DAD-Match: Technique to Prevent DoS Attack on Duplicate Address Detection Process in IPv6 Link-local Network

Ahmed K. Al-Ani, Mohammed Anbar, Selvakumar Manickam, and Ayman Al-Ani
National Advanced IPv6 Centre, USM, 11800 Gelugor, Penang, Malaysia
Email: ahmedkhallel91@nav6.usm.my

Abstract —Duplicate Address Detection (DAD) is one of the core procedures in Internet Protocol version 6 (IPv6). It allows all the nodes locate on the same link to communicate and join the network with a unique IP address. However, DAD is vulnerable to security threats. The DAD procedure is based on two Neighbour Discovery (ND) messages, namely, Neighbour Solicitation (NS) and Neighbour Advertisement (NA), to verify that the tentative IP is multicast to all existing hosts through an NS message. Thus, DAD allows any malicious node on the same link to receive the NS message, and the malicious node may send a spoof reply to prevent the address configuration of a target node, thereby resulting in a Denial of Service (DoS) attack. This study aims to secure the DAD procedure by hiding the tentative IP address during the process, thereby preventing a malicious node from disturbing the target node IP configuration process. The proposed security DAD-match technique builds on SHA-3 hash function by proposing a new option called DAD*match*, which holds the hash value of tentative IP address and attaches to NS and NA messages to become NS-match and NA-match messages. We expect the DAD-match technique can provide less complex lightweight security and will fully prevent DoS attacks during the DAD procedure in IPv6 link-local network.

Index Terms—Duplicate Address Detection, DAD, DoS attack, IPv6 Security, hash function, DAD-match technique

I. Introduction

The Internet Protocol version 6 (IPv6) was designed and engineered to overcome IPv6 address space exhaustion limitations [1]. Google statistics on October 2017 [2] showed the percentage of users reaching Google service over IPv6 surpassed 17% compared with IPv4, and this percentage continues to rise. IPv6 came with a simple header format and new concept mechanisms such as Neighbour Discovery Protocol (NDP) to make network communication more efficient and faster, and to extend its reach to a larger area. NDP [3] introduced several functions including parameter discovery, address resolution, address auto-configuration, and DAD procedure using five messages from ICMPv6 messages [4]. Although IPv6 was designed and developed with compulsory IP Security (IPSec) [5], IPv6 implementation still experiences security challenges.

Manuscript received December 20, 2017; revised May 12, 2018.
doi:10.12720/jcm.13.6.317-324

The NDP considers the essential protocol in IPv6, which does not have a sufficient security strategy to offer verification and authentication of packets exchange among hosts located on the same link. Studies [6], [7] indicated that the trend of insider attacks continues to rise. The growing number of insider attacks could disturb IPv6 correspondences, both internally and externally. This finding also proved that neighbours on local network communication cannot be trusted completely because all neighbours may possibly be an attacker. Various researchers [8]–[10] have published studies on the dangers and weakness of neighbour discovery. Attackers take advantage of vulnerabilities in neighbour discovery to perform DoS attacks, thereby degrading network performance and hijacking traffic.

The DAD procedure is one of the NDP functions that allow the node to configure a unique IP after confirming it with existing hosts on the same link. Any node on the same link can expose the DAD procedure to a DoS attack by responding to each NS message transmitted from the target host, because NDP does not have a security mechanism to secure their messages, namely, NS and NA messages. Eventually, the target host will fail to configure its network interface with IPv6 address, thereby preventing it from joining the IPv6 network. Request for Comment (RFC) 4861 recommended using IPSec [11] and SeND [12] to protect NDP functions including DAD. However, the implementation of the two suggested security mechanisms is not a solid mechanism. IPSec suffers from a bootstrapping problem when used for NDP as reported [13]. SeND mechanism relies on complex algorithm that requires heavy computation resulting in high consumption of both time and resources [14]. The complexity of SeND is also a subject of target for DoS attacks.

This study is an extension of the previous work which aims to propose a security technique based on Hash Function Cryptography to secure a tentative IP address during DAD procedure in IPv6 link-local network. The proposed technique is called the DAD-match technique. The rest of this paper is organized as follows: Section II provides a background of NDP and DAD with its security issues. Related works on securing DAD are explained in Section III. Section IV shows an overview of DAD-match proposal. Section V illustrates the expected results and future work. Section VI provides the conclusion.

II. Background

This section discusses NDP functions, SLAAC, and the importance of the DAD procedure and its main security issues in IPv6 link-local network.

A. Neighbor Discovery Protocol (NDP)

NDP controls the communication among neighbours (Routers and Hosts) using various messages and procedures [3]. NDP comes with new concepts, such as Stateless Address Auto-configuration (SLAAC) [15] for generating an IP address, DAD procedure for verifying the uniqueness of tentative IP address, Neighbour Unreachability Detection (UDP) for keeping reachability track of surrounding neighbours, and Redirect Message for advertising better next-hope [4]. These processes work by employing five ICMPv6 messages [16], as follows:

- Router Solicitation (RS) type 133, which is used from a host to ask a router for Router Advertisement (RA) message.
- Router Advertisement (RA) type 134, which is sent by a router periodically as a reply to RS message to inform its presence and link-specific parameters (link prefixes, link MTU and hope limits).
- Neighbour Solicitation (NS) type 135, which is used from host to ask another neighbouring host's MAC address and utilized for specific procedures such as DAD and NUD.
- Neighbour Advertisement (NA) type 136, which is sent Sent by Host as a reply to NS messages, or in case the host modifies its IP address.
- Redirect Message (RM) type 137, which is sent by a router to redirect traffic of a host from one path to another path.

NDP also plays an important protocol in IPv6 and in facing many attacks. Most common NDP attacks are Router Advertisement Spoofing Attack, NS and NA spoofing, Malicious Last-Hop Router Attack, Spoofed Redirect Message Attack, Replay Attacks, ND Flooding DoS Attack, and DoS on Duplicate Address Detection, which is the focus of this study.

B. Stateless Address Auto-Configuration (SLAAC)

IPv6 presents SLAAC, a new way to generate an IP address automatically for the host, and a new feature for IPv6 [17]. SLAAC works in a "Plug and Play" fashion. Moreover, IP addresses can be generated in different ways, such as the EUI-64 method offered by IEEE (Internet Engineering Task Force) [17]. EUI-64 is an address format accomplished on Ethernet interfaces by referencing the already unique 48-bit MAC address, and reformatting that value to match the EUI-64 specification. However, because this method generates the same IID whenever a node joins a network, intruders can easily track the node. In addition, the privacy extension method is a method for generating an IP address randomly [18]. By using this method, the address continues to change over time, causing the identification of the target host address difficult for intruders and other eavesdroppers [19].

The new proposed mechanism, DAD-match, uses the privacy extension method to generate an IP address during DAD process in IPv6 link-local network, as long as this method provides more security compared with the EUI-64 method.

C. Duplicate Address Detection (DAD) with its Security Problem

DAD is one of the NDP processes which ascertain that the existing host on the same link have unique IP address. Each host performs the DAD procedure before configuring its IP address [7], [20], using two NDP messages, namely, NS and NA. The target node multicasts NS messages carrying the tentative IP address to verify its uniqueness to solicited-node multicast group (SNMA) FF02::1:FF:00:0/104 (based on the last 24bit from the tentative IP). All existing nodes receive the NS message, and if a node is located on the same link and has the same IP address, it will replay via NA message as a response to NS message. Therefore, the target node must generate a new tentative address and wait for NA as a response. If a new host does not receive any response NA to its NS messages from the neighbouring nodes, then the newly generated address is unique and no other neighbouring host will use this IP address. Thus, a node can use this IP address as an interface identifier. Moreover, no response is given or if three seconds have passed and no NA message is received, then the target node considers the tentative IP address unique and that no other existing nodes on the same link uses the address. After three tries [7], the new host stops the DAD process, resulting in its network interface not being assigned to any IPv6 address.

Fig. 1. DoS attack on DAD procedure.

In IPv6 link-local network, existing nodes are considered reliable hosts. Therefore, any host can participate in the DAD process [21]. The DAD procedure uses two messages of NDP messages, which are insecure by design [14]. Thus, any node can disturb the DAD procedure and perform a DoS attack. Studies [4], [7], [21] have shown that the DAD process is exposed to Denial of Service (DoS) attacks. In a DoS attack on the DAD process, an attacker causes the target host to be unable to obtain an IP address by claiming the existence of a

tentative IP address by sending a fake NA message in reply to NS messages. Hence, the victim host will be unable to verify the uniqueness of the tentative IP address. Thus, the IPv6 host cannot obtain an IP address because of the DAD process failure [7], [21]. Figure 1 shows a DoS attack on DAD procedure.

III. Related Work

Many researchers have proposed different mechanisms built on various techniques to secure the DAD process in IPv6 link-local network. This section highlights the most common related works based on the hash function and their drawbacks.

A. Trust – Neighbor Discovery (Trust-ND)

Trust-ND secures NDP messages through extent NDP header by introducing a new security option called Trust-Option so that each message includes NS and NA messages to guarantee secure communication among hosts [7]. Trust-ND builds on SHA-1 hash algorithm to achieve required security with less complexity. According to the study [7], Trust-ND is faster compared with other mechanisms during address verification and performs better because of its design. However, research [22], [23] shows that SHA-1 algorithm is vulnerable to hash collision attacks. Thus, any malicious host has the ability to create hash collision attacks. Because Trust-ND is based on SHA-1, it is susceptible to collision attacks that induce DoS attacks on DAD procedure in IPv6 link local network [21]. Because of its design method, Trust-ND is not a suitable security means for IPv6 DAD procedure.

B. Pull Model

Pull Model secures IPv6 DAD procedure [24]. This mechanism is designed on the basis of the push vs pull concept [25]. The main goal of this study is to diminish processing overhead and enhance flexibility in address generation within DAD procedure by utilizing MD5 hash computation to authenticate the tentative IP address with existing neighbouring hosts on the same link. The disadvantage of this method is that if the hash function is too short, then it is vulnerable to brute force attack. However, if the hash value is found too long, then it facilitates possible inverting attacks. Studies [26], [27] show that Pull Model is vulnerable to DoS attacks during the DAD procedure in IPv6 link-local network. In view of these security vulnerabilities, Pull Model is not recommended for IPv6 DAD procedure.

C. Duplicate Address Detection with Hash Function (DAD-h)

In 2016, Song and Ji [28] proposed another security mechanism to resist DoS attacks during the DAD procedure in IPv6 network. MD5 hash algorithm (as defined in RFC1321 [29]) has been utilized to build up a mechanism named DAD-h. The DAD-h mechanism aims to hide the tentative IP address during the DAD procedure to prevent any attacker from identifying the target address the new host will use. The study assumes that this method can prevent DoS attacks on the DAD procedure in Pv6 link-local network.

Nevertheless, research [30] shows that MD5 hash function has issues with IPv6 protocol during data transmission. Another previous study [31] also shows that problems in using MD5 in IPv6 include the higher latency cost compared to the value used and the processor occupied entirely by the computation of MD5 algorithm. Moreover, MD5 is vulnerable to hash collision attack as mentioned in [22], [23]. MD5 hash function not only has performance issues with IPv6 protocol, but is also vulnerable to security threats. Based on these studies, DAD-h mechanism, which is based on MD5 hash function, cannot be recommended for IPv6 DAD process.

Table I: Summary of Current DAD-based Attacks Defense Mechanisms

Proposed Mechanism	Limitations
Trust-ND	• Vulnerable to collision attacks due to its design. • Lacks of addressing legitimate resource attacks.
Pull Model	• Vulnerable to brute force attacks. • Susceptible to DoS attacks due to its mechanism.
DAD-h	• High computational cost. • Adds more processing overhead in verification process. • Vulnerable to hash collision attacks that can cause DoS-on-DAD attacks.

Table I summarizes the related works on securing DAD procedure in IPv6 link-local network. Most related works suffer from complexity because of their design. In addition, these studies added more processing for the verification process, as well as increase the network overhead bandwidth utilization. With these limitations, this study attempts to propose a new mechanism to provide better security for DAD procedure in IPv6 link-local network as explained in the next section.

IV. Proposed DAD-Match Technique

Because the current existing mechanisms have failed to secure DAD procedure in IPv6 link-local network due to their serious limitations issues, this research aims to propose a new security technique via redesigning the DAD procedure to overcome the existing mechanisms' limitations which were highlighted in the previous section. This study further aims to design sufficient security for IPv6 DAD procedure.

The main issue with the proposed mechanisms is the complexity to generate and verify the message. In addition, some mechanisms need external resources to process the message. As a result, these mechanisms consume CPU and the bandwidth of the node. Disclosing the tentative IP address to the public permits all the nodes on the same link, including malicious nodes, to disturb the DAD procedure. Malicious nodes prevent a victim node from configuring a unique IP by claiming that the

tentative IP has already been used, thereby preventing the node from joining the link. Thus, the DoS attack is launched. The proposed study assumes that by hiding the tentative IP address, the DoS attack can be effectively prevented. Hiding the tentative IP address exchange among hosts (target host and existing hosts) during DAD procedure can be done through encryption or cryptographic hash function.

Encryption introduces heavy calculation as reported in [32]. As a result, encryption is not an appropriate option for the proposed technique. Studies [7], [28] show that the use of a hash function is suitable to fulfil the requirement, as hash functions entail less computation in terms of processing time and are more lightweight compared with encryption cryptography. Moreover, a study [33] shows that hash function is faster in processing than encryption. Many hash functions have been proposed such as MD5, SHA-1 and SHA-2. However, these hash functions are vulnerable to hash collision attacks, as mentioned in [22], [23]. A study [34] presents that SHA-2 hash value is much larger than MD5, and, therefore, this longer string value takes up more space and can take slightly longer to calculate. One research [35] shows that SHA3 is stronger among all the hash function proposals. Furthermore, as mentioned in [34], SHA-3 is a new generation of SHA that shows promise, as it utilizes a fast sponge construction to generate hash values leading to speed advantages. It has an arbitrary output length which is different than traditional hashes in use today. It has notable security strength levels against attacks. In addition, it is flexible for implementation options for performance and security trade-offs.

Previous studies show that SHA-3 hash function can be the most suitable algorithm for the proposed technique and can provide fast processing for hashing. Furthermore, the SHA-3 hash function can offer availability, that is, functionality, as a filtering mechanism for receiving messages is required. The following sections explain the main stages and workflow for DAD-match technique supported by an extensive example.

A. Main Stages of DAD-match Technique

The DAD-match technique is proposed to secure the DAD procedure through hiding tentative IP addresses by redesigning NS and NA messages in IPv6 link-local network. This section describes the three main stages of the DAD-match technique, namely, Tentative IP Address Generation Stage, Secure NS and NA Messages Stage and DoS DAD Prevention Stage.

1) Tentative IP address generation stage

In this stage, the tentative IP address is generated using a privacy extension method, which provides better security than EUI-64. Because the method generates the IP address randomly, users are protected from being tracked, and malicious nodes will have difficulty identifying the IP address of a particular node. After an IP address is generated as a tentative IP, the address is hidden by hashing the first 40-bit of Identifier Interface. The output from this stage is the hash value of 40-bit of Interface Identifier.

2) Secure NS and NA messages stage

The DAD procedure relies on two NDP messages (NS and NA messages) as mentioned previously. Therefore, to secure the DAD procedure, NS and NA messages should be redesigned, because these messages are insecure in design and do not have the ability to differentiate between valid messages among invalid messages. The DAD-match technique introduces an option named DAD*match* option that holds the hash value of the first 40-bit and 64-bit of Interface Identifiers of tentative IP addresses for NS and NA verification purposes, respectively. The DAD*match* option should be attached to each NS and NA to become NS-match and NA-match messages, and its type field values are 135 and 136 respectively. The source address should be an unspecified address, while the destination is an SNMA address (based on the last 24-bit tentative IP address). Each message without the DAD*match* option are discarded. The verification of the message to distinguish whether the message comes from a legitimate or illegitimate node is based on matching the hashing of the incoming hashing IP address with its self-hashing IP address. Fig. 2 shows the NS-match/NA-match messages format.

Part	Description	Value
Ethernet Header	Destination MAC	33:33:FF:SS:SS:SS
	Source MAC	Sender/Receiver MAC
	Type	0x0806
IPv6 Header	Source IP	:: (unspecified address)
	Destination IP	FF02:1:FF00:0/104
	Next header	0x3a
ICMPv6	Type	135 for NS-match 136 for NA-match
	DAD*match*	40_IPhash for NS-match 64_IPhash for NA-match

Fig. 2. NS-match/NA-match message format.

3) DoS DAD Prevention Stage

After the target host attaches a DAD*match* to the NS message to become an NS-match message that holds the hash value, as shown in Fig. 3, the target host sends to the SNMA address (FF02::1:FF00:0/104). All existing hosts on the same link receives the NS-match message, and the existing host should match the hash value. After computation, the hash value matches, performs the DAD procedure and can reply via NA-match message after hash the 64-bit of Interface ID and insert it to the DAD*match* option which should also be appended into NA-match message. Similarly, upon receiving the NA-match message, the new host matches the 64-bit hash value. If matches are found, then a duplicate address has occurred, and the new host repeats the DAD procedure. Otherwise, the new host considers the NA-match message illegitimate, discards the message and configures a unique IPv6 link-local address. Furthermore, if the target host does not receive any NA-match message as a

response to the NS-match message, or if no existing host responds after three seconds, then the tentative IP considers the IP unique, and the target host will configure its IP. Using the DAD-match technique secures a tentative IP address during the entire DAD procedure, thereby preventing malicious nodes from disturbing the process. Therefore, DoS on DAD can be prevented fully, and the target host can configure its IP address and join the IPv6 link-local network.

Type	Code	Checksum
Reserved		
Target Address		
Options		
DAD*match*		

Fig. 3. Message format of DAD-match technique

B. Workflow of DAD-match Technique

The DAD-match technique proposes a secure option named DADmatch, which will be attached to the NS and NA messages to transform them into NS-match and NA-match messages. The validation is performed on the both sides (Receiver and Sender) to provide more security by distinguishing between the legitimate and illegitimate messages. The workflow of the proposed technique is summarized in the following steps:

- When a new node joins the IPv6 link-local network, or an existing node on the same link plans to generate a new address for its own use, the new IP address must be generated through a privacy extension method as a tentative IP address.
- The target host hashes the first 40-bits and the 64-bits of the Interface ID of the tentative IP address. The hash value of the 40-bits is inserted into 40_IPhash field, which is in the DAD*match* option, while the hash value of the 64-bits is saved into the registry cache for NA message verification later on.
- The DAD*match* option is attached to the NS message to become an NS-match message which is then sent to the SNMA address based on the last 24-bit of the tentative IP address (FF02::1:FF00:0/104).
- All existing hosts on the same IPv6 link that have the same SNMA address receive the NS-match message.
- The existing hosts perform a message validation check to make sure the NS-match message comes from a legitimate host based on the existing DAD*match* options. In case the DAD*match* option is not found, the receiver (existing hosts) should discard the message.
- Otherwise, the receiver matches its 40_IPhash with 40_IPhash in the NS-match message to ensure message validation. In case the 40_IPhash matches the IP address, the DAD procedure will procced. Otherwise, the receiver discards the NS-match message.
- Upon successful matching of 40_IPhash, meaning that a duplicate IP address occurred and the receiver should insert the hash value of 64-bit of IP address into 64_IPhash field in DAD*match* option, then it is appended to the NA-match message and sent to the SNMA address.
- The target host receives the NA-match message, and first checks the existing DAD*match* option. If the DAD*match* option is found, it will proceed forward. Otherwise, the message is discarded, and the tentative IP is considered a unique IP address.
- If the DAD*match* option exists, then the target host matches the hash value of 64-bit at the cache registry with the 64_IPhash in NA-match message. Matches found mean that the message comes from a legitimate node and a duplicate IP address has occurred. The target host thus regenerates a new IP address and repeats the DAD process to re-update the neighbour cache table for further communication.
- Otherwise, the NA-match message is discarded and IP address is used as a unique IP.

In this way, a successful DAD process can be accomplished in IPv6 link-local network because the target host can verify the uniqueness of the tentative IP address with existing hosts. Thus, the new host can communicate with neighbouring hosts on the same link-local network. Fig. 4 shows the workflow when a new host (Sender) and existing hosts (Receiver) perform the DAD-match Mechanism process.

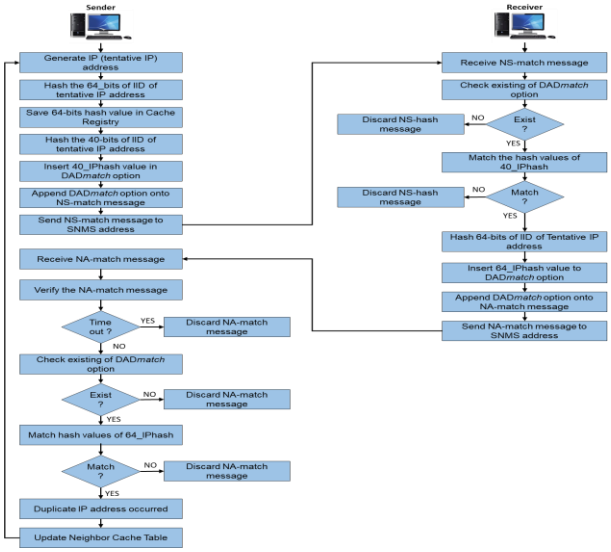


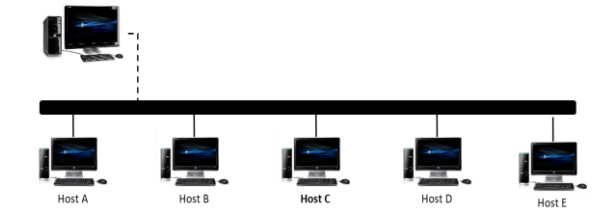
Fig. 4. Workflow of DAD-match technique.

C. Explanation Example of DAD-match

This section presents an example to demonstrate the DAD-match technique procedure in IPv6 link-local network. The assumptions based on five existing hosts, namely A, B, C, D and E, on the IPv6 link-local network and their address configuration information are illustrated in Fig. 5.

Fig. 6 shows that three hosts (A, C and D) joined the same SNMA address, which is FF02::1:FF82:2640. Host A is assumed to generate a new address using a privacy extension method. With FE08::C262:6BFF:FE82:2640 as a tentative IP, host A must check the uniqueness of this

IP to ensure that no existing host is already using it. Before sending any NS messages, host A hashes the first 40-bit and 64-bit of Interface ID of tentative IP address. The hash result of 40-bit is inserted into the DAD*match* option, while the hash result of 64-bit is saved in the cache registry for NA verification later on. The DAD*match* option is appended to an NS message to become an NS-match message and sent through the SNMA address, FF02::1:FF82:2640.



Host Name	IP address	MAC address	40_IPHash	64_IPHash
Host A (New Host)	FE08::C262:6888:FE82:2640	C0:62:6B:82:26:40	5738e5e50c3f73e0cd5c7b38aa	64fbd937be5f272fe69394458ca6
Host B (Exist Host)	FE08::112A:FFA2:FC33:9210	11:2A:A2:33:92:0C	39975jhdsd92sijdoasd5c7b32i4	jkhsd897298hdw62hfj93773hd01
Host C (Exist Host)	FE08::C262:6888:FE82:2640	84:CA:C4:10:33:FE	5738e5e50c3f73e0cd5c7b38aa	64fbd937be5f272fe69394458ca6
Host D (Exist Host)	FE08::C262:6BFF:FE82:2640	12:34:6C:80:00:10	5738e5e50c3f73e0cd5c7b38aa	3aljkd90389wdjsa093hfhaso0923
Host E (Exist Host)	FE08::3909:FFA4:9354:12C3	A4:56:80:20:3C:B1	Lisajd0374ijfow883hfkk302bdg	Lla883hhf4yfjjde02kdbb283dkfn2

Fig. 5. Existing/New host address configuration information

In this case, all existing hosts on the same link that have been joined in the same SNMA receive the NS-match message, which are hosts C and D. Receiving hosts C and D use their 40-bit hashes from the cache registry to match with the DAD*match* option hash. In this example, the host D result does not match because the IP address is different. Host C obtains the match. In this case, host D sends a message to host A that "Duplicate IP address occurred" using an NA message. Host C hashes the 64-bit of its Interface IP address and inserts the hash value into the DAD*match* option by an NA-match message to SNMA address. Host A receives the message and verifies that the 64-bit hash, which was saved earlier in the cache registry matches with the hash value in the DAD*match* option of the NA-match message. If a match is found, then the NA-match message comes from a legitimate host, which means an IP duplicate occurred and the tentative IP is not unique. In this case, host A regenerates a new IP and repeats the DAD process. If no match is found, then the NA-match message is discarded. In this example, the results match because both hosts have the same IP. Moreover, if host A does not receive any NA-match message within three seconds, the tentative IP is considered a unique IP.

Therefore, the DAD-match technique can successfully prevent a DoS attack during the DAD procedure in IPv6 link-local network by hiding the tentative IP address on both sides during the DAD procedure. Doing so allows the new host to configure its IP address securely without disturbances from malicious nodes.

V. Expected Results and Future Works

This study proposed a new security technique called DAD-match for securing the DAD procedure from DoS attacks in IPv6 link-local network. The proposed technique aims to overcome the limitations of the current existing mechanisms and improve the prevention of DoS-on-DAD attacks in terms of processing time and complexity. The DAD-match technique is based on SHA-3 hash function to secure a tentative IP address exchange among hosts during the DAD procedure. The target host verifies the uniqueness of the tentative IP address by matching the hash values, thereby preventing malicious hosts from disturbing the verification process. As a result, new hosts can join the IPv6 network effectively in terms of time, complexity and computation. The next step is to implement the proposed technique and evaluate the results with existing related works.

VI. Conclusion

DoS attack on DAD procedure considers a genuine danger in IPv6 link-local network since there are an expanding number of nodes and the broad utilization of IPv6 addresses. In standard DAD, the target host reveals the tentative IP within DAD procedure, which permits all nodes locate on the same link to know the new address used by the target host, therefore, malicious nodes will be able to do forge replies to launch DoS attacks. The proposed DAD-match technique aims to hide the tentative IP during DAD process through uses SHA-3 hash function to provide a sufficient verification and prevent the malicious node for faking reply in order to secure IPv6 link-local network from any DoS attacks.

Acknowledgment

The author would like to thank his main supervisor, Dr. Mohammed Anbar and his co-supervisor, Dr. Selvakumar Manickam for their extraordinary support during his Ph.D. journey.

References

[1] S. E. Deering, Internet Protocol, Version 6 (IPv6) Specification, 1998.

[2] IPv6 – Google. (2017). [Online]. Available: https://www.google.com/intl/en/ipv6/statistics.html.

[3] T. Narten, W. A. Simpson, E. Nordmark, and H. Soliman, "Neighbor discovery for IP version 6 (IPv6)," 2007.

[4] O. E. Elejla, M. Anbar, and B. Belaton, "ICMPv6-Based DoS and DDoS attacks and defense mechanisms: Review," *IETE Tech. Rev.*, vol. 4602, no. 8, pp. 1–18, 2016.

[5] B. Stockebrand, "Ip security (ipsec)," IPv6 Pract. A Unixer's Guid. to Next Gener. Internet, 2007, pp. 311–317.

[6] C. I. T. Center, "Unintentional insider threats: Social engineering," 2014.

[7] S. Praptodiyono, I. H. Hasbullah, M. M. Kadhum, C. Y. Wey, R. K. Murugesan, and A. Osman, "Securing duplicate address detection on IPv6 using distributed trust mechanism.," *Int. J. Simulation--Systems, Sci. Technol.*, vol. 17, no. 26, 2016.

[8] J. Arkko, T. Aura, J. Kempf, V. M. Mäntylä, P. Nikander, and M. Roe, "Securing IPv6 neighbor and router discovery," in *Proc. 1st ACM Workshop on Wireless Security*, 2002, pp. 77–86.
[9] P. Nikander, J. Kempf, and E. Nordmark, "IPv6 neighbor discovery (ND) trust models and threats," 2004.
[10] Supriyanto, I. H. Hasbullah, R. K. Murugesan, and S. Ramadass, "Survey of internet protocol version 6 link local communication security vulnerability and mitigation methods," *IETE Tech. Rev.*, vol. 30, no. 1, pp. 64–71, 2013.
[11] W. Stallings, *IP Security, The Internet Protocol Journal*, Volume 3, Number 1, 2002.
[12] J. Arkko, J. Kempf, B. Zill, and P. Nikander, "Secure neighbor discovery (SEND)," 2005.
[13] J. Arkko and P. Nikander, "Limitations of IPsec policy mechanisms," in *Proc. International Workshop on Security Protocols*, 2003, pp. 241–251.
[14] A. AlSa'deh and C. Meinel, "Secure neighbor discovery: Review, challenges, perspectives, and recommendations," *IEEE Secur. Priv.*, vol. 10, no. 4, pp. 26–34, 2012.
[15] T. Narten, R. Draves, and S. Krishnan, "Privacy extensions for stateless address autoconfiguration in IPv6," 2007.
[16] O. E. Elejla, B. Belaton, M. Anbar, and A. Alnajjar, "Intrusion detection systems of ICMPv6-based DDoS attacks," *Neural Comput. Appl.*, pp. 1–12, 2016.
[17] T. Narten, S. Thomson, and T. Jinmei, "IPv6 stateless address autoconfiguration," 2007.
[18] T. Narten and R. Draves, "Privacy extensions for stateless address autoconfiguration in IPv6," pp. 1–23, 2007.
[19] P. Tayal, "IPV6 SLAAC related security issues and removal of those security issues," *Inernational J. Eng. Comput. Sci.*, vol. 3, no. 9, p. 4, 2014.
[20] N. Moore, "Optimistic Duplicate Address Detection (DAD) for IPv6," 2006.
[21] S. U. Rehman and S. Manickam, "Improved mechanism to prevent denial of service attack in IPv6 duplicate address detection process," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 2, pp. 63–70, 2017.
[22] E. Andreeva, B. Mennink, and B. Preneel, "Open problems in hash function security," *Des. Codes Cryptogr.*, vol. 77, no. 2–3, pp. 611–631, 2015.
[23] T. Polk, L. Chen, S. Turner, and P. Hoffman, "Security considerations for the sha-0 and sha-1 message-digest algorithms," 2011.
[24] G. Yao, J. Bi, S. Wang, Y. Zhang, and Y. Li, "A pull model IPv6 duplicate address detection," in *Proc. IEEE 35th Conference on Local Computer Networks*, 2010, pp. 372–375.
[25] Z. Duan, K. Gopalan, and Y. Dong, "Push vs. Pull: Implications of protocol design on controlling unwanted traffic.," SRUTI, vol. 5, pp. 25–30, 2005.
[26] L. R. Knudsen and M. J. B. Robshaw, "Brute force attacks," in *The Block Cipher Companion*, Springer, 2011, pp. 95–108.
[27] K. Apostol, "Brute-force attack," 2012.
[28] G. Song and Z. Ji, "Novel duplicate address detection with hash function," PLoS One, vol. 11, no. 3, p. e0151612, 2016.
[29] R. Rivest, "The MD5 message-digest algorithm," 1992.
[30] L. D. Barchett, A. Banerji, J. M. Tracey, and D. L. Cohn, "Problems using MD5 with IPv6," *Perform. Eval.*, vol. 27, pp. 507–518, 1996.
[31] T. Xie, F. Liu, and D. Feng, "Fast collision attack on MD5.," *IACR Cryptol. ePrint Arch.*, vol. 2013, p. 170, 2013.
[32] J. Cordasco and S. Wetzel, "Cryptographic versus trust-based methods for MANET routing security," *Electron. Notes Theor. Comput. Sci.*, vol. 197, no. 2, pp. 131–140, 2008.
[33] J. S. Coron, Y. Dodis, C. Malinaud, and P. Puniya, "Merkle-Damgård revisited: How to construct a hash function," in Advances in Cryptology--CRYPTO 2005, 2005, pp. 430–448.
[34] K. Dunham, "A fuzzy future in malware research," ISSA J., 2013.
[35] V. Melnyk and A. Kit, "Basic operations of modern hashing algorithms," 2013.
[36] B. Fenner, "Experimental values In IPv4, IPv6, ICMPv4, ICMPv6, UDP, and TCP headers," 2006.

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

Mohammed Anbar obtained his Ph.D. in Advance Computer Network from University Sains Malaysia (USM). He is currently a senior lecturer at National Advance IPv6 Center (IPv6), Universiti Sains Malaysia. His current research interests include Malware Detection, Web Security, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Network Monitoring, Internet of Things (IoT), and IPv6 Security.

Selvakumar Manickam is a senior researcher and software developer and works in the area of Cybersecurity, Internet of Things, Industry 4.0 and Machine Learning. He has authored and co-authored more than 130 articles in journals, conference proceedings and book reviews and graduated 8 PhDs and many masters and undergraduate students. He has more than 20 years of software development

experience and have also carried out numerous corporate trainings with focus on software development and security. He also lectures in various Computer Science and IT courses which includes development of new courseware in tandem with current technology trend. He is involved in various committees both at local and international levels. Previously, he was with Intel Corporation, Motorola and few start-ups working in related area before moving to academia. While building his profile academically, he is still very much involved in industrial projects involving machine learning and data analytics using open source platforms building predominantly using C and Python programming languages. He also has experience building Android mobile applications and web-based applications.

Ayman Al-Ani received his B.S degree in from Computer Enginnering in University of Technology and MSc in Information Technology from Universiti Utara Malaysia (UUM) in 2016. Currently, he is a Ph.D. fellow in school of National Advance IPv6 Center (NAv6), Universiti Sains Malaysia (USM). His research interests include Computer Network, Network Security, and Software Defined Network