Performance Enhancement Of Neighbor Discovery Protocol Using Stateful Mode

Gagandeep Kaur[1], Dr Jatinder Singh Saini[2]
[1] *Baba Banda Singh Bahadur Engineering College*
[2] *Baba Banda Singh Bahadur Engineering College*
(E-mail: deepgagan907@yahoo.com[1], sainijatinder@gmail.com[2])

***Abstract*— Internet Protocol version 6 (IPv6) is envisioned as the cornerstone for future internet connectivity and information technology (IT) expansion. Due to its enormous address pool, extendable headers, high level of security, and mobility, IPv6 is positioned as the next-generation Internet Protocol. NDP is an integral component of IPv6 since it resolves addresses, locates routers, and finds duplicated addresses in a local-link network. The proposed DHCP-NDPsec mechanism demonstrates comparable processing times for generating IPv6 addresses when compared to other mechanisms, such as Standard NDPSec. In contrast to SeND, which employs RSA and CGA algorithms leading to higher processing times, DHCP-NDPsec utilizes the Ed25519 digital signature keypairs, resulting in significantly faster IP address generation. Experimental results indicate that DHCP-NDPsec reduces the complexity of generating and verifying NDP messages compared to SeND, being approximately twice as fast as NDPSec. This performance enhancement is particularly beneficial for mobile or IoT devices with limited resources. Moreover, DHCP-NDPsec substantially reduces traffic overhead by approximately 57.08% compared to NDPSec, thereby reducing communication costs and bandwidth utilization. While mechanisms like Standard NDPSec, Match Prevention, and Trust-ND exhibit lower processing times and generate smaller traffic sizes, NDPSec's susceptibility to RA flooding attacks poses a significant drawback. Although NDPSec thwarts the injection of RA messages by attackers, it fails to prevent the consumption of a host's CPU during an attack, rendering it unresponsive to valid incoming messages. In contrast, DHCP-NDPsec is immune to all NDP attacks, including RA flooding, due to its lightweight design and robust security measures. Consequently, adopting DHCP-NDPsec ensures authentication for NDP messages, providing enhanced security for network environments.**

Keywords*—Network, NDPSec*

I. INTRODUCTION

The rise of the digital-world enabled by cutting-edge technologies such as 5G networks, the Internet of Things (IoT), and Cloud Computing has resulted in a massive increase in the number of devices connected to the Internet [1]. The projected expansion of IoT devices is increasing, and Cisco research indicates that there will be 27.1 billion networked devices in 2021, equating to 3.5 networked devices per person worldwide [2]. The Internet Protocol version 4 (IPv4) barely provides enough address space to connect the Internet's approximately 4.3 Billion devices, which has long been recognized as being depleted and in need of replacement with a protocol that provides a larger pool of address space to meet the demands of today's digital world [3]. The Internet Protocol version 6 (IPv6) is the next generation of the Internet Protocol that will supersede the IPv4 protocol [4]. The percentage of devices accessing Google via IPv6 has exceeded 33 percent, according to Google data [5]. Compared to IPv4, IPv6 offers a modest improvement in network security as well as in service quality. IPv6 does, however, continue to face a number of security problems, including Denial of Service (DoS) and Man-in-the-middle (MITM) attacks.

In order to mitigate security problems in a link-local network, IPv6 introduces a new protocol, known as the Neighbor Discovery Protocol (NDP), which is defined in RFC 4861 [7]. NDP is a critical protocol in the IPv6 network, and it performs a variety of tasks, including Address Resolution (AR), Neighbor Unreachability Detection (NUD), router discovery, and Duplicate Address Detection (DAD). IPv6 was designed on the premise that devices connected to a Local Area Network (LAN) are trustworthy and reliable. As a consequence, the NDP treats every device connected to the LAN as trustworthy and lacks security measures for situations in which a malicious host enters the network and initiates network attacks. This situation renders the network vulnerable to a variety of attacks, including DoS and MITM, which is the most severe attack on an IPv6 link-local network. Given the importance of NDP's processes and its susceptibility to attacks, a plethora of techniques have been proposed to protect these processes from being compromised. In this article, the most commonly used techniques are presented and assessed in terms of processing time, bandwidth usage, and effectiveness in preventing attacks on NDP [8]. Thus, this paper introduces a new mechanism called NDPsec that enables authentication for NDP communications in an IPv6 link-local network.

II. NEIGHBOR DISCOVERY PROTOCOL

In 5G networks, Neighbor Discovery Protocol (NDP) is a crucial mechanism that facilitates communication between neighboring nodes. NDP is responsible for identifying and managing neighboring devices in a network, allowing devices to discover each other's presence, capabilities, and other relevant information. The Neighbor Discovery Protocol in 5G networks is an essential part of the overall network architecture, contributing to the establishment and maintenance of efficient communication links.

Here are some key aspects of Neighbor Discovery Protocol in 5G networks:

1. Device Discovery: NDP helps devices in a 5G network discover and identify each other. This is essential for devices to establish communication links, share information, and collaborate in various network functions.
2. Address Resolution: NDP assists in the resolution of network layer addresses (such as IP addresses) to link layer addresses (such as MAC addresses). This ensures that devices can communicate with each other at both the network and data link layers.
3. Neighbor Unreachability Detection: NDP includes mechanisms to detect whether a neighboring device is reachable or not. This is important for maintaining the reliability of communication links. If a neighbor becomes unreachable, appropriate actions can be taken to update routing tables or re-establish communication.
4. Router Discovery: NDP plays a role in discovering routers in the network. Routers are critical for forwarding data packets between different subnets, and NDP helps devices identify and communicate with routers to facilitate efficient data routing.
5. Duplicate Address Detection (DAD): NDP includes a mechanism for preventing the assignment of duplicate addresses within a network. Duplicate addresses can lead to communication issues and network conflicts, so DAD is essential for ensuring unique address assignment.
6. Stateless Address Autoconfiguration: NDP supports stateless address autoconfiguration, allowing devices to automatically configure their IP addresses without the need for a central address assignment mechanism.
7. Router Advertisement and Solicitation: NDP uses router advertisement and solicitation messages to convey information about the presence of routers in the network. This helps devices discover available routers and maintain up-to-date routing information.

III. LITERATURE SURVEY

Al-Ani, A.; et al. [1] proposed an NDP security (NDPsec) mechanism based on the Ed25519 digital signature to authenticate IPv6 hosts to prevent unauthorized devices from joining the network. The proposed NDPsec mechanism is evaluated and compared to Secure NDP (SeND), Match-Prevention, and Trust-ND mechanisms. The performance is measured in terms of processing time, traffic overhead, and resilience against network-based attacks. Because NDP is based on the premise that all nodes in the network are trustworthy, it is subject to a variety of attacks, including Denial of Service (DoS) on Duplicate Address Detection (DAD) attacks (aka. DoS-on-DAD), Address Resolution-based attacks, Router Advertisement (RA) based attacks, and Redirect attacks.

Sun, H.; et al. [2] proposed a new discovery schedule based on the slot model that separates the listening and transmitting of beacons. The discovery schedule can guarantee unidirectional discovery. And the node proactively transmits the beacon to accelerate bidirectional discovery after unilaterally discovering its neighbor nodes. On this basis, a proactive asynchronous neighbor discovery protocol called Fedab is proposed in this paper. Ignoring beacon collisions and other realistic interference factors, Fedab can enable neighbor discovery within the theoretical worst-case discovery latency.

Luo, X.; et al. [3] proposed CREDND, a protocol for creating a Credible Neighbor Discovery against wormholes in WSN, which can detect not only external wormholes through the hop difference between the own exclusive neighbors but also internal wormholes through enabling the common neighbor nodes as witnesses to monitor whether the authentication packets are forwarded by malicious nodes. CREDND is a simple, localized protocol and needs no special hardware, localization, or synchronization, but it improves the ability of wormhole defense. However, the existing solutions are based on additional hardware, incur high communication overhead, or fail to give consideration to all types of wormholes.

Ling, H.; and Yang, S.; [4] proposed a non-integer framework to include all existing protocols. Then, a decentralized adaptive neighbor discovery protocol, named Anole, was designed under the framework. The protocol leveraged the genetic and similarity algorithms to be aware of and adapt to various scenarios with an appropriate discovery strategy. Discovery among fast moving devices requires an immediate exchange of emergency messages (minimum latency), while low-speed devices in crowded environments pay more attention to energy efficiency. Typical neighbor discovery protocols give solutions in a relatively stable scenario, which are not suited for the different environments in urban life.

Mansoor, N.; et al. [5] proposed a spectRum Aware cRoss-layEr (RARE) medium access control protocol for cognitive radio ad-hoc networks. The RARE protocol initially splits the network into clusters, where cluster formation is defined as maximum edge biclique problem. Besides, in order to maintain the integrity of the cluster-based network, super-frame structure, and topology maintenance protocols are also presented in this paper. Moreover, RARE also integrates a delay-aware routing protocol, where the routing protocol is defined as a weighted graph problem. It is anticipated that clusters in RARE adapt themselves dynamically with respect to spectrum availability and nodes mobility. Furthermore, the routing protocol in RARE is expected to select stable paths while ensuring faster data delivery from a source node to the destination. Simulation is conducted to evaluate the performance of the proposed RARE protocol, where it is found that RARE outperforms existing approaches by maintaining a lesser number of clusters and a steady number of common channels.

Grajzer, M. and Glabowski, M. [6] proposed the Neighbor Discovery ++ (ND++) solution for the enhanced stateless address auto-configuration. The ND++ incorporates a well-performing flooding control mechanism to the basic IPv6 ND design, which results in a very low protocol overhead in the order of few messages per node. The IPv6-based mobile ad hoc networks are envisioned to be a good candidate technology for the IoT networks. However, they lack efficient address auto-configuration mechanisms, which could extend the IPv6 to cover the requirements of such a demanding

networking environment. Especially the importance of autonomic, self-configuration capabilities becomes particularly significant.

Bahashwan, A.A.; et al. [7] proposed a flow-based approach to detect abnormal NDP traffic behavior, which is considered an indicator of the presence of NDP-based attacks, such as RA and NS DoS flooding attacks. Also, the proposed approach relies on flow-based network traffic representation and adoption of the Entropy algorithm to detect the randomness in the network traffic. The proposed approach is evaluated in terms of detection accuracy, precision, recall, and F1-Score using a simulated dataset. In these types of attacks, attackers send an enormous volume of abnormal NDP traffic, which causes congestion that degrades network performance. The expected behavior among these attacks is the existence of NDP traffic abnormalities.

Pozza, R. et al. [8] presented a new classification and taxonomy is presented with an emphasis on recent protocols and advances in this area, summarizing issues and ways for potential improvements. Many Internet of Things applications (e.g., smart cities) can, in fact, benefit from such discovery, since end-to-end paths may not directly exist between sources and sinks of data, thus requiring the discovery and exploitation of rare and short connectivity opportunities to relay data. While many of the older discovery approaches are still valid, they are not entirely designed to exploit the properties of these new challenging scenarios. A recent direction in research is, therefore, to learn and exploit knowledge about mobility patterns to improve the efficiency in the discovery process.

Shi, Z.; et al. [9] proposed a wormhole attack resistant secure neighbor discovery (SND) scheme for a centralized 60-GHz directional wireless network. Specifically, the proposed SND scheme consists of three phases: the network controller (NC) broadcasting phase, the network nodes response/authentication phase, and the NC time analysis phase. In the broadcasting phase and the response/authentication phase, local time information and antenna direction information are elegantly exchanged with signature-based authentication techniques between the NC and the legislate network nodes, which can prevent most of the wormhole attacks. In the NC time analysis phase, the NC can further detect the possible attack using the time-delay information from the network nodes. To solve the transmission collision problem in the response/authentication phase, we also introduce a novel random delay multiple access (RDMA) protocol to divide the RA phase into M periods, within which the unsuccessfully transmitting nodes randomly select a time slot to transmit.

Ahmad, A.S.A.M.S. et al. [10] revolved around the survey of the vulnerabilities mitigations approaches of NDP, since the time of the protocol development up to the date. The motive behind NDP is to replace address resolution protocol (ARP), router discovery, and redirect functions in Internet protocol version 4. NDP is known as the stateless protocol as it is utilized by the IPv6 nodes to determine joined hosts as well as routers in an IPv6 network without the need of dynamic host configuration protocol server. NDP is susceptible to attacks due to the deficiency in its authentication process. Securing NDP is extremely crucial as the Internet is prevalent nowadays and it is widely used in communal areas, for instance, airports, where trust does not exist among the users. A malicious host is able to expose denial of service or man-in-the-middle attacks by injecting spoofed address in NDP messages. With the intention to protect the NDP many solutions were proposed by researchers. However, these solutions either introduced new protocols that need to be supported by all nodes or built mechanisms that require the cooperation of all nodes. Moreover, some solutions are deviating from the layering principals of open system interconnection model. Therefore, the necessity to study NDP in details to recognize and identify the points that could be a source of enhancement has become mandatory task.

Al-Ani, A.K. et al. [11] introduced a prevention technique called Match Prevention, which secures target IP addresses and exchange messages (i.e. NS and NA). The processing time, bandwidth consumption and DoS prevention success rate of Match-Prevention in different scenarios are evaluated, and its performance is compared with those of existing techniques, including Standard-Process (i.e., Standard-AR and Standard-DAD), SeND and Trust-ND. Results show that Match-Prevention requires less processing time during AR and DAD processes and less bandwidth consumption compared with other existing techniques. In terms of DoS prevention success rate, the experiments show that Standard-Process and Trust-ND are unable to secure AR and DAD from DoS attacks, whilst SeND is vulnerable to flooding attacks.

Hayat, O.; et al. [12] highlighted security and privacy issues in Device Discovery. It is comprehensive and proved that in-band is much better than out-band with practical and technological reasons. To enhance the scope of the research, network level, and system level Security and Privacy (S&P) issues in the distributed and centralized systems environment with or without central management are surveyed. Along with an extensive survey is provided for the most recent work on DD concerning security and privacy issues, and comparison among in-band and out-band DD is performed.

Sivaram, M.; et al. [13] improved the quality of service (QoS) by enhancing the capability of the DBTMA for better network service in the MANETs. The proposed method uses an improved DBTMA called Retransmission Dual Busy Tone Multiple Access (RDBTMA) protocol. This is based on two elements namely: busy tones and Ready To Send/Clear to Send (RTS/CTS) dialogues. In addition to this fast retransmission, a strategy is used further to improve its effectiveness. The retransmission strategy is adopted using negative acknowledgment after the collision occurred by the hidden nodes. A hidden node, where the collision occurs at access point, listens to the NACK signal and uses the signal to determine the requirement fast retransmission scheme.

Mahmud, I. and Cho, Y.; [14] proposed a novel adaptive hello interval scheme—energy efficient hello (EE-Hello)—based on available mission-related information, such as the volume of the allowed airspace, number of UAVs, UAV transmission range, and UAV speed and present a method to decide the distance that a UAV needs to travel before sending a hello

message and also specify a technique to determine the number of UAVs necessary to achieve specific network requirements, such as packet delivery ratio or throughput, with the expenditure of minimum energy.

Ayub, M.S.; et al. [15] defined that in FANETs, the routing protocols send hello messages periodically for the maintenance of routes. However, the hello messages that are sent in the network increase the bandwidth wastage on some occasions and the excessive number of hello messages can also cause the problem of energy loss. Scarce works deal with the problem of excessive hello messages in dynamic UAVs scenarios, and treat several other problems, such as bandwidth and energy wastage simultaneously. Generally, the existing solutions configure the hello interval to an excessive long or short time period originating delay in neighbors discovery. Thus, a selfacting approach is necessary for calculating the exact number of hello messages with the aim to reduce the bandwidth wastage of the network and the energy loss; this approach needs to be low complex in terms of computational resource consumption. In order to solve this problem, an intelligent Hello dissemination model, AI-Hello, based on reinforcement learning algorithms, that adapts the hello message interval scheme is proposed to produce a dense reward structure, and facilitating the network learning.

Lee, S.; et al. [16] presented a fuzzy logic-based routing scheme for flying ad hoc networks. The proposed routing scheme has two phases: route discovery phase and route maintenance phase. In the first phase, we propose a technique for calculating the score of each node in the network to prevent the broadcast storm problem and control the flood of the control messages, which have been broadcast to discover a new route in the network. This score is calculated based on various parameters such as movement direction, residual energy of nodes, link quality, and node stability. Moreover, in the route selection process, we design a fuzzy system to select routes with more fitness, less delay, and fewer hops for data transfer. The second phase includes two steps: preventing route failure in order to detect and modify paths at the failure threshold, and reconstructing failed routes in order to recognize and quickly replace these routes.

Hajian, E.; et al. [17] proposed a novel SDN architecture aimed at reducing load distribution and prolonging lifetime, which consists of different components such as topology, BS and controller discovery, link, and virtual routing. Accordingly, a new mechanism is proposed for load-balancing routing through SDN and virtualization. Through direct monitoring of the link load information and the network running status, the employed OpenFlow protocol can determine load-balancing routing for every flow in different IoT applications. The flows in different resource applications can be directed to a base station (BS) via various routes. This implementation reduced the exchange of network status and other relevant information.

Praptodiyono, S. et al. [18] proposed Trust-ND with reduced complexity by combining hard security and soft security approaches to be implemented on securing IPv6 link-local communication. The experimentation results showed that Trust-ND managed to successfully secure the IPv6 Neighbour Discovery. However, the standard of the protocol does not specify any security mechanism but only recommends the use of either Internet Protocol Security (IPSec) or Secure Neighbor Discovery (SEND) that has drawbacks when used within IPv6 local network.

Amlak, G.M.H.; et al. [19] reviewed 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. It involved 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.

Sarma, S.; [20] provided a taxonomy for the IPv6 Neighbor and Router Discovery threats, describe two new cryptographic methods, Cryptographically Generated Addresses and Address Based Keys, and discuss how these new methods can be used to secure the Neighbor and Router discovery mechanisms. In this process will provide a certificate of ownership of IP address on network Interface card and Public key to provide authorization. On the other hand, it will also reduce the network load.

IV. DHCP BASED NDPSEC

The proposed NDPsec is designed to authenticate NDP messages. Accordingly, the NDPsec is evaluated and compared against Standard NDP, SeND, Match-Prevention, and TrustND mechanisms in terms of

(i) performance which includes processing time for generating IPv6 address, verifying and generating NDP messages, and

(ii) penetration test. This section shows the NDPsec experiments.

Experiments on a local network were conducted to evaluate the functioning and performance of the proposed NDPsec mechanism. The network topology, which comprises two hosts, one router, and one attacker.

Table 1: Hardware and software requirements for the testbed environment.

Item Name	CPU	Memory	Operating System
Host A	Intel Core i5	2 GB	Ubuntu
Host A	Intel Core i5	4 GB	Windows
Attacker Host	Intel Core i5	4 GB	Ubuntu
Switch	Cisco Catalyst 2960 Fast Ethernet		

Router	Cisco Router C7200

The hosts and router were modified to use NDPsec. The NDPsec is developed by using the python programming language. The Python-based cryptography library is utilized for the Ed25519 digital signature algorithm. The attacker runs on Kali Linux, which is used for Penetration Testing. IPv6 attacks are carried out using Scapy and flood_router26.c, whereas Wireshark is used to monitor network activities. In order to protect the RA message, the router's public key is pre-configured on all hosts in the network as the proposed mechanism does not provide a mechanism to distribute the public key of the router. The specifications of the hardware and software used for deploying the testbed environment are presented in Table 1.

The mechanisms discussed in the section below is to solve security problems with NDP processes require an excessive amount of time to process NDP messages, which attackers may use to flood the network with these messages and launch a DoS and MITM attacks in the link-local network.

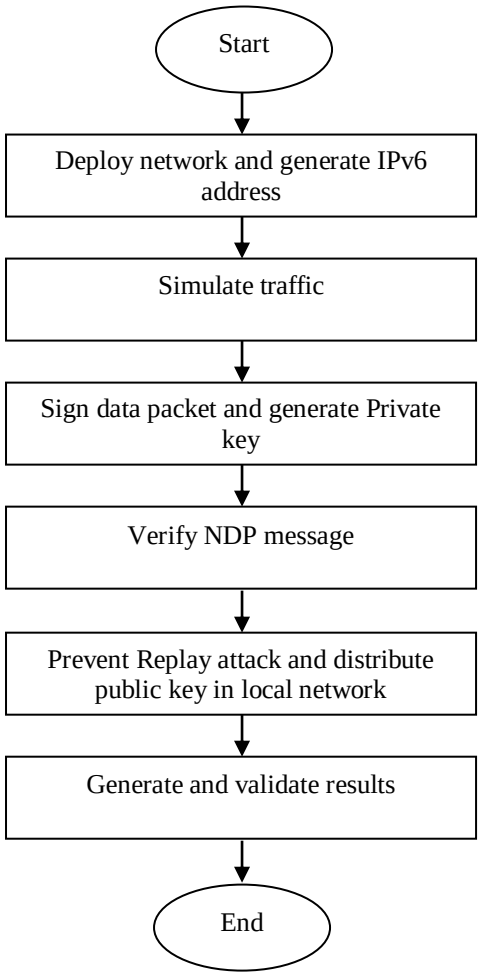

Fig 1: Flow of Work

Generating IPv6 Address

This step aims to generate IPv6 address for the host in the link-local network. In IPv6 network, SLAAC is used to generate an IP address and configure itself after checking the DAD process.

Secure Option

The step aim to append NDPsec parameters with NDP messages without compromising the original structure of NDP messages. NDPsec uses a digital signature to sign the NDP messages and hence, achieves authentication and integrity required to protect NDP messages from being attacked. Each NDP message is required to carry additional information such as a digital signature, the public key, etc., which is usually not seen in standard NDP messages.

Security in NDPSec

The primary goal is to integrate NDPsec parameters seamlessly with NDP messages while preserving the original NDP message structure. NDPsec employs digital signatures to sign NDP messages, ensuring authentication and integrity to safeguard against potential attacks. Each NDP message must include additional information, such as a digital signature and the public key, which is typically absent in standard NDP messages. Utilizing the option field, known as Secure-option, is proposed for conveying this additional information without altering the standard NDP message format. Secure-option encompasses four key fields: RDM, RDM-Info, LF, and DS. The main purpose of introducing this option is to distinguish legitimate NDP messages from unauthorized ones. Table 2 illustrates the structure and format of the Secure-option and its associated fields.

Type	Length	RDM (2 Bytes)
RDM – Info (4 Bytes)		
RF (24 Bytes)		
DS (32 Bytes)		

Table 2: Secure Option and its field

The Secure-option comprises 68 bytes divided into five fields as follows:

Type: A 1-byte identifier indicating the option type carried by the NDP message. In the case of the Secure-option, the type is set to 253, designated for experimental use.

Length: A 1-byte field indicating the total length of the Secure-option, inclusive of the type and length fields, measured in 8-byte units (64 bits). With the total length of the Secure-option being 68 bytes, the Length field is assigned a value of 8.

RDM: A 2-byte field indicating the replay detection method utilized within this Secure-option.

RDM-Info: A 4-byte field providing replay information specific to the Replay Mode.

RF: This 24-byte field stores the generated RF during the initial step, which will later be combined with the IPv6 address.

DS: A 32-byte field carrying the signature value resulting from the network layer.

Signing NDP Message

This step aims to explain how the sender of the IPv6 host signs the NDP message. The NDPsec messages must be digitally signed with the private key generated in step one to prevent them from being altered in transit or spoofed by threat actors in order to launch cyber-attacks.

Verify NDP Message

This step attempts to verify the NDP message by validating the digital signature that was included in the message. Upon receiving the NDP messages, the receiving host must first verify that the NDPsec option field is present in the NDP message; otherwise, the message must be regarded as an attack initiated by the threat actors and must be rejected immediately

Prevent Replay Attack

Replay attacks are one of the most common types of attacks against authentication security mechanisms. In replay attacks, the attacker uses an old authentication message to configure the victim with old configuration information, leading to a DoS attack or MITM.

V. RESULT AND COMPARISON

The designers of IPv6 initially assumed trust among all users within a local area network. However, this assumption doesn't hold true in public environments like airports or coffee shops, where users cannot be automatically trusted. Additionally, employees themselves can pose security risks. Therefore, understanding and analyzing NDP (Neighbor Discovery Protocol) attacks is crucial to mitigating them and safeguarding networks.

To study and analyze the normal behavior of the NDP protocol, a testbed employs both Windows and Linux operating systems. This approach is necessary because modern operating systems are required to support IPv6. Network packets are captured and filtered using Wireshark to isolate NDP packets, allowing focused analysis of NDP behavior and message flow. These captured packets are then compared against the expected behavior outlined in the protocol's RFC (Request for Comments), confirming adherence to protocol specifications by both Windows and Linux systems.

Evaluation

The experiment aims to measure the processing time required for generating an IPv6 address across various protocols: Standard NDP, SeND, Match-Prevention, Trust-ND, and NDPsec. Processing time is calculated by subtracting the ending time of IPv6 address generation from the starting time of the verification process. To ensure the reliability of the findings and account for potential interference from other OS processes, each experiment is repeated 25 times.

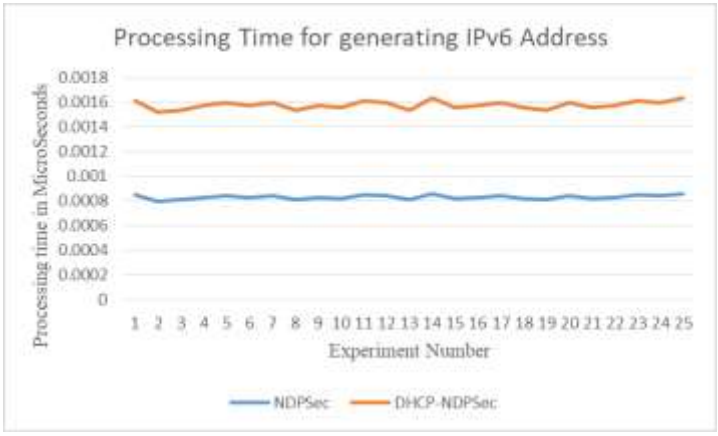

Figure 2: Processing time for generating IPv6 address

Figure 2 depicts a line chart illustrating the IPv6 address generation process. The results indicate that SeND exhibits the highest processing time due to its utilization of RSA digital signatures and CGA, both of which entail computationally intensive operations. Conversely, protocols such as Standard NDP, Match-Prevention, and Trust-ND demonstrate nearly identical processing times, attributed to their use of the Privacy Extensions mechanism. NDPsec registers slightly higher processing times as it employs DHCP-Ed25519 for IPv6 generation.

Traffic Overhead

This experiment aims to measure the traffic overhead associated with Standard NDP, SeND, Trust-ND, and the proposed NDPsec mechanism. The total message size for NDP messages has been calculated by summing the message sizes for the different mechanisms, which include NA, NS, RS, RA, and R. The traffic overhead is calculated by comparing it to the total size of Standard NDP messages (i.e., baseline). Table 2 shows that a larger message size can significantly influence network traffic.

	NDPSec					DHCP-NDPSec				
	NA	NS	RA	RS	R	NA	NS	RA	RS	R
Overheads	156.26	142.12	147.32	145.23	148.12	151.23	137.23	138.34	139.35	143.22

Table 3: Overheads in NDPSec vs DHCP-NDPSec

Technique / Overhead	NDPSec	DHCP-NDPSec
NS	149	146
NA	143	139
RS	132	128
RA	186	175
R	238	225

Table 4: Summation Overheads in NDPSec vs DHCP-NDPSec

Therefore, using a small message size can improve the performance of the network. The existing mechanisms have large message sizes due to their designs.

Address Resolution

In an AR spoofing attack, the attacker aims to spoof the NS message to inject the attacker's MAC address. If Host A saves

the attack's MAC address in the neighbor cache table, the attack is deemed successful; otherwise, the attack is considered unsuccessful, and the message is discarded.. Table 5 summarizes the outcome of the experiments.

Technique / Metrics	NDPSec	DHCP-NDPSec
Successful Number	0	0
Successful Rate	0%	0%

Table 5: DoS-on-DAD experiment results

The attacks sometimes fail because both mechanisms (Standard NDP Match-Prevention, and Trust-ND) cannot distinguish between messages sent by a legitimate host and those sent by an attacker, in consequence, the host configures itself with a legitimate message. Furthermore, the NDPsec and DHCP-NDPsec successfully thwarted AR attacks because an attacker cannot spoof IPv6 addresses without having a valid key to sign the messages.

VI. CONCLUSION

The proposed DHCP-NDPsec mechanism has almost the same processing time for generating IPv6 addresses as compared to other mechanisms, including the Standard NDPSec. The SeND requires a high processing time for generating IP addresses because it employs RSA and CGA algorithms. The DHCP-NDPsec's IP generation process relies on the Ed25519 digital signature keypairs, which is considerably faster than the NDPSec's RSA and CGA. Based on the experiments, it is clear that DHCP-NDPsec can reduce the complexity of the process while generating and verifying NDP messages compared with SeND mechanism. The DHCP-NDPsec is around two times faster than NDPSec. Consequently, this leads to limitations for using NDPSec in mobile or IoT devices with limited resources. Besides reducing the complexity, the NDPsec also reduced the traffic overhead by around 57.08% compared to the NDPSec mechanism. Hence, DHCP-NDPsec significantly reduces communication cost and bandwidth utilization. Furthermore, the Standard NDPSec, MatchPrevention, and Trust-ND mechanisms have less processing time when generating and verifying messages and generate less traffic size. On the other hand, the NDPSec prevents DoS-on-DAD, Address Resolution, and Redirect attacks, like the proposed mechanism. However, NDPSec failed to prevent RA flooding attacks. Although NDPSec prevents the attacker from injecting RA messages into the IPv6 host, the attacker consumes the host's CPU, causing the host to stop responding to any valid incoming message while under attack. In contrast, the proposed DHCP-NDPsec mechanism is immune against all the NDP attacks, including the RA flooding attack, as it is designed to be a lightweight process and preserve security; accordingly, using DHCP-NDPsec can provide authentication for the NDP messages.

Future Scope

The future scope of the NDPSec algorithm involves several potential directions for further development and enhancement:

DHCP-NDPSec could be integrated with other security technologies and protocols to create a more comprehensive security framework. For example, integration with Intrusion Detection Systems (IDS) or Security Information and Event Management (SIEM) systems could provide enhanced threat detection and response capabilities.

REFERENCES

[1]. Al-Ani, A.; Al-Ani, A. K.; Laghari, S.A.; Manickam, S.; Lai, K.W.; Hasikin, K.; "NDPsec: Neighbor Discovery Protocol Security Mechanism", IEEE Access, Volume: 10, 2022, page: 83650-83663

[2]. Sun, H.; Meng, Z.; Wang, D.; Li, H.; "Fedab: A Low-Latency Energy-Efficient Proactive Neighbor Discovery Protocol in MLDC-WSN", IEEE Access, Volume: 10, 2022, page: 22843-22854

[3]. Luo, X.; Chen, Y.; Li, M.; Luo, Q.; Xue, K.; Liu, S.; Chen, L.; "CREDND: A Novel Secure Neighbor Discovery Algorithm for Wormhole Attack", IEEE Access, Volume: 7, 2019, page: 18194-18205

[4]. Ling, H.; Yang, S.; "Anole: An Adaptive Neighbor Discovery Under Urban Environments", IEEE Access, Volume: 6, 2018, page: 64817-64827

[5]. Mansoor, N.; Islam, A.K.M.M.; Zareei, M.; Rosales, C.V.; "RARE: A Spectrum Aware Cross-Layer MAC Protocol for Cognitive Radio Ad-Hoc Networks", IEEE, Access, Volume: 6, 2018, page: 22210-22227

[6]. Grajzer, M.; Glabowski, M.; "Neighbor Discovery ++— a Scalable and Robust Address Auto-Configuration for Future Internet of Things Networks", IEEE Access, Volume: 7, 2019, page: 61083- 61108

[7]. Bahashwan, A.A.; Anbar, M.; Hasbullah, I.H.; Alashhab, Z.R.; Salem, A.B.; "Flow-Based Approach to Detect Abnormal Behavior in Neighbor Discovery Protocol (NDP)", Volume: 9, 2021, page: 45512- 45526

[8]. Pozza, R.; Nati, M.; Georgoulas, S.; Moesnner, K.; Gluhak, A.; "Neighbor Discovery for Opportunistic Networking in Internet of Things Scenarios: A Survey", Special Section On Artificial Intelligence Enabled Networking, IEEE Access, Volume: 3, 2015, page: 1101-1131

[9]. Shi, Z.; Sun, R.; Lu, R.; Qiao, J.; Chen, J.; Shen, X.; "A Wormhole Attack Resistant Neighbor Discovery Scheme With RDMA Protocol for 60 GHz Directional Network", IEEE Access, IEEE Transactions On Emerging Topics In Computing, Volume: 1, No: 2, 2013, page: 342-352

[10]. Ahmad, A.S.A.M.S.; Hassan, R.; Othman, N.E.; "IPv6 Neighbor Discovery Protocol Specifications, Threats and Countermeasures: A Survey", IEEE Access, Volume: 5, 2017, page: 18187-18210

[11]. Al-Ani, A.K.; Anbar, M.; Al-Ani, A.; Ibrahim, D.R.; "Match-Prevention Technique Against Denial-of-Service Attack on Address Resolution and Duplicate Address Detection Processes in IPv6 Link-Local Network", IEEE Access, Volume: 8, 2020, page: 27122-27138

[12]. Hayat, O.; Ngah, R.; Kaleem, Z.; Hashim, S.Z.M.; Rodrigues, J.P.C.; "A Survey on Security and Privacy

Challenges in Device Discovery for Next-Generation Systems", IEEE, Volume: 8, 2020, page: 84584-84603

[13]. Sivaram, M.; Porkodi, V.; Mohammad, A.S.; Manikandan, V.; Yuvraj, N.; "Retransmission DBTMA Protocol With Fast Retransmission Strategy to Improve the Performance of MANETs", IEEE, Volume: 7, page: 85098-85109

[14]. Mahmud, I.; Cho, Y.; "Adaptive Hello Interval in FANET Routing Protocols for Green UAVs", IEEE, Volume: 7, 2019, page: 63004-63015

[15]. Ayub, M.S.; Adasme, P.; Melgarejo, D.C.; Rosa, R.L.; Rodriguez, D.Z.; "Intelligent Hello Dissemination Model for FANET Routing Protocols", IEEE, Volume: 10, 2022, page: 46513- 46525

[16]. Lee, S.; Ali, S.; Yousefpoor, M.S.; Yousefpoor, E.; Lalbaksh, P.; Javaheri, D.; Rahmani, A.M.; Hosseinzadeh, M.; "An Energy-Aware and Predictive Fuzzy Logic-Based Routing Scheme in Flying Ad Hoc Networks (FANETs)", IEEE, Volume: 9, 2021, page: 129977- 130005

[17]. Hajian, E.; Khayyambashi, R.; Movahhedinia, N.; "A Mechanism for Load Balancing Routing and Virtualization