UTM UNIVERSITI TEKNOLOGI MALAYSIA
INTERNATIONAL JOURNAL OF INNOVATIVE COMPUTING
ISSN 2180-4370
Journal Homepage : https://ijic.utm.my/

A New Concept of Duplicate Address Detection Processes in IPv6 Link-Local Network

Adamu Abubakar Ibrahim*, Rawad Abdulkhaleq Abdulmolla Abdulghafor & Sharyar Wani
Department of Computer Science
International Islamic University Malaysia
Kuala Lumpur, Malaysia
Email: adamu@iium.edu.my

Submitted: 6/4/2022. Revised edition: 11/9/2022. Accepted: 14/9/2022. Published online: 20/11/2022
DOI: https://doi.org/10.11113/ijic.v12n2.368

***Abstract*—The Neighbor Discovery Protocol (NDP) enables nodes on the same IPv6 link to advertise their existence to their neighbors and learn about their neighbors' existences in an IPv6 link-local network. Duplicate Address Detection (DAD) on NDP is used to determine whether or not an address requested by a node is already in use by another node. The Neighbor Solicitation (NS) and Neighbor Advertisement (NA) operations are associated to DAD checks in order to ensure that each interface within the transmission session is unique. Unfortunately, NS and NA operations have a significant disadvantage in that they are based on insecure architectures and lack verification procedures for determining whether incoming messages originate from a valid or illegitimate node. This will eventually allow any node in the same link to be manipulated during NS and NA message transmission sessions. Despite some attempts to secure the entire NDP operations, they still suffer from computing resources requirement for their operations. As a result, this study proposes an Initial Neighbor Inspection (INI) on DAD operation. The proposed techniques allow for an initial round of verification of the nodes on the same link before a broadcast request on the existence of neighbors, which is followed by another round of learning about neighbors' existences. Conclusively, using this idea, as a simple verification will indicate the presence of neighbors, we may restrict solicitation and advertising to only those who are eligible. This means that the computational processing time for NS and NA on DAD operations would not rise.**

***Keywords*—Neighbor discovery protocol, neighbor solicitation, neighbor advertisement, IPv6**

I. INTRODUCTION

Internet Protocol (IP) addresses are a logical way to identify and locate computers and devices, as well as a means of directing Internet traffic [1]. IP addresses come in two types: IP Address Version 4 and IP Address Version 6, respectively (IPv4 & IPv6) [2]. Typically, sending a message to a specific destination in an end-to-end local connection or a remote connection requires the use of either IPv4 or IPv6. Both IPv4 and IPv6 addresses can be used, and the data packet is always created at the source host before being forwarded using either IPv4 or IPv6. In IPv4, the source device uses its own subnet mask, along with its own IPv4 address and the destination IPv4 address, to make a decision for forwarding the packet if the destination target is within a local network [3]. In IPv6, on the other hand, the local router broadcasts the local network address (prefix) to all devices connected to the network IPv6 was created by the Internet Engineering Task Force (IETF) in order to address the IPv4 address exhaustion problem and improve connectivity. Because of this, IPv6 will eventually replace IPv4 as the most commonly used Internet Protocol. IETF selected IPv6 as a Draft Standard in December 1998, which was adopted as an Internet Standard on July 14, 2017 [4]. Currently, IPv6 is the most flexible communications protocol, and it is expected to replace IPv4 in most cases.

The address space provided by IPv6 is enormous. It also relies on NDP to perform address resolution and router discovery and redirection functions using ICMPv6 in IP version 6. Similar to ARP in IPv4, ICMPv6 NDP uses "Neighbor Solicitation" and "Neighbor Advertisement" to resolve addresses in device-to-device connections. When an IP address is used to obtain the final destination's MAC address. Routing messages such as "Router Solicitation" and "Router Advertisement" are used to communicate with routers. Router discovery is typically used for dynamic address allocation and "stateless address autoconfiguration (SLAAC)". Resolving MAC addresses makes use of the Neighbor Solicitation and Neighbor Advertisement messages in ICMP version 6. Similar

to the ARP Requests and ARP Responses used by ARP for IPv4, this is a type of ARP communication

DAD is one of the NDP functions that determines whether the IPv6 addresses of two or more nodes are the same or conflicting. The DAD procedure has also been established to accommodate thousands of different devices on a single network connection [5]. The IPv6 network's ability to accomplish this is widely regarded as one of its most critical features. As a network link is shared, it ensures that IP addresses do not conflict with one another. There is a potential of being into a trap of a Denial-of-Service (DoS) attack on the DAD process. That is, DAD, on the other hand, is vulnerable to Denial of Service (DoS) attacks because NDP messages aren't verified during the transmission session, that is during the NDP process, an attacker will exploit the process by forcing the host to respond to each neighbour solicitation (NS) with a fake neighbour advertisement, this threat prevents the host from configuring its IP address (NA). Existing solutions are difficult to implement because of their high level of complexity and security, as well as the fact that they require changes to the NDP or have a single point of failure [6].

This study considers the fact that while for every IPv6 transmission, the MAC address of a device known to have an IPv6 address is determined using IPv6 NDP, then "Initial Neighbor Inspection" (INI) check of the NDP is established. Due to the obvious inefficiencies of NDP operations and the lack of authentication methods, it is impossible to determine whether receiving messages originate from a legal or illegitimate node. It was because of this that the current study looked into how any compute node on the same network might be pre-checked right before NDP activities in transmission sessions took place. This will aid in the security of the entire NDP operation while also reducing the load on computing resources.

This research has contribute toward giving a straightforward verification that will point to the existence of neighbors in DAD. In addition to this, it contributes to bringing attention to the restriction of advertising and solicitation to just those who are eligible. In addition to that, the research makes a contribution by providing information regarding the performance of the computational processing time for NS and NA on DAD procedures.

This paper has five sections in total, including the current one. The remaining sections are as follows: Section 2 presents and discusses the pertinent supporting literature within the related work. Section 3 presents the research experiment and results. Section 4 then discusses the research. Section 5 presents the work's conclusion at its final stage.

II. RELATED WORK

The current trend of research associated with NDP lies with the possibilities of investigating whether or not messages originating from unauthorized computing nodes can be determined. This opens up new possibilities for determining the degree of IPv6 link-local addresses ability to allows nodes to discover and broadcast an IPv6 address that corresponds to a certain link-layer address. There are many previous research studies on securing solicited message, specifically ICMPv6 NS and NA messages that are used for MAC address resolution. Crucial to that is the work of Al-Ani el al. [7], which proposes match-prevention approach during DAD to verify incoming messages and discard fake messages prior to further processing, thereby preventing a DoS attack during DAD in an IPv6 link-local network. Machana and Narsimha [8] took a similar tack, arguing that while researchers have developed numerous techniques to address DAD vulnerabilities, they appear to be neither robust nor performance-oriented, and thus there is a need for an approach that detects and mitigates attacks while consuming minimal bandwidth and overhead in DAD.

Prior to addressing NS issues, it was proposed in Najjar *et al*. [9] that an initial security mechanism should be used to monitor network traffic. It was revealed that by investigating NDP behaviour using an extended finite state machine to model the main NDP processes and to detect abnormal behavior, a strict anomaly detection will be established. Unfortunately, In order to detect NDP anomalies, NDPmon requires the deployment of a central server in a LAN. Emails are sent to the administrator via a report or in the system log. The computing processes of the entire transmission session will be severely hampered as a result of this, hence it is difficult to identify other infractions, such as IP or MAC address spoofing, a faked IP address can be used to flood a network with NDP messages, making INDPmon unable to distinguish between a real and spoofed one [7]. Although, a combination of contemporary high-speed active probing and dynamic search space reduction makes it possible to keep track of IPv6 clients as they move around the network, yet, a transmission session can be compromise by the intended anti-tracking capability of these commonly used technologies [10]. A hash-based strategy for protecting NDP NS and NA messages was proposed by Usman *et al*. [11]. This technique made use of SHA-512 for the encryption of target IPv6, as well as the usage of only 64-bits of hashed data in the NS and NA messages. While evaluating the technique it, there is an issue with bandwidth consumption and processing time that cannot be accepted in order to protect DAD from denial of service (DoS) attack. The authors of El Ksimi and Leghris [12] presented a solution for protecting a target IPv6 address by employing a combination of strong hash key and robust encryption technology, which was to be employed before transmitting any NS messages, in a similar vein. The outcome demonstrates that a good security mechanism has been put in place, but the computing complexity is extremely high.

There is no doubt that the IPv6 addressing mechanisms improve the efficiency of transmission, but it could do more if a machine learning approach could be applied to IPv6 addresses as proposed by Roychaudhary and Shahapurkar [13] in order to minimize the security issues faced by the IPv6 operation. Following this, using KNN optimization in machine learning based on the measure of the influence of the reverse distance, Alharbi *et al*. [14] suggest a method for addressing IPv6 security issues while simultaneously improving the overall detection performance of IPv6 network traffic detection.

To this day, "Secure NDP (SeND)" and "Trust-NDP (Trust-ND)" continue to be the most commonly utilised strategies in

NDP header extension in order to protect NDP protocols from being compromised [11]. It has been determined that "SeND" provides various new options to the NDP protocol, including the option to verify addresses produced using cryptographic methods [8]. Unfortunatley, it has been revealed that the security choices of SeND make implementation difficult because they do not allow the identification of a valid host to be determined, allowing attackers to intercept NDP messages, modify them, and ultimately compromise the target hosts. Because of these shortcomings of SeND, particularly its complexity, hostile hosts can perform denial-of-service (DoS) attacks, such as flooding attacks, during NDP processes, allowing them to take advantage of the approach. In order to address this issue, Praptodiyono *et al*. [15] introduced a novel solution known as Trust-ND for protecting DAD processes and securing the exchange of NDP messages between hosts in an IPv6 link-local network.

It is worth noting that the aforementioned previous research works [7–15] continue to place an emphasis on theoretical information on DAD as well as the blocking access of transmission sessions that does not involve in the DAD processes. However, there hasn't been much discussion about how to apply diligent checking operations in actual applications. As a result, following the previous successful applications of the Match-prevention technique for preventing DAD by Al-Ani *et al*. [7] and the DAD-match technique by Al-Ani *et al*. [16] for securing DAD, and motivated by the works of [1–5], this paper presents an Initial Neighbor Inspection approach to DAD operation by establishing an initial round of verification of the nodes on the same link before a broadcast request on the existence.

III. EXPERIMENT AND PRESENTATION OF THE RESULTS

The current study's research methodology is based on conceptualizing a new approach for INI in order to secure DAD against attacks in an IPv6 link-local network, and then experimenting a certain approach. The simulation of some scenarios involving the DAD processes was then performed.

A. Conceptualization

IPv6 link local address will be assigned to the new host as soon as it connects to a local network by NDP. In most cases, the new host must first complete DAD before being assigned a specific IPv6 address (see Fig. 1). As the new host requesting for IPv6 address is introduce, the IPv6 link local address for it can be configured manually on an interface, or the device will automatically generate its own using Extended Unique Identifier (EUI-64) where the 48 bits MAC address of the device will be utilised, in that 16 bits (FFFE) hexadecimal will be inserted in the middle of the 48 bits and then invert the 7th bits of the first 24 bits of the MAC address in order to generate the EUI-64 of IPv6 link local interface ID and then append to the FE80::/10 allocate range of the IPv6 link local address. This enables IPv6-enabled devices to communicate with other IPv6-enabled devices on the same subnet when they are on the same network. Communication with the default gateway is included in this category as well.

Before any transmission can begin, a DAD will be performed on the newly generated link local IPv6 address. As a result, once an IP address has been generated, it will not be able to proceed with transmission until it has been verified as unique by the DAD processes, at which point a NA message will be broadcast to the network's local link. This is done in order to prevent IP addresses from conflicting with one another on the same network link. Essentially, this broadcast is in the form of a question, asking if there is any node in the network that is using an IPv6 address that was either manually or automatically configured. As a result, a NA message will only be responded to if and when there is a match. Unless there is another host that is already using that particular IP address, of course. In Fig. 2, it can be seen that when a new host is added to the network, an NS message is broadcast to the network and a NA message is received indicating that the particular address has already been assigned (fe80::dabc: fe13: 5246: 1002). As a result, the new incoming device will not be able to acquire that address. On the other hand, if no NA message is received after a specific amount of time that varies depending on the device (ranging from 4 to 600 seconds), it indicates that the IPv6 address that was generated for the device should be considered unique because it is not being used by any of the other hosts on the network.

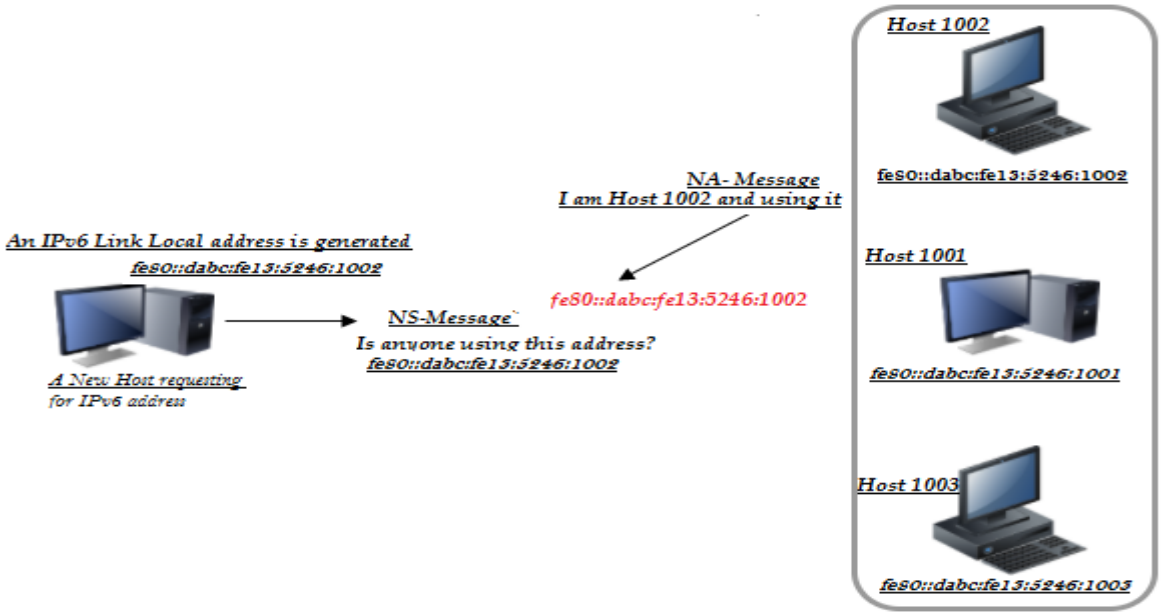


Fig. 1. DAD operation in IPv6 link-local network

In the event that a new node is added to the network, a similar technique will be used. As a result, the DAD process will be performed for each incoming network node, resulting in the creation of a record for that particular DAD process. As a result of creating the record, a mechanism for keeping track of any new incoming devices to the network will be provided, which is why it is used as a method of detecting duplicates. Unfortunately, because the NS message is broadcast over the local link, intruders and other eavesdroppers will have an opportunity to listen in on the NS and NA conversation on DAD. NS message broadcast over local link On the one hand, the disadvantage is that an attacker could either claim that there is a duplicate when there is none, or vice versa, depending on the situation. This could result in an attack such as a Denial of Service attack. As a result, this paper proposed a prior check and monitoring of the NS message transmission session.

The propose conceptual framework is presented in Fig. 2. New notes that allow access to the same link as other nodes on the network should be able to execute an initial transmission to detect other computing notes on the network, as part of the suggested conceptual approach. That is the network should be able to send out an initial transmission to detect the presence of other computing notes on the network, which is what the proposed conceptual approach is based on. Before the NS and NA message transmission sessions, there will be a pause. This study conceptualizes sending and ICMPv6 with FE80::n:x/10 in the first round, and FE80::n:y/10 in the second round, where n is the beginning range of the IPv6 link local address and x and y are within the subnet of the configured address for the first round and y for the second round, respectively, and n is the beginning range of the IPv6 link local address. The primary goal is to determine whether or not a location is reachable or not. That is, all nodes must respond to a previous multicast transmission before the solicited-node multicast transmission can be sent. It will be necessary to conduct another round of testing for reachability if no reachability is found in the first round. This time, the y range will be different from the one that was used in the first round. In addition to the benefits of prior communication before a multicast transmission to a solicited node, the transmission session can map those free IPv6 link-locals to by examining the available once and not sending NS. The NS message should be sent in order to receive the NA advertisement if the range contained within the y has been determined to be reachable. Also included will be a sorting process that will determine which parts of the range (from fe80::/10 to febf::/10) were not used and which parts will be saved in the buffer. Therefore, any new incoming node will be assigned an IPv6 address from one of the available ranges as a result of this. As a result, the NS message will be transmitted.

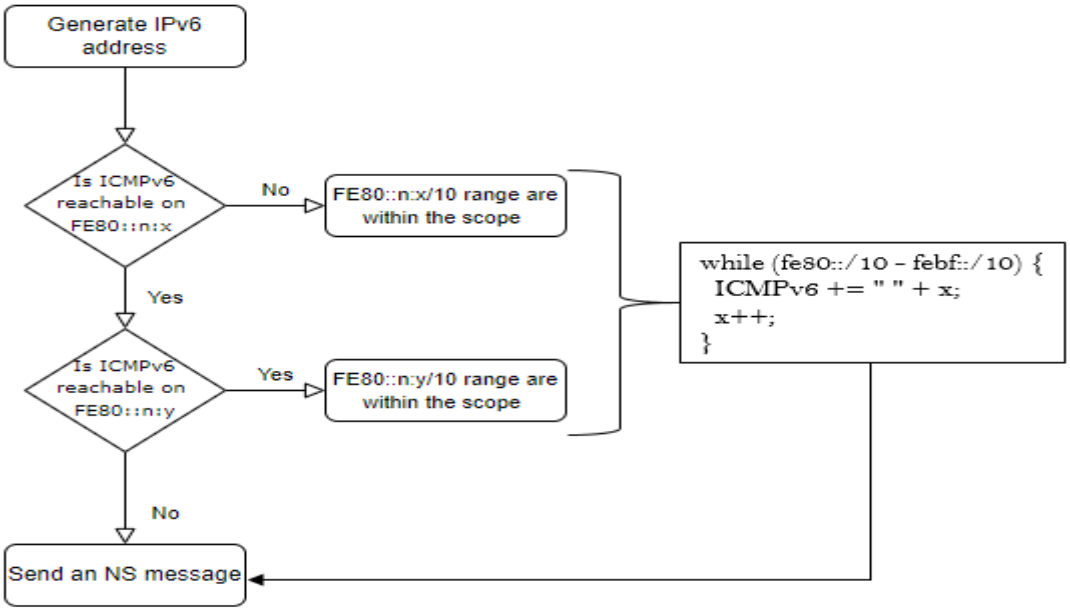


Fig. 2. The conceptual framework

B. Experimental Simulation and Presentation of the Results

An experimental testbed was established running on virtual network security sandbox of multi-virtual machine environment useful for security analysis and testing. This multi-VM environment comprising of multicore processors and large amounts of RAM in order to take advantage of the ability to use virtualization. This has allowed the research to utilized several computing nodes from different virtual machines to operate inside one physical computer. a virtual workstation as the main central workstation which serves as a container for holding the local area network environment where IPv6 link-local connections will be established alongside a Wireshark and Iperf for capturing the transmission session. Both Wireshark and Iperf are network monitoring tool for capturing variety of transmission session events that include everything that is involve in the transmission. Additional VMs: kali_linux, Python-IDLE, metasploitable, and security_onion. The kali_linux has built-in THC-IPv6 attacking toolkit support. THC-IPv6 is the central tool that detect-new-ip6 Usage that can start ICMP6 DAD detection. It is a useful tool set to attack the inherent protocol weakness of IPv6 and ICMP6. The network scenarios designed inside virtual workstation and utilized four mininet setup as shown in Fig. 3. Where the is need for stashing transmission within the local network.

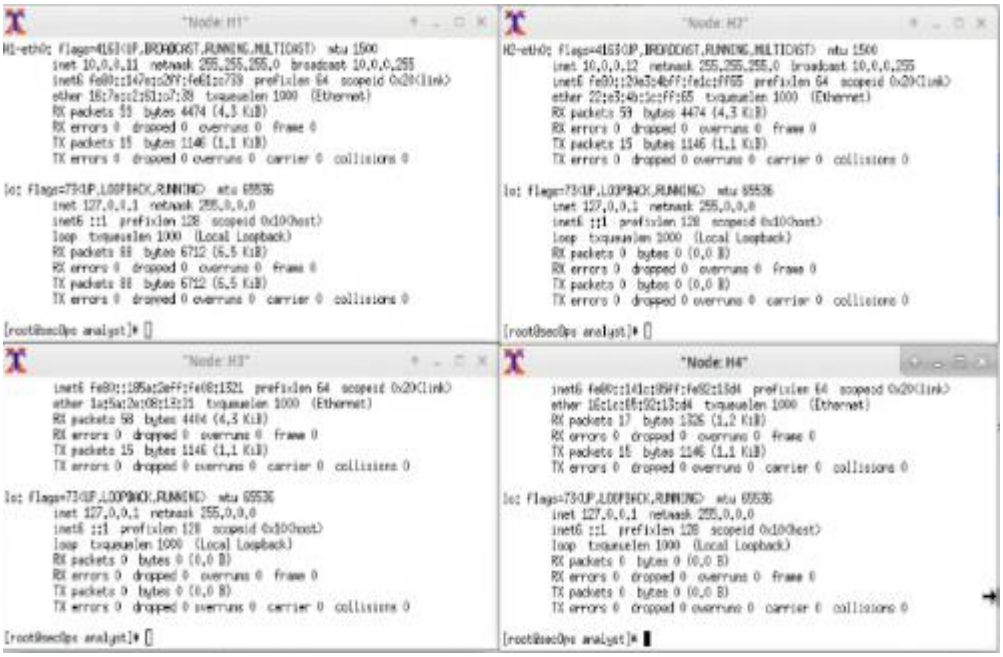
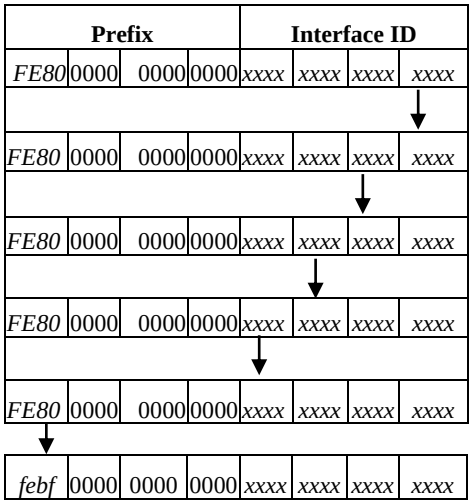


Fig 3. The four mininet setup network scenarios

At the start of the experiment, all hosts should first generate IP addresses that are valid IPv6 link local addresses for this network in the range "fe80::/10 – febf::/10." In this range, there will be a preliminary examination to determine whether there are any linkages between this research and other trials in progress. This stage checks to see that the IPv6 link local addresses that are meant to be used are within the range of IPv6 link local addresses that are available to be utilized. Prior to the introduction of the NS and NA messages, there was no method to predict the arrival of incoming ICMPv6 messages, which implies that there is a possibility that the period may be exploited to conduct an inspection. The round of inspections is now taking place inside the range of IPv6 link local addresses, as shown in Table I. That is, a transmission was initiated among them.

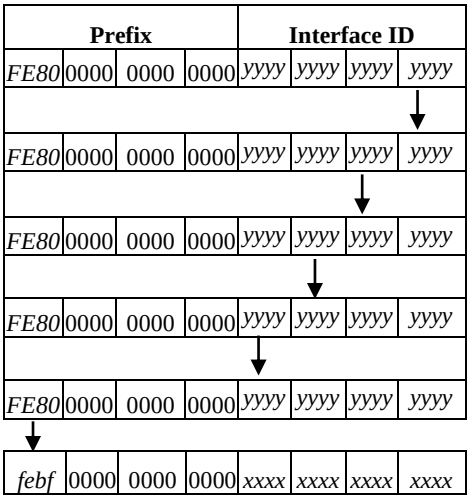
TABLE I. THE FIRST ROUND INSPECTION



After searching for access to a specific range of links on the network to discover whether or not there are already additional nodes on the network, a second round will be conducted to ascertain whether or not the searches conducted in the previous round were complete or covered. It is vital for all nodes to react by the end of this second round since it is the last remaining component inside the range of the IPv6 link-local address (see Table II). This is required in order to undertake reachability testing within the set of address ranges.

It is possible to verify that all of the IPV6 addresses that will be used have been identified after the first and second rounds of inspections of possible IPV6 addresses have been completed. The DAD process that will follow will ensure that the prior inspection results in the discovery of the available address, which will save time because there is assurance that DAD will not find a duplicate address as a result of the initial inspection, which highlighted the presence of the IPv6 link local address that was in use at the time of the initial inspection, and this will save money because there is assurance that DAD will not find a duplicate address as a result of the initial inspection, which highlighted the presence of the IPv6 link local address.

TABLE II. THE FIRST ROUND INSPECTION



As shown in Fig. 3, the workstation assigns link-local addresses to the four nodes (H1, H2, H3, and H4) that are connected to it via the link local network. Using Iperf and wireshark, which are both open source programmes, they are used in keeping track of what is happening during the transmission session on the entire transmission session. Due to the fact that Kali Linux is the attacker node, it will launch attacks from its IPv6 link-local address, which will be exploited prior to the deployment of the DAD protocol. A vulnerable server known as the "Metasplotable" will be exploited prior to DAD. In order to provide log analysis services for the entire connection for all of the victims together, "Security Onion" was used. It is possible to measure transmission performance both prior to and during the DAD process.

In addition, while the transmission was being established, an inspection of the entire link-local IPv6 addressess (FE80::/10 - FEbf::/10) within the four nodes was performed, and the corresponding addressess were returned with the addressess. The number of transmission messages was calculated based on the number of packets received and sent by both workstations and the attacker on the victim, respectively, during the transmission process. In accordance with the results of this transmission, the number of messages sent prior to the initial inspection and the number of messages sent after the inspection are analysed. When inspections are not performed, i.e., when the link-locals are not identified, the message sent increases the processing time for each transmission by 10.3 percent when compared to the message sent after inspections have been performed. This is due to the fact that the inspection reveals the presence of the IPv6 address and then eliminates the time required by DAD to capture, buffer, and report a duplicate.

IV. DISCUSSION

In light of the criticality of the DAD procedure, failure to complete it on time may result in a significant drop in the performance of network service operations, which may be

catastrophic. Furthermore, it has been claimed that it may be finished in advance and that, as a result, it may be feasible to reduce the latency that is associated with it [17]. The DAD process cannot be finished prior to the establishment of the transmission session, despite the fact that certain earlier study findings show that it can be completed prior to the establishment of the transmission session [18]. In spite of the fact that there is an attempt to optimise a transmission associated with the DAD process, it has been discovered that the optimistic IPv6 address should only be used when there is no other appropriate address available [19]. Following the specification, optimistic DAD is favourable since the DAD technique has a far greater chance of success than it does of failure in the vast majority of instances. However, system performance and security difficulties remain, and it is for this reason that the current research considers safeguarding the criticality of the DAD procedure, so that it does not fail to complete on time, in order to avoid a substantial decline in the performance of network service operations. As a result, it was suggested that an initial round of inspection of accessible IPV6 inside the link local address on the nodes in the connection be established first so that DAD process can be completed in advance, before the transmission session gets established. This would allow for the DAD to be finished earlier. It is feasible to eliminate the latency that is associated with the DAD process as a result of this.

The findings of this study have revealed an important result. In order to identify IPv6 link-local addresses, data packets were analyzed, and the relevant addresses were returned along with the data packets. Previously, it was demonstrated that the issuance of an IPv6 link local address to a new host does not indicate that the address is definitive after the host connects to a local network. In the vast majority of cases, it is important to validate the new IPv6 link local address with the other connecting node before proceeding. The process of checking for duplicates is done here. For the purposes of determining the total number of transmission messages transmitted, it was necessary to count the number of transmission messages sent by both workstations and the attacker, according to the results of the research that was conducted.

In addition, the research discovered that the IPv6 link local address can be configured manually on an interface if a new host requests one, or the device can generate its own automatically; however, in all cases, there is a requirement for duplicate checking within the local network. The findings of the study demonstrate that, because the IPv6 link-local addresses are known, they can be checked first against the ranges before being sent to the duplicate detection system. Thus, when devices on the same subnet with IPv6 capabilities are connected to the same network, they can communicate and exchange information that is used for recording researchability as well as keeping track of the addresses that are currently in use. So that when an address is assigned again, the one that was previously used will not even be considered for assignment in the first place. Moreover, the initial communication with devices will result in a better understanding of the addresses that are taken, making it impossible for an attacker to block those addresses. Furthermore, before any communication can take place, it is necessary to perform a DAD on the newly generated link local IPv6 address as a final check to ensure that the IP addresses are still present. This is necessary because it has now been established that an IP address will not be able to be used for transmission unless the DAD processes verify that it is unique. That is, despite the initial review, the DAD report is the final and most easily accessible report that will be used to determine whether or not to take action. As a result, IP addresses on the same network link are not permitted to conflict with one another, and DAD takes steps to ensure that there is no duplication of IP addresses. A new host joining the network should be assigned the specific IPv6 address that has not yet been assigned, provided that any IPv6 addresses that were either manually or automatically configured on a node in the link-local network are aware of their existence.

To summarize, the findings of this study indicate that transmission must include an opportunity for initial checking of duplicates prior to the final check in order to be effective. DAD's total time for each transmission for detecting duplicates is reduced by 10.3 percent when the initial check is performed. In other words, DAD is able to detect and report a duplicate IPv6 address in a shorter amount of time than in the past because the IPv6 address exists and the inspection confirms that it does in fact exist.

V. CONCLUSION

This paper presents a novel strategy for detecting duplicate IPv6 Link-Local Network addresses in IPv6 Link-Local Networks. It has been brought to the attention of the researchers that previous studies have concentrated on theoretical methods for DAD transmission sessions rather than conducting extensive inspections in practical systems. It was on this basis that they proposed a set of methods for confirming the existence of nodes on the same link before broadcasting a request to learn about the presence of neighbors and then conducting a second round of learning about the presence of neighbours, as described in this work. A preliminary check will determine whether or not there are any neighbours, and if so, whether or not this concept can be employed to ensure that only the most appropriate solicitation and advertising are launched. As a result, there would be no difference in the computational processing time for NS and NA on DAD procedures. According to the conclusions of the study, an analysis of all link-local IPv6 addresses is required and should be undertaken when the transmission is being created, and the matched addresses that are returned should be the ones that are subjected to further investigation and testing. It is necessary to take into consideration the number of transmission messages that have been successfully transmitted. In addition, the number of messages provided before and after the initial inspection is compared to the number of messages delivered as a result of the transmission session results. The time required for transmission processing increases by 10.3 percent when inspections are not performed (i.e., when the link-locals are not identified), compared with the time required for transmission processing when inspections are performed and a message is broadcast. As a result of the inspection showing the presence of

a duplicate IPv6 address, DAD no longer has to record, buffer, and report the duplicate IPv6 address.

ACKNOWLEDGEMENT

This research is made possible and supported by UMP-IIUM Sustainable Research Collaboration 2022 Research Grant.

REFERENCES

[1] W. Luo, S. Liu, YJia, Y., Chen, Z., & Jiang, S. (2022). Flexible IP: An Adaptable IP Address Structure and Its Efficient Addressing Scheme. *Computer Networks*, 203, 108700.

[2] N. Jain, Payal, A., & Jain, A. (2021). Performance Analysis of Routing Protocols on IPv4 and IPv6 Addressing Networks. *Journal of Web Engineering*, 1327-1366.

[3] A. Mathew. (2022). An Inadvertent Standard: IPv4 Address Prefix Lengths in Interdomain Routing. In Workshop on Internet Standard Setting Research Methods.

[4] T. Rooney. (2011). *IP Address Management: Principles and Practice*. John Wiley & Sons.

[5] L. He, Kuang, P., Liu, Y., Ren, G., & Yang, J. (2021). Towards securing Duplicate Address Detection using P4. *Computer Networks*, 198, 108323.

[6] G. Kumar, & Tomar, P. (2021). A Stateless Spatial IPv6 Address Configuration Scheme for Internet of Things. *IETE Journal of Research*, 1-14.

[7] A. K. Al-Ani, Anbar, M., Al-Ani, A., & Ibrahim, D. R. (2020). Match-prevention Technique against Denial-of-service Attack on Address Resolution and Duplicate Address Detection Processes in IPv6 Link-local Network. *IEEE Access*, 8, 27122-27138.

[8] J. R. Machana, & Narsimha, G. (2022). Optimization of IPv6 Neighbor Discovery Protocol. *Journal of Interconnection Networks*, 2141025.

[9] F. Najjar, Kadhum, M., & El-Taj, H. (2015). Neighbor Discovery Protocol Anomaly Detection using Finite State Machine and Strict Anomaly Detection. *Proceedings of the 4th International Conference on Internet Applications, Protocols and Services* (NETAPPS2015), 967-978.

[10] E. Rye, Beverly, R., & Claffy, K. C. (2021). Follow the Scent: Defeating IPv6 Prefix Rotation Privacy. *Proceedings of the 21st ACM Internet Measurement Conference*, 739-752.

[11] M. Usman, Kamboh, U. R., Taqdees, M. D., Waheed, Z., Shehzad, M. N., & Zafar, H. (2021). Enhance Neighbor Discovery Protocol Security by Using Secure Hash Algorithm. *2021 International Conference on Innovative Computing (ICIC), IEEE,* 1-8.

[12] A. El Ksimi, & Leghris, C. (2018). Towards a New Algorithm to Optimize IPv6 Neighbor Discovery Security for Small Objects Networks. *Security and Communication Networks*, 2018.

[13] R. Roychaudhary, & Shahapurkar, R. (2021). A Proposed Method to Improve Efficiency in IPv6 Network Using Machine Learning Algorithms: An Overview. Information and Communication Technology for Competitive Strategies (ICTCS 2020), 165-173.

[14] Y. Alharbi, Alferaidi, A., Yadav, K., Dhiman, G., & Kautish, S. (2021). Denial-of-Service Attack Detection over IPv6 Network Based on KNN Algorithm. *Wireless Communications and Mobile Computing*, 2021.

[15] S. Praptodiyono, Hasbullah, I. H., Kadhum, M. M., Wey, C. Y., Murugesan, R. K., & Osman, A. (2016). Securing Duplicate Address Detection on IPv6 using Distributed Trust Mechanism. *Int J Simulation—Systems, Sci Technol*, 17(26).

[16] A. K. Al-Ani AK, Anbar, M., Manickam, S., Al-Ani, A. (2019) DAD-match; Security Technique to Prevent Denial of Service Attack on Duplicate Address Detection Process in IPv6 Link-local Network. *PLoS ONE*, 14(4), e0214518.

[17] M. M. Sajjad, Jayalath, D., & Bernardos, C. J. (2018). A Comprehensive Review of Enhancements and Prospects of Fast Handovers for Mobile IPv6 Protocol. *IEEE Access*, 7, 4948-4978.

[18] A. K. Al-Ani, M. Anbar, M., Manickam, S., Wey, C. Y., Leau, Y. B., & Al-Ani, A. (2019). Detection and Defense Mechanisms on Duplicate Address Detection Process in IPv6 Link-local Network: A Survey on Limitations and Requirements. *Arabian Journal for Science and Engineering*, 44(4), 3745-3763.

[19] N. Moore, (2006). Optimistic Duplicate Address Detection (DAD) for IPv6. RFC 4429, IETF.

[20] D. B. Farouq, A. A. Alarood, N. Aljojo, and A. Abubakar, 2020. Unidirectional and Bidirectional Optimistic Modes IP Header Compression for Real-time Video Streaming. *IEEE Access*, 8, 83155-83166.