SADetection: Security Mechanisms to Detect SLAAC Attack in IPv6 Link-Local Network

Mahmood A. Al-Shareeda[1], Selvakumar Manickam[1], Murtaja Ali Saare[2] and Nazrool Bin Omar[1]
[1]National Advanced IPv6 Centre, Universiti Sains Malaysia, 11800, Penang, Malaysia
[2]Department of Computer Technology Engineering, Shatt Al-Arab University College, Basrah, Iraq
E-mail: alshareeda022@usm.my, selva@usm.my, murtaja.a.sari@sa-uc.edu.iq, nazriomar@unimap.edu.my

Keywords: SLAAC attack, IPv6, Security mechanism, SADetection

Received: October 9, 2022

Neighbour Discovery Protocol (NDP) attacks are a serious security concern for IPv6. Attackers utilize the Stateless Address Auto-configuration (SLAAC) NDP attack type of targeting the SLAAC process. SLAAC attacks can compromise an IPv6 link-local network and expose private data. Attack detection mechanisms, including RA-Guard, Snort IPv6 Plugin, SLAAC detection method by Buenaventura et al., and SLAAC Security Method by Massamba et al. have been proposed by researchers to address this issue. However, the detection algorithms have a number of shortcomings, including a complete reliance on preconfigured router databases. Additionally, fragment packets and packets with Hop-by-Hop Options and Destination Options extension headers are not detectable by the detection techniques for hidden RA messages. In this study, a rule-based detection method called SADetection is proposed for use in IPv6 link-local networks to identify SLAAC attacks. Both an illegal Router Advertisement (RA) message and a concealed RA message in a packet with an extension header have been found by SADetection. SADetection has demonstrated a detection accuracy of 98% percent and the capacity to defend an IPv6 link-local network from SLAAC attacks.

Povzetek: Opisana je nova metoda SADetection za detekcijo SLAAC napadov v IPv6 omrežjih.

1 Introduction

End-to-end security, address depletion and overhead routing processing are among the issues with Internet Protocol version 4 (IPv4) that are intended to be fixed by Internet Protocol version 6 (IPv6) (1; 2). The Internet Engineering Task Force (IETF) created IPv6 in 1998 to take the place of IPv4 on the internet. Deering and Hinden (3; 4) define IPv6 and explain its standard and specification in RFC 8200 - Internet Protocol, Version 6 (IPv6) Specification (5).

All IPv6 nodes should adhere to the Neighbor Discovery Protocol (NDP) standard, which is outlined in RFC 4861. Address Resolution Protocol (ARP) in IPv4 is replaced by NDP's link-layer address resolution capability, according to Narten et al. (6).

IPv6's Stateless Address Auto-Configuration is a key feature (SLAAC). By employing Router Advertisement (RA) messages, IPv6 nodes can create and set their own IPv6 addresses Thomson et al. (7). Although IPv6 addresses can also be allocated statically or through DHCPv6 services, network managers prefer SLAAC due to its quick and easy configuration (8; 9; 10).

Many private and public organizations have already deployed SLAAC in their IPv6 network environment. Although SLAAC is protected by existing security measures, several aspects of its security still need to be enhanced. An attacker could pose as a router and promote unauthorized network prefix Nikander et al. (11; 12) in an unprotected network. Using an unauthorized network prefix to create and configure IP addresses is a risky practice for IPv6 hosts (13; 14).

The main continuation of this paper is listed as follows. (I) This research has proposed a rule-based mechanism to detect SLAAC attacks during IPv6 address creation in IPv6 link-local network, (II) This research has designed detection rulesets to detect RA messages concealed in fragment packets or in packet with extension option header, (III) This research has proposed IPv6 link-local network testbed setup for SLAAC attack simulation and detection as well as benchmark dataset with related features and fields for future use to enhance research in SLAAC attack.

The remainder of this paper is structured as follows. Section 2 reviews related work in details. Section 3 describes the background of this paper. Section 4 presents the proposed SADetection mechanisms. Section 5 and Section 6 provide security analysis and performance evaluation of this work, respectively. critical analysis of this paper. Finally, Section 7 concludes this manuscript.

2 Related work

Many strategies have been put out by previous researchers to protect IPv6 link-local networks from SLAAC attacks. Related efforts addressing protection against SLAAC as-

sault can be split into two categories: attack defense and attack detection. Table 1 shows the similarity of attack detection and defense mechanisms.

2.1 Attack detection mechanisms

To stop a SLAAC assault by Gont (15), a detection and prevention mechanism called RA Guard was installed in layer two network switches. Only RA messages received from a switch's permitted ports may be broadcast to other ports thanks to RA Guard. Unauthorized ports will not receive RA messages. NDPMon was proposed by Beck et al. (16) to identify attacks on SLAAC in IPv6 link-local networks. NDPMon tracks changes in network activity on each host according to their IP and MAC address to identify SLAAC attacks. Massamba and Cheikh (17) secure SLAAC in a domestic IPv6 link-local communication by managing the router's decision to relay or discard RA according to a trusted table. To protect against SLAAC attacks, Nelle and Scheffler (18) suggested an authentication system based on Software-Defined Networking (SDN). A modern technology called SDN is being implemented utilizing the OpenFlow communication protocol. Buenaventura et al. (19) suggested a SLAAC detection system that completely relies on a legal router database that has been specified to detect SLAAC attacks. Schutte's proposed Snort IPv6 Plugin is a signature-based detection system, as noted in (20). The Snort IPv6 plugin makes use of the intrusion detection system's plugin functionality. Snort is free software.

2.2 Attack defence mechanisms

We discuss different security defenses against SLAAC attacks in IPv6 link-local networks in this subsection (21).

By proposing additional choices, namely SecMac tag for the message of RA/RS that contain a nonce, timestamp, and a MAC, Arjuman et al. (22) suggested an efficient security router discovery mechanism. The mechanism also suggests a novel authentication server-based method of verifying valid Routers during Router Discovery. The host creates the SecMac tag and appends it to the RS message. To protect NDP, Praptodiyono et al. (23) suggested using Trust-ND. By integrating a lightweight hash function, Trust-ND improved and optimized the cryptographic address creation technique.

2.3 Critical review

In this subsection, we provide critical review of State Of The Art (SOAT) in details and why we need SADetection mechanism in this paper. The main goal of this research is to increase the security of SLAAC by proposing a detection mechanism that can identify SLAAC attacks based on packet characteristics and behaviours rather than solely on predefined databases. It should also be independent of specific hardware and software and able to recognise hidden RA messages in fragment packets and packets with extension headers. Because it can meet all of the requirements listed above and at the same time provides simplicity, scalability, and manageability of IPv6 network, this research suggests rule-based detection technique (24; 25; 26).

By comparing RA messages with predefined authentication data or by verifying a switch port's authorisation to send RA messages, existing detection systems can identify SLAAC attacks. Predetermined or preconfigured data and allowed switch ports are used. The issue is that because the detection system has already run, reconfiguring and retraining must be done when a new valid router appears. This issue is resolved by the suggested rule-based detection technique by dynamically changing authentication data in the present without reconfiguration or reinitialization (27; 21).

Because it only inspects ICMPv6 type 134 packets, the current detection mechanism is also unable to identify hidden RA messages in fragmentation packets and packets with extension headers. The proposed rule-based detection system is improved to scan the first fragmented packet, which has an extension header for Hop-by-Hop Options and Destination Options and an Offset field value of zero (zero). When a concealed RA message is found, the detection method will be improved to intelligently go through any fragment and extension headers that are included in the packet and inform the administrator.

3 Background

3.1 Threat model

SLAAC attacks on IPv6 networks are risky and dangerous, as explained by the threat model. It also explains to the victims the effects of the SLAAC attack. The threat model includes the following:

- In various situations, an attacker may be present in an IPv6 network. A malicious individual who links to any public wireless system or a disgruntled worker in a company who already has access to the internal network can both be an adversary.
- Once within the network, the attacker will listen for RS and RA messages to gather the essential data.
- Attacker will pretend to be a router and transmit a false RA message with a forge system prefix and false DNS configuration after gathering information such as router information and network prefix.
- Due to the fact that default NDP does not need NDP message verification and validation, normal hosts will trust and process RA messages from attackers.
- Utilizing fictitious data from the attacker's RA message, the host will establish an IP address or configure DNS settings.

Table 1: Summary of attack detection and defence mechanisms.

Mechanisms	Limitations
RA-Guard	* Only defend the network against malicious Router Advertisements. * There are impending compatibility difficulties with RA-Guard, and not all Layer 2 devices (switches) support it. * Evasion and DoS attacks are possible.
NDPMon	* Keep track of any specific assaults, whether they are related to routers or neighbors. * Susceptible to evasion * Not intellectual and lacking in support.
SLAAC Security Method	* Implementation in the router uses up additional processing resources. * Local RA that does not transit through the router cannot be filtered; only RA from outside segments can be filtered.
SDN-Based Authentication Mechanism	* Network device compatibility issue with OpenFlow. * Destroy SDN's ability to act as a network controller and not a network security measure.
SLAAC detection mechanism	* Depend entirely on reliable router databases. * Extremely high rate of false positives. * Uses neither a dynamic nor intelligent method of detection.
Snort IPv6 Plugin	* If new accurate information becomes available, reconfiguration is necessary. * Resource-intensive, requiring the verification of every packet and involving numerous attack profiles and attack signatures * Only the Linux platform supports the installation.
Lightweight Secure Router Discovery	* Change NDP by adding additional message options. * Require a server for authentication. * The host and router must incur additional processing costs for the generation and verification of security choices.
Trust-ND	* Modified NDP by default. * Additional processing resources are needed for implementation. * Hash collision attack vulnerable.
Secure Neighbor Discovery protocol (SeND) ADD	* High CPU and memory requirements for the cryptographic and verification processes * Modifications to current NDP (require new ICMPv6 messages). * Management of trust anchors and keys at a cost. * DoS attacks are a threat. * Popular operating systems compatibility problem.

– All packets will be sent to the attacker's workstation if the victim starts any network communication using an unlawful IP address and DNS setup.

– An attacker can temporarily disable a reliable router. All are leaving messages from the segment will be compulsory to pass through the adversary's workstation if the legitimate router is down.

3.2 Design goal

The purpose of this study is to enhance and reinforce the security defenses for the SLAAC procedure. As a result, it suggests SADetection as a detection method for SLAAC attacks (28; 29).

No additional software needs to be installed on the monitored hosts because SADetection serves as a monitoring server. SADetection, on the other hand, just examines and examines particular packets. When a RA message is suspected to be suspicious, SADetection will notify the network administrator.

3.3 Design requirements

The three key requirements for SADetection are: implementing rule-based detection mechanisms; preventing the abuse of packets with extension headers; and ensuring device independence, cross-platform compatibility, and network compatibility.

– Incorporating rule-based detection mechanism: SADetection will add a rule-based detection technique to lessen reliance on a predetermined genuine information database during the packet verification procedure.

– Keep Extension Header Packets from Being Exploited: An exploited packet with a fragment, destination options, and hop-by-hop options extension header was used to attack the SLAAC process on an IPv6 host.

– Network interoperability, cross-platform functionality, and device independence: SADetection will be created as a web-based program that can be used with any operating system and doesn't need specialized hardware for filtering or monitoring.

3.4 Components of SADetection

The intrusion detection system (IDS) design is the foundation for SADetection's design. The three elements that make up the standard design are packet acquisition, packet normalization, and packet analysis (30).

– Packet Acquisition: The data gathering stage is the packet acquisition component. Packet acquisition in SADetection is intended to gather network packets using third-party open-source packet capture software.

– Packet Normalization: The packet must be normalised in order to allow for exact and accurate data processing and analysis.

– Packet Analysis: Most importantly, packet analysis is a requirement. There is a detecting algorithm in it.

3.5 Database architecture of SADetection

Data packet storage and retrieval are made easier by the usage of database tables. Tables are used to hold information about data packets, attack signatures, and lawful and unauthorized packets. In SADetection, seven tables are employed. The tables are the Packet Table, Signature Table, Fragment Table, Log Table, Extension Table, Authentication Table, and RA Table. The Packet Table, RA Table, Fragment Table, and Extension Table are cleaned as part of database maintenance. In order to avoid having a high storage consumption rate, validated packets will be removed from storage after a two-and-a-half (2.5) hour interval. The NDP RFC stipulates that a router's lifetime should not exceed two and a half (2.5) hours; as a result, RAs with lifetimes of more than 2.5 hours may be deemed invalid and destroyed.

4 Proposed SADetection mechanism

A Windows 2016 server running SADetection has Wireshark and Npcap installed as packet capture tools, mySQL installed as a DBMS, PHP installed as an application server, and IIS turned on as a web server. During packet capture, the network interface is set to promiscuous mode so that it can receive all network packets.

It is necessary to preconfigure and tweak Wireshark, Npcap, MySQL server, PHP application server, and IIS webserver. Wireshark and Npcap have been configured to only capture ICMPv6 type 134, fragment packets with a Fragment Offset value of 0, and packets with extension headers for Hop-by-Hop Options, Routing, and Destination Options. In the MySQL database, packet tables, RA tables, fragment tables, extension tables, Auth tables, log tables, and signature tables are constructed beforehand. The database tables that are involved in the implementation.

The victim, attacker, and SADetection server are all located on the same network segment. It is attached to a network switch's mirror port so that it can sniff all network traffic from every machine that is linked to the switch. A network diagram of SADetection in a SLAAC assault scenario is shown in Figure 1. The ideal setup to prevent packet loss and network congestion is to be in the same segment.

Network administrators must set up legitimate router information and a SLAAC attack signature before SADetection is activated. When a new attack packet is discovered, the log table will be filled. When SADetection first starts up, it starts a background packet capture procedure and waits for the Packet Table to fill up with data packets. When Packet Table is full of data packets, SADetection starts the verification process by repeatedly requesting data packets from Packet Table.

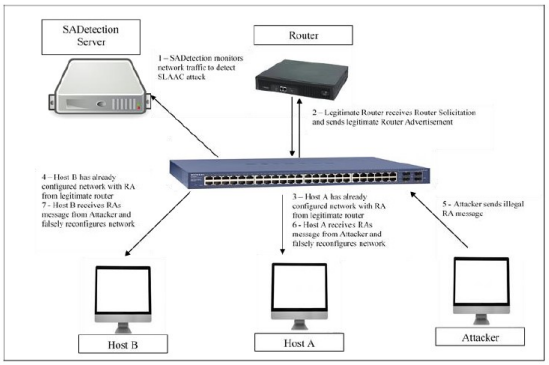


Figure 1: Testbed network for SADetection implementation

Following the capture of the targeted packet, the data packet will initially pass via the Generic Verification (GV) Handler. For the subsequent verification procedure, the GV Handler will route the captured packet to the appropriate module. The RA Handler will handle standard ICMPv6 RA packets, the Fragment Handler will handle fragment packets, and the Extension Handler will handle packets containing Hop-by-Hop Options, Routing, and Destination Options header extensions.

The IP address, MAC address, and network prefix of the packet will be examined after RA Handler has been activated. If a packet's IP address and network prefix match a record in the Authentication table, but its MAC address differs, the Verify MACAddress function will process the packet. On the other hand, the Verify All function will be disabled if the packet being examined's IP address, MAC address, or network prefix does not match any entry in the authentication table. Figure 2 shows RA Handler process flow.

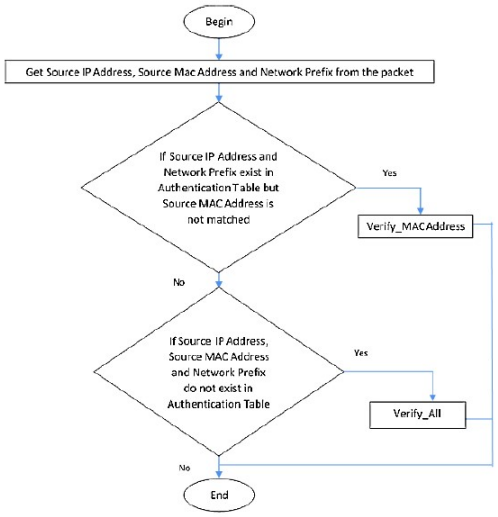
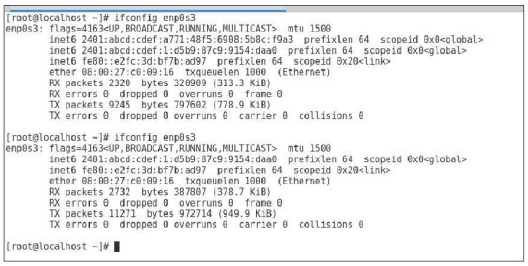


Figure 2: Flow chart of RA handler

5 Security analysis

An examination of security protection is conducted to clarify how SADetection safeguards the IPv6 link-local network. SADetection shields IPv6 hosts against attackers by confirming that no illegitimate prefixes are being spread and utilized by IPv6 hosts when generating IP addresses and configuring DNS settings. Because only approved routers are capable of receiving and sending packets, this condition ensures that no illegal access will occur.

The victims set up a DNS server from the attacker's RA message and generated an IP address with the network prefix 2401:abcd:cdef:a771::. Following the deployment of SADetection in the second scenario, the victim's IP address and DNS server are noted and shown in Figure 3 for Linux CentOS 7 users. Attacker's IP address and DNS server have been blocked on the victims' computers.



A) Neutralized IP address in CentOS 7

B) Neutralized DNS server setup in CentOS 7

Figure 3: Victim's IP address and DNS server in Linux CentOS 7

6 Results and discussion

Based on the study objectives listed in Section 3 and the two criteria of detection capability and network compatibility, SADetection will be assessed. The capacity to detect SLAAC attacks launched using IPv6 extension header-enabled packets as well as IMCPv6 packets is measured as the detection capability of the rule-based detection mechanism.

6.1 Detection capability

Analysis of the detection findings collected during the implementation phase is done to assess detection capabilities. The results of the analysis indicate that SADetection has caught all three SLAAC assault types. Two attack variants are launched by exploiting packets with fragment extension headers and packets with Hop-by-Hop Options extension headers. One attack is initiated using an ICMPv6 packet.

SADetection has proven its capacity to stop the use of packets with extension headers and to identify SLAAC attacks. By guaranteeing no illegal prefix is propagating and being utilised by IPv6 hosts while establishing IP addresses and configuring DNS settings, SADetection can defend IPv6 link-local networks from SLAAC attacks. For the purpose of removing it from the network, SADetection finds suspicious or unauthorised routers. Consequently, only permit reputable and trustworthy routers to remain in the network.

SADetection's capacity to detect SLAAC attacks is compared to other SLAAC attack detection systems for comparative analysis. The SLAAC Security Method by Massamba et al., the SLAAC detection mechanism by Buenaventura et al., and RA Guard are unable to identify illicit RA messages sent using IPv6 packets with extension headers since they do not filter such packets. Table 3 contains an overview of the comparison analysis.

According to the comparison, SADetection is more useful because it can identify SLAAC attacks launched both utilizing IPv6 extension header and ICMPv6 packets. Snort IPv6 Plugin has the ability to identify SLAAC attacks launched using IPv6 packets with extension headers, although the verification mechanism has a very high false positive rate. The Snort IPv6 Plugin mostly relies on predetermined data rather than scanning over IPv6 packets with extension headers.

6.2 Network compatibility

SADetection can be implemented in any IPv6 network that already exists and doesn't need any special hardware. Wireless or wired networks can both be monitored by SADetection. SADetection may be installed to monitor multiple networks at the gateway level because it just needs a dedicated mirror switch port to sniff every packet in the network being monitored. Because SADetection does not interfere with network traffic or use a lot of network capacity, it may be incorporated into or implemented on top of already-existing security tools like firewalls or content filtering.

Windows and Linux servers can both run SADetection. The majority of the equipment and programs required to create and maintain SADetection are open source. Because SADetection was created using a high-level programming language that is compatible with both Windows and Linux platforms, deployment problems will not arise.

6.3 Findings

According to the research's findings, the testbed setup that was suggested for implementation successfully replicated SLAAC attacks and SADetection attack detection. In order to research and monitor SLAAC attack, the testbed has proposed a dummy IPv6 addressing scheme, victim and

Table 2: Impact of SLAAC attack variants on Windows 10 and Linux CentOS 7.

Attack Variant	Impact Windows 10	Impact on Linux CentOS 7
ICMPv6 type 134 attack	Victim generates new IPv6 address with phony RA	Using a bogus RA, the victim generates a new IPv6 address.
Fragment packets attack	Using a bogus RA, and the victim generates a new IPv6 address.	No impact
Attack utilizing the extension header for Hop-by-Hop Options	Using a bogus RA, and the victim generates a new IPv6 address.	Using a bogus RA, the victim generates a new IPv6 address.

Table 3: Comparison of detection capability with other detection mechanisms.

Security Mechanism	Detect Illegal RA message using ICMPv6 packet	Detect Illegal RA message in Packet with Extension Header
SLAAC Security Method by Massamba et al.	Can detect	Cannot detect
SLAAC detection mechanism by Buenaventura et al.	Can detect	Cannot detect
Snort IPv6 Plugin	Can detect	Can detect but very high false positive rate
RA Guard	Can detect	Cannot detect
SADetection	Can detect	Can detect

client machine network configuration and topology, attacking command, and attack scenario.

The testbed may be duplicated to defend against SLAAC attacks on IPv6 link-local networks by locating attackers using any detection mechanism and alerting network administrators so that attackers can be permanently removed from networks. Table 2 below shows how the testbed has determined the effects of each SLAAC attack type on contemporary Linux and Windows operating systems. Windows 10 is affected by all three SLAAC attack versions, however, Linux CentOS 7 is only affected by the attacks using ICMPv6 type 134 and packets with the Hop-by-Hop Options extension header.

7 Conclusion

In order to defend IPv6 link-local networks against SLAAC attacks, this research has suggested a rule-based detection technique. Research aims and objectives have been met by the suggested rule-based detection method. To further improve IPv6 security, it may be possible to expand on the findings of this research in the future. Future work may expand on SADetection directly or from various security and technological vantage points. SADetection is not intended to alter or interfere with any current network setup, network protocol, or host operating system. Additionally, SADetection supports network scalability and dependability, allowing for easy changes in the number of monitored hosts. Due to SADetection's self-control and independence, if it were to become compromised, other hosts or network devices operating inside the same network would not be impacted.

References

[1] J. R. Machana and G. Narsimha, "Optimization of ipv6 neighbor discovery protocol," *Journal of Interconnection Networks*, p. 2141025, 2022. [Online]. Available: https://doi.org/10.1142/S0219265921410255

[2] N. Liu, J. Xia, Z. Cai, T. Yang, B. Hou, and Z. Wang, "A survey on ipv6 security threats and defense mechanisms," in *International Conference on Adaptive and Intelligent Systems*. Springer, 2022, pp. 583–598. [Online]. Available: https://doi.org/10.1007/978-3-031-06794-5_47

[3] S. Deering and R. Hinden, "Internet protocol, version 6 (ipv6) specification," Tech. Rep., 2017. [Online]. Available: http://www.rfc-editor.org/info/rfc8200.

[4] 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, 2020. [Online]. Available: https://doi.org/10.1109/JSEN.2020.3021731

[5] Z. Hamid, S. Daud, I. S. A. Razak, and N. A. Razak, "A comparative study between ipv4 and ipv6," *ANP Journal of Social Science and Humanities*, vol. 2, no. 2, pp. 43–47, 2021.

[6] T. Narten, E. Nordmark, W. Simpson, and H. Soliman, "Neighbor discovery for ip version 6 (ipv6)," Tech. Rep., 2007. [Online]. Available: https://www.rfc-editor.org/rfc/rfc4861.html

[7] S. Thomson, T. Narten, and T. Jinmei, "Ipv6 stateless address autoconfiguration," Tech. Rep., 2007. [Online]. Available: https://www.rfc-editor.org/rfc/rfc4862

[8] M. A. Al-Shareeda and S. Manickam, "Man-in-the-middle attacks in mobile ad hoc networks (manets): Analysis and evaluation," *Symmetry*, vol. 14, no. 8, p. 1543, 2022. [Online]. Available: https://doi.org/10.3390/sym14081543

[9] M. A. Al-Shareeda, S. Manickam, B. A. Mohammed, Z. G. Al-Mekhlafi, A. Qtaish, A. J. Alzahrani, G. Alshammari, A. A. Sallam, and K. Almekhlafi, "Cm-cppa: Chaotic map-based conditional privacy-preserving authentication scheme in 5g-enabled vehicular networks," *Sensors*, vol. 22, no. 13, p. 5026, 2022. [Online]. Available: https://doi.org/10.3390/s22135026

[10] M. A. Al-shareeda, M. A. Alazzawi, M. Anbar, S. Manickam, and A. K. Al-Ani, "A comprehensive survey on vehicular ad hoc networks (vanets)," in *2021 International Conference on Advanced Computer Applications (ACA)*. IEEE, 2021, pp. 156–160. [Online]. Available: http://doi.org/10.1109/ACA52198.2021.9626779

[11] P. Nikander, J. Kempf, and E. Nordmark, "Ipv6 neighbor discovery (nd) trust models and threats," Tech. Rep., 2004. [Online]. Available: https://www.rfc-editor.org/rfc/rfc3756

[12] 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. [Online]. Available: https://doi.org/10.3390/app12031383

[13] A. T. H. Al-hamadani and G. Lencse, "A survey on the performance analysis of ipv6 transition technologies," *Acta Technica Jaurinensis*, vol. 14, no. 2, pp. 186–211, 2021. [Online]. Available: https://doi.org/10.14513/actatechjaur.00577

[14] M. A. Al-Shareeda, S. Manickam, B. A. Mohammed, Z. G. Al-Mekhlafi, A. Qtaish, A. J. Alzahrani, G. Alshammari, A. A. Sallam, and K. Almekhlafi, "Chebyshev polynomial-based scheme for resisting side-channel attacks in 5g-enabled vehicular networks," *Applied Sciences*, vol. 12, no. 12, p. 5939, 2022. [Online]. Available: https://doi.org/10.3390/app12125939

[15] F. Gont, "Implementation advice for ipv6 router advertisement guard (ra-guard)," Tech. Rep., 2014. [Online]. Available: http://www.rfc-editor.org/info/rfc7113.

[16] F. Beck, T. Cholez, O. Festor, and I. Chrisment, "Monitoring the neighbor discovery protocol," in *2007 International Multi-Conference on Computing in the Global Information Technology (ICCGI'07)*. IEEE, 2007, pp. 57–57. [Online]. Available: https://doi.org/10.1109/ICCGI.2007.39

[17] S. Massamba and S. Cheikh, "Securisation of an ipv6 address obtaining with slaac in home networks," *Open Access Library Journal*, vol. 5, no. 3, pp. 1–12, 2018. [Online]. Available: https://doi.org/10.4236/oalib.1104424

[18] D. Nelle and T. Scheffler, "Securing ipv6 neighbor discovery and slaac in access networks through sdn," in *Proceedings of the Applied Networking Research Workshop*, 2019, pp. 23–29. [Online]. Available: https://doi.org/10.1145/3340301.3341132

[19] F. J. Buenaventura, J. P. Gonzales, M. E. Lu, and A. V. Ong, "Ipv6 stateless address autoconfiguration (slaac) attacks and detection," in *Proceedings of the DLSU Research Congress*, vol. 3, 2015, pp. 2–4. [Online]. Available: https://www.dlsu.edu.ph/wp-content/uploads/pdf/conferences/research-congress-proceedings/2015/HCT/015-HCT_Ong_AVL.pdf

[20] M. Schütte, "The ipv6 snort plugin," 2014. [Online]. Available: https://www.idsv6.de/Downloads/TROOPERS14-The_IPv6_Snort_Plugin-Martin_Schuette.pdf

[21] M. A. Al-Shareeda and S. Manickam, "Msr-dos: Modular square root-based scheme to resist denial of service (dos) attacks in 5g-enabled vehicular networks," *IEEE Access*, 2022. [Online]. Available: https://doi.org/10.1109/ACCESS.2022.3222488

[22] N. C. Arjuman, S. Manickam, and S. Karuppayah, "Lightweight secure router discovery mechanism to overcome dos attack in ipv6 network," *International Journal of Computing and Digital Systems*, vol. 8, no. 02, pp. 179–187, 2019. [Online]. Available: http://dx.doi.org/10.12785/ijcds/080209

[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," in *2015 International Conference on Automation, Cognitive Science, Optics, Micro Electro-Mechanical System, and Information Technology (ICACOMIT)*. IEEE, 2015, pp. 31–36. [Online]. Available: https://doi.org/10.1109/ICACOMIT.2015.7440150

[24] M. A. Al-Shareeda, S. Manickam, M. A. Saare, and N. C. Arjuman, "Proposed security mechanism for preventing fake router advertisement attack in ipv6 link-local network," *Indones. J. Electr. Eng.*

Comput. Sci, vol. 2023, no. 29, pp. 518–526, 2023. [Online]. Available: https://doi.org/10.11591/ijeecs.v29.i1.pp518-526

[25] H. Kaur and A. Kaur, "An empirical study of aging related bug prediction using cross project in cloud oriented software," *Informatica*, vol. 46, no. 8, 2022. [Online]. Available: https://doi.org/10.31449/inf.v46i8.4197

[26] M. A. Al-Shareeda, S. Manickam, S. A. Laghari, and A. Jaisan, "Replay-attack detection and prevention mechanism in industry 4.0 landscape for secure secs/gem communications," *Sustainability*, vol. 14, no. 23, p. 15900, 2022. [Online]. Available: https://doi.org/10.3390/su142315900

[27] S. Bourougaa-Tria, F. Mokhati, H. Tria, and O. Bouziane, "Spubbin: Smart public bin based on deep learning waste classification an iot system for smart environment in algeria," *Informatica*, vol. 46, no. 8, 2022. [Online]. Available: https://doi.org/10.31449/inf.v46i8.4331

[28] S. Nie, "Evaluation of innovative design of clothing image elements using image processing," *Informatica*, vol. 46, no. 8, 2022. [Online]. Available: https://doi.org/10.31449/inf.v46i8.4250

[29] M. A. Al-Shareeda and S. Manickam, "Covid-19 vehicle based on an efficient mutual authentication scheme for 5g-enabled vehicular fog computing," *International Journal of Environmental Research and Public Health*, vol. 19, no. 23, p. 15618, 2022. [Online]. Available: https://doi.org/10.3390/ijerph192315618

[30] H. Ran, "Methodology for interval-valued intuitionistic fuzzy multiple attribute decision making and applications to performance evaluation of sustainable microfinance groups lending," *Informatica*, vol. 46, no. 8, 2022. [Online]. Available: https://doi.org/10.31449/inf.v46i8.4355