Indonesian Journal of Electrical Engineering and Computer Science
Vol. 29, No. 1, January 2023, pp. 518∼526
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v29.i1.pp518-526

Proposed security mechanism for preventing fake router advertisement attack in IPv6 link-local network

Mahmood A. Al-Shareeda[1], Selvakumar Manickam[1], Murtaja Ali Saare[2], Navaneethan C. Arjuman[1]
[1]National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, Penang, Malaysia
[2]Department of Computer Technology Engineering, Shatt Al-Arab University College, Basrah, Iraq

Article Info

Article history:

Received Jul 18, 2022
Revised Sep 12, 2022
Accepted Oct 5, 2022

Keywords:

Fake router advertisement attack
Internet of things IPv6
Neighbor discovery protocol
Pv6 link-local network
Security mechanism

ABSTRACT

The design of router discovery (RD) is a trust mechanism to confirm the legitimacy of the host and router. Fake router advertisement (RA) attacks have been made possible by this RD protocol design defect. Studies show that the standard RD protocol is vulnerable to a fake RA attack where the host will be denied a valid gateway. To cope with this problem, several prevention techniques have been proposed in the past to secure the RD process. Nevertheless, these methods have a significant temporal complexity as well as other flaws, including the bootstrapping issue and hash collision attacks. Thus, the SecMac-secure router discovery (SecMac-SRD) technique, which requires reduced processing time and may thwart fake RA assaults, is proposed in this study as an improved secure RD mechanism. SecMac-SRD is built based on a UMAC hashing algorithm with ElGamal public key distribution cryptosystem that hides the RD message exchange in the IPv6 link-local network. Based on the obtained expected results display that the SecMac-SRD mechanism achieved less processing time compared to the existing secure RD mechanism and can resist fake RA attacks. The outcome of the expected results clearly proves that the SecMac-SRD mechanism effectively copes with the fake RA attacks during the RD process.

Corresponding Author:

Selvakumar Manickam
National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia
11800 USM, Penang, Malaysia
Email: selva@usm.my

1. INTRODUCTION

Today's global economy largely depends on the Internet [1], [2]. The global internet of things (IoT) market was USD 151 billion in the year 2018 and is expected to grow to USD 1,567 billion by 2025. There are already more than 17 billion linked devices in use worldwide, with 7 billion of those being the IoT devices (that number does not include smartphones, tablets, laptops, or fixed-line phones) [3], [4]. Sensors and wireless devices can now be connected to the internet thanks to the IoT [5], [6]. The number of devices linked to the Internet has increased steadily since the switch from the ARPANET to the modern internet [7]-[9]. Nevertheless, the internet's expansion is currently in jeopardy due to the exhaustion of available internet protocol version 4 (IPv4) addresses [10]-[12].

The internet engineering task force (IETF), which oversees the internet community, established IPv6 to solve the lack of IPv4 global addresses [13]. The RFC 2460 provides a detailed explanation of the IPv6 characteristics and functions [14]. Even though IPv6 offers more security features than IPv4, the protocol still has security problems as a result of design flaws, deployment concerns, and transitional problems [15]. The

RFC 4942 has a detailed explanation of these difficulties [16].

Due to the absence of a trust mechanism in the standard protocol, the host is unable to verify the legitimacy of the gateway router throughout the normal router discovery (RD) procedure. This flaw enables fake routers to be set up as valid gateways [17]. The attacker will spread a fake router advertisement (RA) message and give the host the ability to set up a fake set of router options. This ultimately denies the valid host service, and this attack would be classified as a fake RA attack [18], [19].

The rest of this paper is organized as follows. Section 2 reviews some of the related work. A critical review of related work, research problem, and need for improved secure RD mechanism are reviewed in section 3. Section 4 provides the design of the proposed SecMac-SRD mechanism in detail. Section 5 evaluates the expected result of the proposed SecMac-SRD mechanism. Finally, conclusion is described in section 6.

2. RELATED WORK

This section discusses some of the related work to trust-based solutions that will secure the RD process in the IPv6 link-local network. The following existing related works are provided. Rehman and Manickam [20] proposed an alternative duplicate address detection (DAD) method to address the denial of service (DoS) attack during the DAD process in the IPv6 network. The secure DAD method works based on hiding the tentative IP address during the DAD process to prevent any attack from determining the target address of the new host. The secure DAD mechanism has introduced two new neighbor discovery protocol (NDP) messages type known as secure neighbour solicitation (NS) and secure neighbour advertisement (NA). Secure DAD introduces a new secure tag field known as secure-tag option using message authentication code (MAC). Hashing technique for MAC done using universal MAC (UMAC).

Song and Ji [21] proposed an alternative DAD method to address the DoS attack during the DAD process in the IPv6 network. The DAD-h method works based on hiding the tentative IP address during the DAD process to prevent any attack from determining the target address of the new host. DAD-h has introduced two new NDP messages type known as NSDAD-h and NADAD-h. DAD-h introduces a new secure tag field known as Hash_64. Hash_64 has the value of the last 64 bits of the target address.

Al-Ani *et al.* [22] proposed an alternative DAD method to address the DoS attack during the DAD process in the IPv6 network. DAD-match have introduced two new NDP message types known as NS-match and NA-match. DAD-match introduces a new secure tag field known as IP hash. Hash has value of the last 96 bits of the target address and RandomIntegerNumber, which is a random integer number. This method is designed based on SHA-3 (shake 128) hashing algorithm.

Praptodiyono *et al.* [23] showed the trust-ND approach workflow because the trust-ND is regarded to be lightweight because it employs SHA-1 hash functions to satisfy the security needs. Key security characteristics in this method include the trust-ND method with trust value and trust option. Every host that receives NDP messages has their trust value assessed and compared before accepting their NDP communications. Each NDP message has the secure trust option tag applied to it to ensure secure communications in IPv6 networks. When receiving NDP messages such as router solicitation (RS), RA, NS, NA, and redirect (RR), each host must verify the trust model used by trust-ND.

Tall and Farssi [24] suggested using authentication header (AH) to authenticate the RA message to propose the cryptographically generated addresses (CGA) plus IPSEC AH NDP technique. The IPSEC family of products includes AH [25]. Utilizing AH, the protection of NDP messages can be built to guarantee their amicability and integrity. The primary aspect of preserving the statelessness of the NDP messages is the ability to validate the validity of the NDP messages received from the host based on AH SAs.

3. CRITICAL REVIEW

This section first provides a critical review of related work in detail. Then, we provide research problems in this paper. Finally, the need for an improved secure RD mechanism is provided. These parts will explain as follows.

3.1. Critical review of related work

For the purpose of securing the RD, this part presents a tabular summary of the relevant works. Table 1 includes a list of all relevant works that have been done to protect RD in IPv6 network connections. This gives a clearer picture of the linked works' shortcomings in terms of protecting the RD process.

Table 1. The secure RD mechanism in summary

Authors	Proposed mechanisms	Limitations
Rehman and Manickam [20]	Secure DAD	i) suffers from DoS attack; ii) suffers from Replay attack, and iii) only implemented for neighbor discovery, not for RD.
Song and Ji [21]	DAD-h	i) vulnerable to hash collision attack because using MD5, ii) suffers from Dos attack, and iii) only implemented for neighbor discovery, not for RD.
Al-Ani *et al.* [22]	DAD-match	i) suffers from pre-image attack; ii) has lower hash power, and iii) only implemented for neighbor discovery not for RD.
Praptodiyono *et al.* [23]	Trust-ND	i) the hash collision attack can be used against the SHA-1 hashing algorithm, ii) unreliable generation of trust value, iii) vulnerable to DoS attack, and iv) complex processing overhead.
Tall and Farssi [24]	CGA+ IPSEC AH NDP	i) the IPSEC AH is well known for bootstrapping problems, ii) a new host needs a functional IP address to perform the IPSEC AH, iii) not suitable for the new host joining the network, and iv) vulnerable to DoS attack.

3.2. Research problem

In order to acquire the gateway router prefix for the host under the IPv6 address configuration process, RD is a crucial action required in the address auto-configuration mechanism, i.e., the SLAAC mechanism [18]. Nevertheless, research has demonstrated that because there is no mechanism in place to confirm the legitimacy of the gateway router, the typical RD operation is susceptible to Fake RA assaults [26]. In order to address this, several prevention techniques such as secure DAD, DAD-h, DAD-match, trust-ND, and CGA + IPSEC AH NDP mechanisms have been proposed in the past.

Because of its decreased computing cost, the Trust-ND mechanism put out by Praptodiyono *et al.* [23] is said to be a lightweight mechanism. The SHA-1 hashing technique, which was used to create this system, is extremely susceptible to hash collision attacks [27], [28]. Tall and Farssi [24] have presented the CGA + IPSec AH NDP mechanism, which makes the claim that it is a lightweight mechanism due to its decreased computational cost. AH uses security associations (SAs), which were developed in accordance with internet key exchange version 2, which requires a working IP address. As a result, when a new host joins the network, it lacks a working IP address, which creates a problem known as the bootstrapping situation [29]. So the problems can be summarised as follows: i) because there is no trust mechanism to confirm the legitimacy of the gateway router, standard RD functioning is insecure by design and open to Fake RA attacks; and ii) even though the most recent secure RD mechanisms, such as Trust-ND and CGA + IPSEC AH NDP, can stop fake RA attacks, they still have high time complexity and built-in flaws like hash collision attacks and bootstrapping issues that can be exploited during the RD process in IPv6 network link-local communication.

3.3. Need for improved secure RD mechanism

This subsection reviews the drawbacks of the existing secure RD mechanism by explaining the data in detail. Then, we show an improved security mechanism requirement in this paper. These two parts are explained as follows.

3.3.1. Drawbacks of the existing secure RD mechanism

According to subsection 3.1, the existing mechanism for RD mechanism has some drawbacks. The implementation issues of the RD mechanism can be categorized into two categories as follows: i) high complexity: complexity is the difficulty rate on how to run the machines and the number of processes required to fulfill the operation of the mechanism. High complexity will lead to high computational costs and can be exploited by the malicious host; and ii) partial protection for IPv6 RD process: partial protection is defined as an action that is unable to provide full security for the secure RD mechanism. Attackers can disable this security mechanism by launching other types of DoS attacks. Therefore, these mechanisms unable to protect the IPv6 RD mechanism fully.

3.3.2. Requirements for better security mechanisms

The suggested security mechanism would include the following elements to secure the RD process and prevent fake RA Attacks in the IPv6 network, based on the study of the shortcomings of the current security mechanisms for a safe RD that was done above. Less processing time: in order to address the issue of high complexity, which contributes to high computational cost, the newly proposed mechanism should use a less complex mechanism to reduce the processing time. The less complex mechanism will provide less processing time. A less complex mechanism means a simple security mechanism with lower complexity. Intact security solution: the proposed techniques, such as Trust-ND and CGA+IPSEC NDP, are unable to defend against RD attacks because of other problems with its foundational flaws, such as hash collision attacks and bootstrapping issues.

4. DESIGN OF THE PROPOSED SECMAC-SRD MECHANISM

4.1. Design objectives

This subsection presents the design objectives of the proposed SecMac-SRD mechanism as follows: i) implementation of cryptographic hashing algorithm to generate a secure tag; ii) Redesign the RD message structure using the secure tag without compromising the original structure; and iii) During the RD procedure on the IPv6 link-local network, prevent the fake RA attack.

4.2. Architecture of SecMac-SRD mechanism

This section illustrates the design of the SecMac-SRD technique we suggest using to guard against fake RA attacks in IPv6 network connection local communication. The host controller (HC) and router controller (RC), which issued secure RS and RA messages, respectively, to protect the RD message process and thwart the Fake RA attack, are the two main components of the overall architecture, as shown in Figure 1. The operation of these components in order to achieve the secure RD process's security objective-preventing the fake RA attack-will be covered in depth in the following subsections.

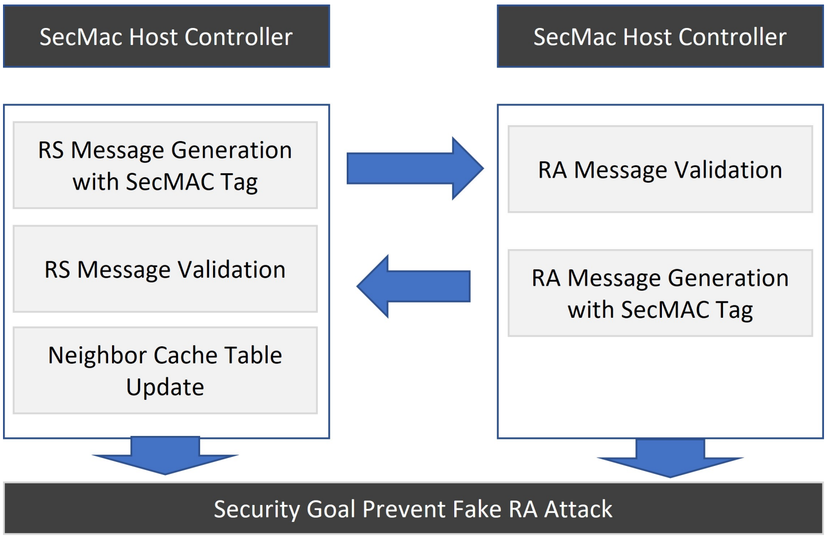
SecMac Host Controller
SecMac Host Controller
RS Message Generation with SecMAC Tag
RS Message Validation
Neighbor Cache Table Update
RA Message Validation
RA Message Generation with SecMAC Tag
Security Goal Prevent Fake RA Attack

Figure 1. Architecture of SecMac-SRD mechanism

4.2.1. Host controller

The HC of our SecMac-SRD mechanism is a heuristic-based module that is designed to conduct three key functions of heuristic-based operations within the host as follows: i) SecMac-tag RS message generation: is in charge of producing RS Messages with the new SecMac-tag secure tag option that will be transmitted to all of the routers on the link; ii) process for validating RA Messages: is to confirm that the RA messages received from valid routers; and iii) update of neighbour cache table: Is the database of existing nodes' IP addresses and corresponding MAC addresses that were given to the host and routers that already exist on the same link. The neighbour cache table is updated after validating the received routers.

4.2.2. Router controller

The RC of our SecMac-SRD mechanism is the heuristic-based controller that was designed to conduct two key functions within the router as follows: i) RS message validation process: is to confirm that the RS message came from a legitimate host; and ii) RA message generation process: is responsible for generating RA messages with a new secure tag option i.e., SecMac-tag that will be sent out to requesting host on the link.

4.3. Techniques used

4.3.1. Hashing functions algorithms

To secure the RD message exchange, our proposal doesn't use encryption or a digital certificate since it requires heavy calculation and 3rd party trust anchors to verify the certificate, respectively. Thus, our proposal will use the hash function since it is more appropriate to meet the security requirement for in link-local IPv6 communication. Hashing technique is less complex and uses less processing time based on [30]. There are some hash functions such as MD5, and SHA-1 is vulnerable to hash collision attacks. The UMAC hashing algorithm is not vulnerable to hash collision attacks. Therefore, our proposal will use UMAC function by adding additional fields such as Timestamp and Nonce have been added to strengthen SecMac-tag options.

4.3.2. Key distribution system

In the above hashing implementation, proposing technique required keys to complete the able process. Generally, there are two options of key distribution available to distribute keys in the network iproposaletric key distribution or asymmetric key distribution. There are several public keys system a valuable i.e, ElGamal, Rivest Shamir Adleman (RSA), elliptic curve cryptography (ECC). Based on [31], ElGamal is better compared to RSA and ECC in terms of security and performance. Therefore, the proposed will use the ElGamal public key cryptosystem [32] to fulfill this requirement.

4.3.3. Network prefix distribution

For the SLAAC IP addressing mechanism, proposals, when the in the IPv6 network would need to have a tentative IP address (128 bits) which includes first 64 bits, is as a network prefix and another last remaining 64bits would be the interface ID [33]. The host will obtain the network prefix using the RD process. The interface ID of the IP address would be generated by the ND process using extended unique identifier-64 (EU-64) or privacy extension. In this research work, the focus would be host to obtain the network prefix securely from the legitimate router. So our proposal will improve the secure RD mechanism i.e., the SecMac-SRD mechanism would be able to prevent the Fake RA attack using the following improved hashing technique.

4.3.4. SecMac-SRD secure tag generation

The secure message authentication code (SMAC) for the secure tag option generated using the source MAC address generated random nonce and private keys of the sending node. After the SMAC is generated based on the above process, this hash value will be inserted into the new secure tag known as the SecMac-tag option. The SecMac-tag option format adheres to the RFC 4861 option format [34]; type and length are required for all NDP options. The NDP option must be at least 8 bytes (64 bits) in length; otherwise, it must be padded. The 20-byte SecMac-tag is broken up into six fields.

4.3.5. Generation and validation

This subsection shows the host and router to verify SecMac-RS and SecMac-RA whether come from valid or illegal nodes. Under the standard RD processes, there is no mechanism to check whether the host or router is legitimate. The standard RD process is unable to verify whether the host or router is trustworthy. Hence, under the standard RD process, any malicious node can become the default gateway. One or more routers could act as malicious nodes that launch Fake RA attacks on the other hosts [35]. In order to differentiate a valid router, there is a real need to use a security mechanism during the RD process. The following section explains how the above generation and validation processes are done in the SecMac-SRD mechanism.

4.4. Process flow SecMac-SRD mechanism

This subsection describes the process flow of our proposed SecMac-SRD mechanism in terms of generation and validation. As shown in Figure 2, the process flow SecMac-SRD mechanism. The suggested SecMac-SRD mechanism in the aforementioned procedure guards against bogus RA messages in the IPv6 network. The attacker can prevent the host from receiving legitimate service if the host accepts the phony RA message and sets a malicious router as the default gateway. The regular RS and RA messages have been modified in the aforementioned SecMac-SRD method by having the SecMac-tag option added. To determine if a router is a genuine router or a malicious router, the SecMac-tag option offers integrity checks on the router. This method prevents the rogue router from being set as the default gateway if it is a rogue router.

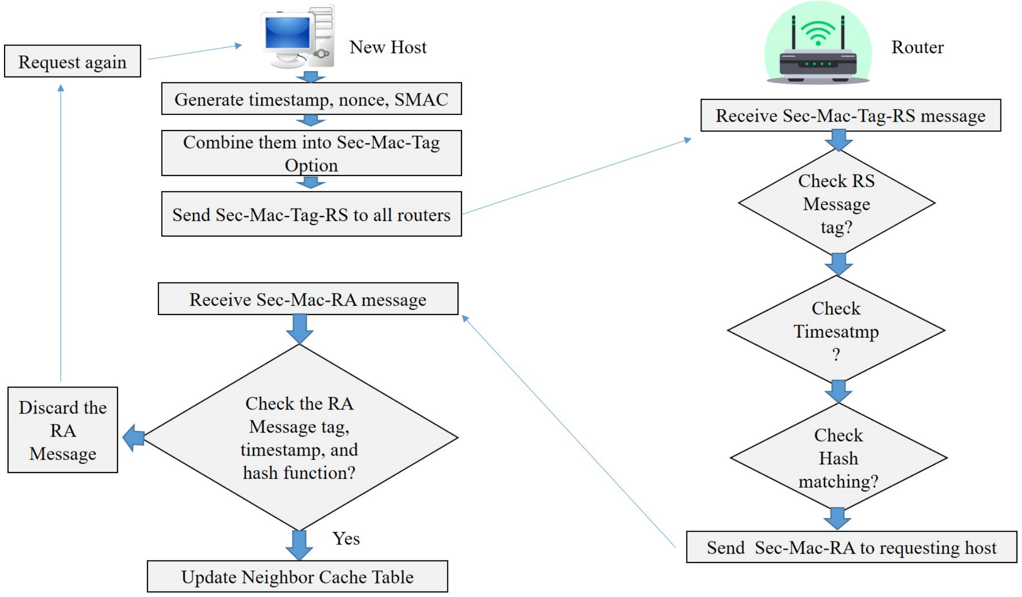
Request again
New Host
Generate timestamp, nonce, SMAC
Combine them into Sec-Mac-Tag Option
Send Sec-Mac-Tag-RS to all routers
Receive Sec-Mac-RA message
Discard the RA Message
Check the RA Message tag, timestamp, and hash function?
Yes
Update Neighbor Cache Table
Router
Receive Sec-Mac-Tag-RS message
Check RS Message tag?
Check Timesatmp ?
Check Hash matching?
Send Sec-Mac-RA to requesting host

Figure 2. Process flow SecMac-SRD mechanism

5. EXPECTED RESULTS

This section outlines the anticipated outcomes for the analysis and functionality of the SecMac-SRD mechanism. Firstly, we analyze the result of our proposal in terms of security analysis. Then, a network overhead analysis is provided in detail. We show processing time analysis in this paper. Finally, we evaluate the performance of this work. These parts will show as follows.

5.1. Analysis

This subsection analyses the security analysis of the proposed work. Then we provide the network overhead of the work. Finally, the processing time of the proposed SecMac-SRD mechanism is provided. These analyses are explained as follows.

5.1.1. Security analysis

This study's main objective is to safeguard the RD procedure by guarding against false RA attacks in the IPv6 link-local network. According to security experts [36]-[38], in order to safeguard the information and information system, the system must meet three important criteria, namely confidentiality, integrity, and availability (CIA): i) confidentiality is the measure that is implemented in the information security design to protect from unauthorized access to sensitive data. This criterion will be tested and verified under the Fake RA attack scenario using the closed IPv6 testbed; ii) integrity is the measure that is implemented in the information security design to prevent data or a portion of the data from being changed or deleted by an unauthorized user. This criterion is also will be tested and verified using the closed IPv6 testbed; and iii) availability is the measure that is implemented in the information security design to provide the ability to access the data as and when required by legitimate users. This criterion is also will be tested and verified using the closed IPv6 testbed.

The expected outcomes that demonstrate how the SecMac-SRD mechanism prevents Fake RA attacks will be shown in the steps that follow. This attack was conducted using the Fake_Router6 command from the the hacker choice's (THC) attacking toolkit on a Kali Linux computer: i) the THC attacking tool Fake_router6 inside the Kali Linux computer allows the attacker to transmit a RA packet that is presumed to originate from the current valid router gateway under the normal scenario without the SecMac-SRD mechanism; and ii) the purpose of this experiment is to demonstrate if the secure RD mechanism, which includes SecMac-SRD, Trust ND, and CGA+ IPSEC AH NDP, is capable of stopping a fake RA attack in the aforementioned IPv6 Testbed environment.

5.1.2. Network overhead analysis

The objective of the network overhead analysis is to measure the impact of network performance of introducing the SecMac-SRD mechanism on the network. Since multiple hosts exist on the same network and generate secure SecMac-RS and SecMac-RA, the additional network load needs to be ascertained to ensure the network is not overloaded. It would not be efficient to introduce a secure RD mechanism with higher network overhead. The following section discusses and explains the calculation of the network overhead of introducing the SecMac-SRD mechanism on the host and router: i) SecMac-RS generation: assumed there are ten hosts, i.e., Nn, in the network, and each host sends additional Ds bytes i.e., 20 bytes of the additional SecMac-tag byte size, and generates SecMac-RS within Ts seconds. i.e.1 seconds; and ii) SecMac-RA generation: for every SecMac-RS request, there will be a SecMac-RA reply from the router. Assume we have Nr active routers, i.e., two on the network replying to the SecMac-RS messages request on the network.

5.1.3. Processing time analysis

This section examines how long each RD technique takes to generate and verify RS and RA messages. As a result, it is necessary to assess if the SecMac-SRD mechanism is effective in terms of requiring less processing time. The findings from trials comparing the Standard RD, SecMac-SRD, Trust-ND, and CGA+IPSEC AH NDP mechanisms are covered in this section: i) generation of RS messages: this step will discuss RS message generation time for standard RD, SecMac-SRD, trust-ND, and CGA+IPSEC AH NDP mechanisms; ii) validation of RS messages in the router: for all incoming RS messages on the IPv6 network, the receiving router will carry out a message validation procedure. To ensure that the message is coming from a legitimate host, the RS message validation is carried out. SecMac-RS, Trust-RS, and CGA+IPSEC AH NDP-RS all go through this message validation process; iii) generation of RA messages in the router: the generation times of RA messages for the Standard RD, SecMac-SRD, Trust-ND, and CGA+IPSEC AH NDP methods are covered in this section. The message generation time, or TGRA, is calculated by deducting the RA message generating process's start time from its processing time end, RAet; and iv) host validation of RA: the host will also carry out RA message validation for all incoming messages, much like the router does. The host earlier sent out an RS message in the same IPv6 network to finish the RD procedure. The received RA message is a response to that message.

5.2. Performance

This section discusses in detail the overall comparative analysis of all the mechanisms carried out in the above experiments based on the processing time and security criteria: i) processing time performance: based on our expected results, overall, the SecMac-SRD mechanism performed better in terms of processing time compared to Trust-ND and CGA+IPSEC AH NDP mechanisms for both generation and validation of the RS and RA messages. Overall the Standard Deviation for SecMac-SRD is also lower for both generations, and validation of the RS and RA messages shows that the SecMac-SRD mechanism is a more stable and consistent mechanism; and ii) security performance: according to the findings we predicted, the SecMac-SRD mechanism was successful in stopping the Fake RA attack in the IPv6 network. The Fake RA attack was not stopped by the CGA+IPSEC AH NDP mechanism or the Trust-ND mechanism. In order for the IPv6 host to complete the RD process in the link-local communication of the IPv6 network, the 126 SecMac-SRD mechanism is the most practical RD security mechanism.

A method called secure router discovery (SecMac-SRD) guards against Fake RA attacks during the RD process in the IPv6 network's link-local communication. Secure SecMac-tag possibilities in redesigned secure RS and RA messages. For safe RD message exchange, the key exchange process was redesigned by utilizing a public key distribution mechanism.

6. CONCLUSION

The host can acquire RA messages from the router, such as the network prefix, MTU size, and other information, using the standard RD protocol. When the RA message is received from a reliable router, the normal RD process lacks a security feature, which leads to a fake RA attack. The suggested SecMac-detail unique is utilized in this paper to distinguish between RS and RA messages in the link-local IPv6 network by combining the ElGamal public key distribution with the UMAC hashing algorithm. In contrast to Trust-ND and CGA+IPSEC AH NDP techniques, the achieved predicted router shows that the SecMac-SRD mechanism has less processing time and mechanisms prevent the fake RA attack. The SecMac-SRD method effectively prevents fake RA attacks in the connection IPv6 network, according to comparative predicted outcome analysis. The redesigned RS and RA with SecMac-tag based on the common NDP as specified in RFC 4861 were used to build the SecMac-SRD method. The RFC 4727-specified NDP option types 253 and 254 are only used for testing purposes. Therefore, NDP option 253 with SecMac-tag has to recognize all the devices in the IPv6 network in order to implement this mechanism in the company. Currently, only a tiny portion of the IPv6 network has the SecMac-SRD deployed.

REFERENCES

[1] B. Rezabakhsh, D. Bornemann, U. Hansen, and U. Schrader, "Consumer power: a comparison of the old economy and the internet economy," *Journal of Consumer Policy*, vol. 29, no. 1, pp. 3-36, 2006, doi: 10.1007/s10603-005-3307-7.

[2] M. A. Al-Shareeda *et al.*, "CM-CPPA: chaotic map-based conditional privacy-preserving authentication scheme in 5G-enabled vehicular networks," *Sensors*, vol. 22, no. 13, 2022, doi: 10.3390/s22135026.

[3] M. A. Al-Shareeda, M. Anbar, I. H. Hasbullah, and S. Manickam, "Survey of authentication and privacy schemes in vehicular ad hoc networks," *IEEE Sensors Journal*, vol. 21, no. 2, pp. 2422-2433, 2021, doi: 10.1109/JSEN.2020.3021731.

[4] M. A. Al-Shareeda, M. Anbar, S. Manickam, and A. A. Yassin, "VPPCS: VANET-based privacy-preserving communication scheme," *IEEE Access*, vol. 8, pp. 150914-150928, 2020, doi: 10.1109/ACCESS.2020.3017018.

[5] F. Caro and R. Sadr, "The internet of things (IoT) in retail: Bridging supply and demand," *Business Horizons*, vol. 62, no. 1, pp. 47-54, 2019, doi: 10.1016/j.bushor.2018.08.002.

[6] M. A. Al-Shareeda, M. Anbar, M. A. Alazzawi, S. Manickam, and A. S. Al-Hiti, "LSWBVM: A lightweight security without using batch verification method scheme for a vehicle ad hoc network," *IEEE Access*, vol. 8, 2020, doi: 10.1109/ACCESS.2020.3024587.

[7] M. Hauben, "History of ARPANET," *Site de l'Instituto Superior de Engenharia do Porto*, vol. 17, pp. 1-20, 2007.

[8] B. M. Leiner *et al.*, "A brief history of the internet," *ACM SIGCOMM Computer Communication Review*, vol. 39, no. 5, pp. 22-31, doi: 10.1145/1629607.1629613, 2009.

[9] M. A. Al-shareeda, M. Anbar, S. Manickam, and I. H. Hasbullah, "Review of prevention schemes for man-in-the-middle (MITM) attack in vehicular ad hoc networks," *International Journal of Engineering and Management Research*, vol. 10, no. 3, pp. 153-158, 2020, doi: 10.31033/ijemr.10.3.23.

[10] P. Richter, M. Allman, R. Bush, and V. Paxson, "A primer on IPv4 scarcity," *ACM SIGCOMM Computer Communication Review*, vol. 45, no. 2, pp. 21-31, 2015, doi: 10.1145/2766330.2766335.

[11] P. Wu, Y. Cui, J. Wu, J. Liu, and C. Metz, "Transition from ipv4 to ipv6: A state-of-the-art survey," *IEEE Communications Surveys & Tutorials*, ol. 15, no. 3, pp. 1407-1424, 2013, doi: 10.1109/SURV.2012.110112.00200.

[12] M. A. Al-shareeda *et al.*, "NE-CPPA: a new and efficient conditional privacy-preserving authentication scheme for vehicular ad hoc networks (vanets)," *Applied Mathematics Information Sciences*, vol. 14, no. 6, pp. 1-10, 2020.

[13] S. Bradner, Ed., "IETF Rights in Contributions," RFC 3978, 2005, doi: 10.17487/rfc3978.

[14] S. Deering and R. Hinden, "Internet protocol, version 6 (IPv6) specification," RFC 2460, 1998, doi: 10.17487/rfc2460.

[15] A. R. Choudhary, "In-depth analysis of ipv6 security posture," *2009 5th International Conference on Collaborative Computing: Networking, Applications and Worksharing*, 2009, pp. 1-7, doi: 10.4108/ICST.COLLABORATECOM2009.8393.

[16] E. Davies, S. Krishnan, and P. Savola, "IPv6 transition/co-existence security considerations," RFC 4942, 2007, doi: 10.17487/rfc4942.

[17] D. J. Tian, K. R. Butler, J. I. Choi, P. McDaniel, and P. Krishnaswamy, "Securing arp/ndp from the ground up," *IEEE Transactions on Information Forensics and Security*, vvol. 12, no. 9, pp. 2131-2143, 2017, doi: 10.1109/TIFS.2017.2695983.

[18] J. Arkko, T. Aura, J. Kempf, V.-M. Mäntylä, P. Nikander, and M. Roe, "Securing IPv6 neighbor and router discovery," *Proceedings of the 1st ACM workshop on Wireless security*, 2002, pp. 77-86, doi: 10.1145/570681.570690.

[19] M. A. Al-Shareeda, M. Anbar, S. Manickam, and I. H. Hasbullah, "Password-guessing attack-aware authentication scheme based on chinese remainder theorem for 5G-enabled vehicular networks," *Applied Sciences*, vol. 12, no. 3, p. 1383, 2022, doi: 10.3390/app12031383.

[20] S. U. Rehman and S. Manickam, "Novel mechanism to prevent denial of service (DoS) attacks in IPv6 duplicate address detection process," *International Journal of Security and Its Applications*, vol. 10, no. 4, pp. 143-154, 2016, doi: 10.14257/ijsia.2016.10.4.15.

[21] G. Song and Z. Ji, "Novel duplicate address detection with hash function," *PloS one*, vol. 11, no. 3, p. e0151612, 2016, doi: 10.1371/journal.pone.0151612.

[22] A. K. Al-Ani, M. Anbar, S. Manickam, and A. Al-Ani, "DAD-match; security technique to prevent denial of service attack on duplicate address detection process in IPv6 link-local network," *PloS one*, vol. 14, no. 4, p. e0214518, 2019, doi: 10.1371/journal.pone.0214518.

[23] S. Praptodiyono, R. K. Murugesan, I. H. Hasbullah, C. Y. Wey, M. M. Kadhum, and A. Osman, "Security mechanism for IPv6 stateless address autoconfiguration," *2015 International Conference on Automation, Cognitive Science, Optics, Micro Electro-Mechanical System, and Information Technology (ICACOMIT)*, 2015, pp. 31-36, doi: 10.1109/ICACOMIT.2015.7440150.

[24] K. Tall and S. M. Farssi, "Proposition of a model for securing the neighbor discovery protocol (NDP) in IPv6 environment," *International Conference on Algebra, Codes and Cryptology*, 2019, pp. 204–215, doi: 10.1007/978-3-030-36237-9_12.

[25] S. Kent and R. Atkinson, "IP authentication header," RFC 2402, 1998, doi: 10.17487/rfc2402.

[26] J. Kempf and E. Nordmark, "IPv6 neighbor discovery (ND) trust models and threats," RFC 3756, 2004, doi: 10.17487/rfc3756.

[27] K. Bhargavan and G. Leurent, "Transcript collision attacks: Breaking authentication in TLS, IKE, and SSH," in *Network and Distributed System Security Symposium–NDSS 2016*, 2016, doi: 10.14722/ndss.2016.23418.

[28] E. Andreeva, B. Mennink, and B. Preneel, "Open problems in hash function security," *Designs, Codes and Cryptography*, vol. 77, no. 2, pp. 611-631, 2015, doi: 10.1007/s10623-015-0096-0.

[29] S. B. I. Shah, M. Anbar, A. Al-Ani, and A. K. Al-Ani, "Hybridizing entropy based mechanism with adaptive threshold algorithm to detect RA flooding attack in IPv6 networks," *Computational Science and Technology*, R. Alfred, Y. Lim, A. Ibrahim, and P. Anthony, Eds. Singapore: Springer, 2019, pp. 315–323, doi: 10.1007/978-981-13-2622-6_31.

[30] M. Hollick, C. Nita-Rotaru, P. Papadimitratos, A. Perrig, and S. Schmid, “Toward a taxonomy and attacker model for secure routing protocols,” *ACM SIGCOMM Computer Communication Review*, vol. 47, no. 1, pp. 43–48, 2017, doi: 10.1145/3041027.3041033.

[31] M. Joye, “Secure ElGamal-type cryptosystems without message encoding,” in *The New Codebreakers*, P. Ryan, D. Naccache, and J. Quisquater, Eds. Berlin: Springer, 2016, pp. 470–478, doi: 10.1007/978-3-662-49301-4_29.

[32] S. Irawadi *et al.*, “Nonsingular matrix as private key on ElGamal cryptosystem,” in *Journal of Physics: Conference Series*, vol. 1821, no. 1, p. 012018, 2021, doi: 10.1088/1742-6596/1821/1/012018.

[33] O. E. Elejla, B. Belaton, M. Anbar, B. Alabsi, and A. K. Al-Ani, “Comparison of classification algorithms on ICMPv6-based DDoS attacks detection,” in *Computational Science and Technology*, R. Alfred, Y. Lim, A. Ibrahim, and P. Anthony, Eds. Singapore: Springer, 2019, pp. 347-357, doi: 10.1007/978-981-13-2622-6_34.

[34] T. Narten, E. Nordmark, W. Simpson, and H. Soliman, “Neighbor discovery for IP version 6 (IPv6),” RFC 4861, 2007, doi: 10.17487/rfc4861.

[35] A. N. Healey, “The insider threat to nuclear safety and security,” *Security Journal*, vol. 29, no. 1, pp. 23-38, 2016, doi: 10.1057/sj.2015.42.

[36] H. Taherdoost, S. Chaeikar, M. Jafari, and N. Shojae Chaei Kar, “Definitions and criteria of CIA security triangle in electronic voting system,” *International Journal of Advanced Computer Science and Information Technology (IJACSIT)*, vol. 1, no. 1, pp. 14-24, 2013.

[37] S. Samonas and D. Coss, “The CIA strikes back: redefining confidentiality, integrity and availability in security,” *Journal of Information System Security*, vol. 10, no. 3, pp. 21-45, 2014.

[38] J. Andress, *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*, Syngress, 2014.

BIOGRAPHIES OF AUTHORS

Mahmood A. Al-Shareeda obtained his Ph.D. in Advanced Computer Network from University Sains Malaysia (USM). He is currently a researcher at National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia. His current research interests include network monitoring, internet of things (IoT), vehicular Ad hoc network (VANET) security and IPv6 security. He can be contacted at email: alshareeda022@gmail.com.

Selvakumar Manickam is currently working as an Associate Professor at National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia. His research interests include Cybersecurity, Internet of Things, Industry 4.0, and Machine Learning. He has authored and co-authored more than 160 articles in journals, conference proceedings, and book reviews and graduated 13 PhDs. He has 10 years of industrial experience prior to joining academia. He is a member of technical forums at national and international levels. He also has experience building IoT, embedded, server, mobile, and web-based applications. He can be contacted at email: selva@usm.my.

Murtaja Ali Saare Murtaja Ali Saare is an Assistant Professor at the Department of Computer Technology Engineering, Shatt Al-Arab University College, Iraq. He received his master’s degree in Information Technology at Universiti Utara Malaysia (UUM), in 2017. He completed his Ph. D at School of Computing, Sintok, UUM, Kedah, Malaysia, in 2021. His research interest includes aging and cognition, e-health, and human-centered computing. He has published his research work inreputablescopus indexed journal. He can be contacted at email: mmurtaja88@gmail.com and murtaja.a.sari@sa-uc.edu.iq.

Navaneethan C. Arjuman obtained his Ph.D. in Advanced Computer Network from University Sains Malaysia (USM). My current research interest are in the area Cyber Security, IPv6, IoT and 5G. He can be contacted at email: nava@nav6.usm.my.