicted in Figure 5 and 6.

3. RESULTS AND DISCUSSION

A detailed analysis of the existing and the proposed methods are discussed in this section. The NDP by itself is by mandate run on the IPsec, which is anycast address compatible but is inefficient for preventing DoS attacks. The SEND protocol developed to battle this is incompatible with anycast addresses. Since the ISEND is an improved version of the SEND protocol, this deficiency in SEND is carried forward to ISEND. The effective CGA is a method for faster CGA generation of link-local addresses and is not compatible with anycast addresses. The trust-ND protocol is based on soft security and uses the CGA generation strategy of the SEND family, which makes this protocol incompatible with anycast addresses. The SAVI method proposes binding the anchor information with the tentative, link-local IID and is incapable of linking the anycast address. Since the solution proposed in this paper is a hybrid of the ISEND and SAVI protocols and uses the efficient CGA algorithm, this is also incompatible with the anycast address. The comparative analysis based on compatibility is listed in Table 3.

Since IPsec is a primary security mandate, it does not include the option of delegating proxy nodes for mobile nodes in a mobility network. While SEND is a reasonably advanced protocol when compared with IPsec, the incompatibility of proxy nodes persists in this protocol too. The ISEND was developed to tackle this hurdle and hence is specifically compatible with the proxy-ND system. The SAVI protocol binds to any link-local address and has no restrictions in the binding with the proxy nodes. The trust-ND method opens new areas of research in this aspect as the compatibility is not verified as yet. Owing to its hybrid nature, and the fact that the root protocols used in the proposed method are already proxy ND compatible, it is also consistent and can be put to practical use in the MIPv6 domain.

Table 3. Comparative analysis based on compatibility

ICMPv6 Compatible	IPsec	SEND	ISEND	Effective CGA	trust-ND	SAVI	Proposed
Anycast address	Yes	No	No	No	No	No	No
Proxy ND	No	No	Yes	Not applicable	Not verified	Yes	Yes
SLAAC and DHCPv6	Yes	Yes	Yes	Yes	Yes	No	Yes

All other existing methods are compatible with dynamic address assignment feature, the SAVI proves incompatible with binding the anchor information with dynamically changing addresses. The proposed method is designed to overcome this problem and is hence compatible with SLAAC and DHCPv6. Using SAVI in the proposed method enables the prevention of source address spoofing and as the trade-off, this inefficiency of SAVI at managing multiple addresses assigned to a single node is carried here.

Apart from these compatibility issues, there are many other parameters based on which the existing and proposed method can be compared Table 4. The trust management is a concept of soft security as used in the trust-ND protocol. Though efficient, it cannot be incorporated in any of the other suggested methods. It is noted that the different ways are not only useful at preventing DoS attacks but also can be implemented at wireless, mobile and LAN networks. This property of trust-ND is not verified as yet, and hence in the trade-off, the other methods weigh more significant, as the proposed method includes the features of ISEND and SAVI, this concept of trust management is not incorporated. The CGA is a feature introduced by SEND and carried forward by ISEND. It is unavailable in the essential IPsec mandate, SAVI, and the trust-ND protocol. The primary reason behind the inefficiency of IPsec regarding computational speed even in the absence of CGA is that it has a moderately higher computational cost. The CGA generation and verification processes in SEND and ISEND are susceptible to DoS attacks as well. The proposed method is designed to tackle this by using the efficient CGA algorithm. All the existing protocols except the trust-ND are proved to be scalable. It enables the proposed method also to be scalable.

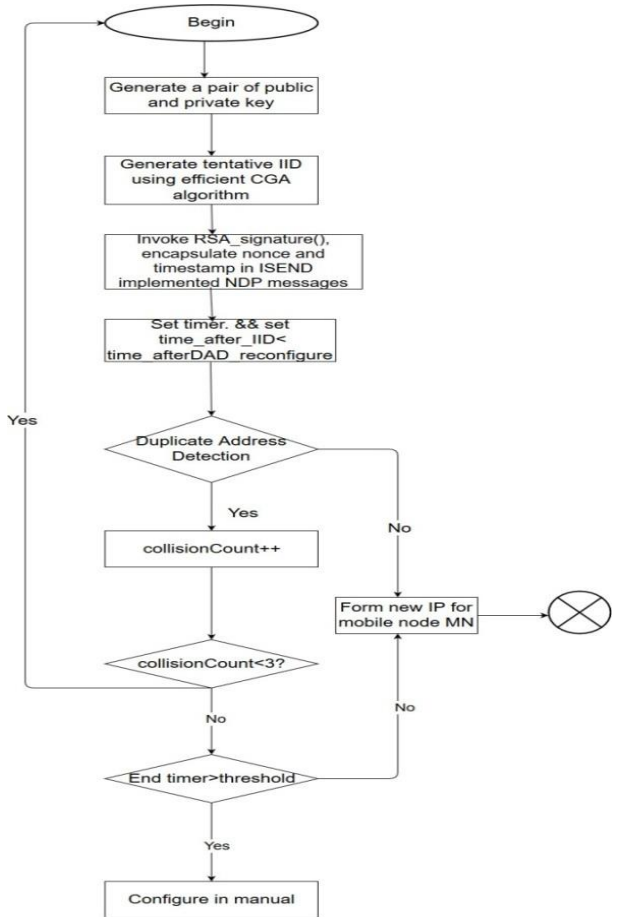

Figure 5. Modified version of ISEND

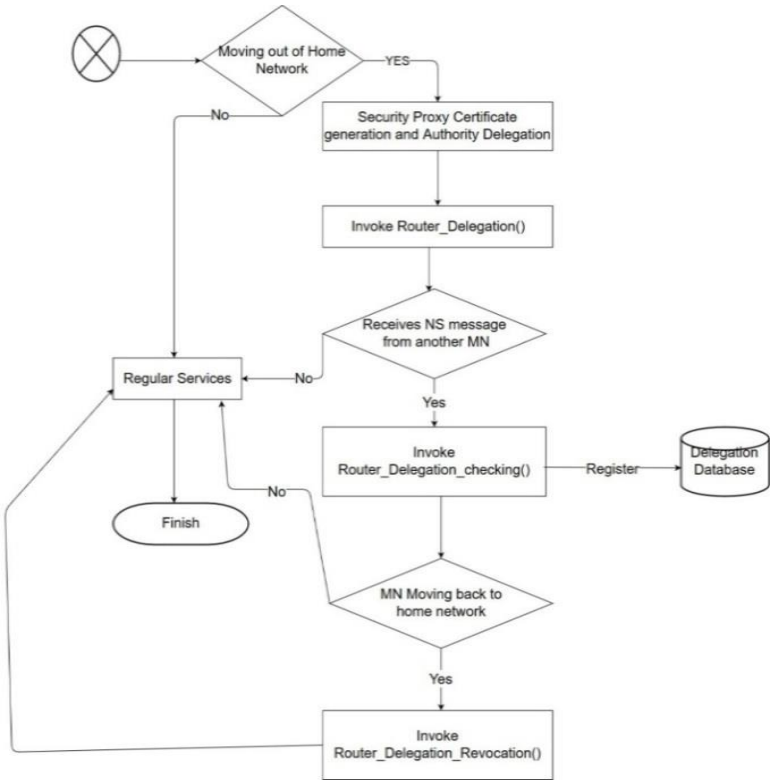

Figure 6. Flow diagram of the proxy node assignment process in modified ISEND

Table 4. Comparative analysis based on other parameters

ICMPv6 message	IPsec	SEND	ISEND	Effective CGA	trust-ND	SAVI	Proposed
Trust management	No	No	No	Not applicable	Yes	No	No
Faster CGA	No	No	No	Yes	No	No	Yes
Scalability	Yes	Yes	Yes	Not applicable	Not verified	Yes	Yes

4. CONCLUSION

IPv6 is a dynamically evolving domain, and mobility is the future. It emphasizes that the security of MIPv6 is also paramount. The DoS attacks are one of the deadliest that have plagued the internet security for ages and continue to do so. Though there have been many advances and many stand-alone protocols and algorithms have been developed to battle this, the mitigation of this attack in the MIPv6 domain is very few. The proposed method is designed as one such mechanism to ensure security and the prevention of DoS attacks on these networks. The proposed method is a modified and hybrid solution. From the investigation, it is noted that the proposed solution provides a robust, and a scalable MIPv6 security mechanism to battle the DoS attacks on the DAD mechanism and also on the other applications of the NDP.

REFERENCES

[1] Anbar M, Abdullah R, Saad RM, Alomari E, Alsaleem S. "Review of security vulnerabilities in the IPv6 neighbor discovery protocol". *InInformation Science and Applications (ICISA)*. 2016 (pp. 603-612). Springer, Singapore.
[2] Mathi S. "An optimized and secure BUTE–binding update using twofold encryption for next generation IP mobility". *Journal of Intelligent & Fuzzy Systems*. 2018 Jan 1; 34(3):1311-22.
[3] Zhang T, Wang Z. "Research on IPv6 Neighbor Discovery Protocol (NDP) security". *In Computer and Communications (ICCC), 2016 2nd IEEE International Conference on 2016 Oct 14* (pp. 2032-2035).
[4] Tian DJ, Butler KR, Choi JI, McDaniel P, Krishnaswamy P. "Securing ARP/NDP From the Ground Up". *IEEE Transactions on Information Forensics and Security*. 2017 Sep; 12(9):2131-43.
[5] Masood AM, Muthusundar SK. "Incursion Recognition Mechanism Based on Secure Network System". *Indonesian Journal of Electrical Engineering and Computer Science(IJEECS)*. 2018 Mar 1;9(3).
[6] Durdağı E, Buldu A. "IPV4/IPV6 security and threat comparisons". *Procedia-Social and Behavioral Sciences*. 2010 Jan 1; 2(2):5285-91.

[7] Mathi S, Nivetha R, Priyadharshini B, Padma S. "A certificateless public key encryption based return routability protocol for next-generation IP mobility to enhance signalling security and reduce latency". *Sādhanā*. 2017 Dec 1; 42(12):1987-96.
[8] Samad F, Memon ZA. "The Future of Internet: IPv6 Fulfilling the Routing Needs in Internet of Things". *International Journal of Future Generation Communication and Networking*. 2018 Jan 1;11(1).
[9] Ahmed AS, Hassan R, Othman NE. "IPv6 Neighbor Discovery Protocol Specifications, Threats and Countermeasures: A Survey". *IEEE Access*. 2017; 5:18187-210.
[10] Ullrich J, Krombholz K, Hobel H, Dabrowski A, Weippl ER. "IPv6 Security: Attacks and Countermeasures in a Nutshell". *InWOOT* 2014 Aug 19.
[11] Kanagasabapathi K, Deepak S, Prakash P. "A Study on Security Issues in Cloud Computing". *InProceedings of the International Conference on Soft Computing Systems 2016* (pp. 167-175). Springer, New Delhi.
[12] Conti M, Dragoni N, Lesyk V. "A survey of man in the middle attacks". *IEEE Communications Surveys & Tutorials*. 2016 Jan 1; 18(3):2027-51.
[13] Stajkic A, Clazzer F, Liva G. "Neighbor discovery in wireless networks: A graph-based analysis and optimization". *In Communications Workshops, IEEE International Conference*, 2016, pp. 511-516.
[14] Rehman SU, Manickam S. "Denial of Service Attack in IPv6 Duplicate Address Detection Process". *International Journal of Advanced Computer Science & Applications*. 2016; 7:232-8.
[15] Praptodiyono S, Hasbullah IH, Kadhum MM, Wey CY, Murugesan RK, Osman A. "Securing Duplicate Address Detection on IPv6 Using Distributed Trust Mechanism". *International Journal of Simulation--Systems, Science & Technology*. 2016 Oct 1; 17(26).
[16] Xi H. "The research and application of the NDP protocol vulnerability attack and the defense technology based on SEND". *In AIP Conference Proceedings 2017 May 8* (Vol. 1839, No. 1, p. 020195). AIP Publishing.
[17] Sumathi P, Patel S. "Secure Neighbor Discovery (SEND) Protocol challenges and approaches. InIntelligent Systems and Control (ISCO)". *10th International Conference on 2016 Jan 7* (pp. 1-6).
[18] El Bouabidi I, Smaoui S, Zarai F, Obaidat MS, Kamoun L. "ISEND: An Improved Secure Neighbor Discovery Protocol for Wireless Networks". *InInternational Conference on E-Business and Telecommunications 2014 Aug 28* (pp. 518-535). Springer, Cham.
[19] Shah JL. "A novel approach for securing IPv6 link local communication". *Information Security Journal: A Global Perspective*. 2016 Apr 4; 25(1-3):136-50.
[20] Yao G, Bi J, Xiao P. "Source address validation solution with OpenFlow/NOX architecture". *In Network Protocols (ICNP), 2011 19th IEEE International Conference on 2011 Oct 17* (pp. 7-12).
[21] Praptodiyono S, Hasbullah IH, Kadhum MM, Murugesan RK, Wey CY, Osman A. "Improving Security of Duplicate Address Detection on IPv6 Local Network in Public Area". *In Modelling Symposium (AMS), 2015 9th Asia* 2015 Sep 7 (pp. 123-128). IEEE.
[22] Moslehpour M, Khorsandi S. "Improving cryptographically generated address algorithm in IPv6 secure neighbor discovery protocol through trust management". *In Proc. 18th Int. Conf. Inf. Commun. Secur*. (ICICS) 2016 Jun 9 (pp. 1-5).
[23] Raza S, Duquennoy S, Höglund J, Roedig U, Voigt T. "Secure communication for the Internet of Things - a comparison of link-layer security and IPsec for 6LoWPAN". *Security and Communication Networks*. 2014 Dec 1; 7(12):2654-68.
[24] Rehman SU, Manickam S. "Rule-based mechanism to detect Denial of Service (DoS) attacks on Duplicate Address Detection process in IPv6 link local communication". *In Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), 2015 4th International Conference on* 2015 Sep 2 (pp. 1-6).
[25] Abdul AM, Umar S. "Attacks of Denial-of-Service on Networks Layer of OSI Model and Maintaining of Security". *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*. 2017 Jan 1; 5(1):181-6.