NDPSEC: Security Mechanism for NEIGHBOR Discovery Protocol

[1]Kammari Swarnalatha, [2]Mekala Abhinav, [3]KondraAkshay, [4] Dr. Ch. Narasimha Chary
[1, 2, 3,] *UG Scholars,* [4]*Assistant Professor*
[1,2,3,4,]*Department of Computer Science and Engineering*
[1,2,3,4,]*Guru Nanak Institutions Technical Campus, Hyderabad, Telangana, India.*

ABSTRACT: IPv6, as the foundation for future internet and IT growth, offers features like a vast address pool, extendable headers, enhanced security, and mobility. A critical component of IPv6 is the Neighbor Discovery Protocol (NDP), which facilitates address resolution, router discovery, and duplicate address detection within local-link networks. However, NDP's trust-based design makes it vulnerable to attacks such as Denial of Service (DoS) on Duplicate Address Detection (DAD), Address Resolution attacks, Router Advertisement (RA) attacks, and Redirect attacks. To address these vulnerabilities, this study introduces an NDP security mechanism (NDPsec) utilizing Ed25519 digital signatures to authenticate IPv6 hosts and prevent unauthorized network access. Compared to existing mechanisms like Secure NDP (SeND), Match-Prevention, and Trust-ND NDPsec demonstrates superior performance, achieving 144% faster processing, over 50% reduced traffic overhead, and enhanced resilience against network attacks in experimental evaluations.

I. INTRODUCTION

The rapid growth of the digital world, driven by advanced technologies like 5G networks, the Internet of Things (IoT), and Cloud Computing, has led to a significant increase in the number of internet-connected devices. According to Cisco, the number of networked devices reached 27.1 billion in 2021, averaging 3.5 devices per person globally. The limited address space of Internet Protocol version 4 (IPv4), which can accommodate approximately 4.3 billion devices, has long been insufficient to meet these demands, necessitating a transition to a protocol with a larger address pool. Internet Protocol version 6 (IPv6) was introduced as the next-generation solution to address this limitation.

Adoption of IPv6 has grown steadily, with over 33% of devices accessing Google using IPv6, as reported by Google. IPv6 provides modest improvements in network security and service quality compared to IPv4. However, it also faces several security challenges, including Denial of Service (DoS) and Man-in-the-Middle (MITM) attacks. To mitigate these issues in link-local networks, IPv6 introduces the Neighbor Discovery Protocol (NDP), defined in RFC 4861. NDP performs critical functions such as Address Resolution (AR), Neighbor Unreachability Detection (NUD), router discovery, and Duplicate Address Detection (DAD).

Despite its importance, NDP was designed with the assumption that devices in a Local Area Network (LAN) are trustworthy. This lack of built-in security measures makes NDP vulnerable to malicious actors who can exploit its processes, leading to DoS, MITM, and other attacks. These vulnerabilities highlight the need for robust security mechanisms to protect NDP operations.

This paper introduces NDPsec, a new mechanism for authenticating NDP communications in IPv6 link-local networks. It builds upon existing methods and assesses their performance in terms of processing time, bandwidth usage, and attack prevention. The structure of the paper includes a review of NDP's processes and associated security threats, as well as privacy concerns related to IPv6 addressing. It details the design and implementation of NDPsec and evaluates its performance compared to existing security measures. The findings demonstrate the effectiveness of NDPsec in enhancing security for NDP communications by mitigating vulnerabilities in message exchanges, such as Address Resolution, DAD, and router discovery, which are critical to IPv6 network functionality.

II. RELATED WORK

The Neighbor Discovery Protocol (NDP) in IPv6 link-local networks faces significant security challenges, including vulnerabilities to Denial of Service (DoS) and Man-in-the Middle(MITM) attacks. Various mechanisms have been proposed to address these issues, but they have notable limitations:

NDPmon: While capable of detecting threats and issuing alerts, NDPmon fails to prevent attacks, especially from legitimate users or when attackers spoof IP or MAC addresses. It also struggles with false positives during network modifications.

INDPmon: This mechanism uses an Extended Finite State Machine (EFSM) to detect protocol violations through strict anomaly detection. However, it cannot handle spoofed packets effectively, leaving it inadequate for securing NDP processes.

SAVA and SAVI: The Source Address Validation Architecture (SAVA) and its improvement, SAVI, authenticate source IP addresses and map them to MAC addresses and switch ports. While effective in addressing spoofing, these mechanisms fail to cover other NDP vulnerabilities, such as DoS attacks during Duplicate Address Detection (DAD) and Address Resolution.

Secure NDP (SeND): SeND enhances security by adding options like cryptographically generated addresses (CGA) and RSA-based signatures. However, it introduces high processing overhead, increased bandwidth usage, and complexity, making it unsuitable for certain environments.

Trust-ND: This lightweight mechanism uses the SHA-1 hash algorithm for address verification. However, it remains vulnerable to hash spoofing and does not comprehensively secure NDP messages.

Match-Prevention: This approach uses SHA-3 to hash tentative IP addresses and verify messages in Address Resolution and DAD processes. While effective in some scenarios, it cannot secure all NDP messages, especially if attackers know the sender's IPv6 address.

Given the limitations of these methods, an effective and comprehensive mechanism is needed to secure NDP processes in IPv6 link-local networks, particularly against DoS attacks.

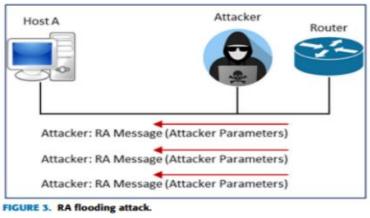
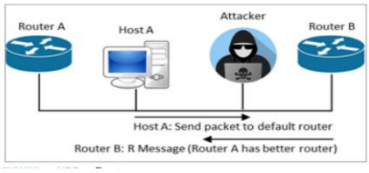


FIGURE 3. RA flooding attack.



III. METHODOLOGY- ALGORITHMS USED

MITM Attacks:

IPv6 link-local networks are particularly susceptible to Denial of Service (DoS) and Man-in-the-Middle (MITM) attacks, with MITM being one of the most critical threats. These vulnerabilities arise from the inherent trust assumed in the Neighbor Discovery Protocol (NDP), which underpins essential network operations such as Address Resolution (AR), Duplicate Address Detection (DAD), and router discovery. Attackers with access to the same local network can exploit this trust by intercepting or altering NDP messages exchanged between devices. This manipulation allows them to disrupt communication, impersonate other nodes, and execute targeted attacks at will, including DoS attacks that overwhelm network resources. As a result, NDP processes are frequently targeted by cyberattacks, making robust security measures critical to protecting IPv6 networks from significant risks.

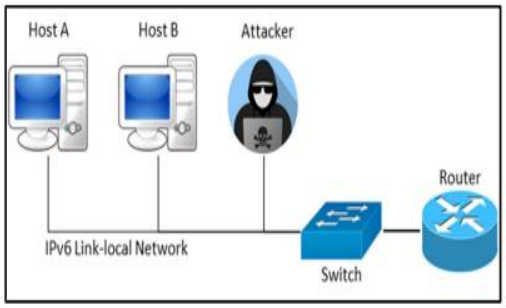
NDPsec Model:

Existing mechanisms to secure NDP processes in IPv6 link-local networks often face challenges like high processing times, making them susceptible to DoS and MITM attacks through message flooding. To address these vulnerabilities, this study proposes NDPsec, a mechanism that enhances security using digital signatures. NDPsec utilizes the Link Fingerprint (LF) as an Interface Identifier (IID) to create a secure IPv6 address. The Router Fingerprint (RF) works with the IID to reconstruct a public key on the receiving host, enabling message validation and ensuring integrity. This approach offers an efficient, lightweight, and robust solution to secure NDP messages against attacks.

IV. RESULTS

The proposed NDPsec mechanism is designed to authenticate NDP messages, and its performance is evaluated through experiments. The evaluation compares NDPsec with existing mechanisms, including Standard NDP, SeND, Match-Prevention, and Trust-ND, focusing on two main criteria: (i) performance, which includes the processing time for generating IPv6 addresses, verifying, and generating NDP messages, and (ii) penetration testing, which assesses the mechanism's ability to withstand attacks. The results of these experiments are presented in this section, demonstrating the effectiveness and efficiency

of NDPsec in enhancing the security of NDP processes in IPv6 link-local networks.



Item Name	CPU	Memory	Operating System
Host A	Intel(R) Core(TM) i7-2640M CPU @ 2.3 GHz × 4	4.00 Gb	Ubuntu 16.04
Host B	Intel(R) Core(TM) i7-3770M CPU @ 3.40GHz × 8	8.00 Gb	Windows 10 Pro
Attacker Host	Intel(R) Core(TM) i7-2640M CPU @ 2. 30GHz × 4	6.00 Gb	Ubuntu 16.04
Switch (SW)	Cisco Catalyst 2960 Fast Ethernet		
Router	Cisco Router C7200		

V.CONCLUSION

Securing NDP messages is crucial for IPv6 link-local networks, as the standard NDP protocol lacks message verification, allowing attackers to exploit NDP messages for attacks. NDPsec addresses these issues with a modern approach, using the Ed25519 digital signature for IPv6 address generation and authentication. The experiments show that NDPsec outperforms SeND, Match-Prevention, and Trust-ND in most cases, making it a better alternative for securing NDP messages. Future work could focus on adapting NDPsec for use with stateful modes like DHCPv6 and developing a mechanism to distribute router public keys in the network.

VI. REFERENCE

[1] Y. Huang, S. Nazir, X. Ma, S. Kong, and Y. Liu, ‘‘Acquiring data traffic for sustainable IoT and smart devices using machine learning algorithm,’’ Secur. Commun. Netw., vol. 2021, pp. 1–11, Jun. 2021.

[2] S. Suryavansh, A. Benna, C. Guest, and S. Chaterji, ‘‘Ambrosia: Reduction in data transfer from sensor to server for increased lifetime of IoT sensor nodes,’’ 2021, arXiv:2107.05090.

[3] K.-H. Li and K.-Y. Wong, ‘‘Empirical analysis of IPv4 and IPv6 networks through dual-stack sites,’’ Information, vol. 12, no. 6, p. 246, Jun. 2021.

[4] A. Al-Ani, M. Anbar, S. A. Laghari, and A. K. Al-Ani, ‘‘Mechanism to prevent the abuse of IPv6 fragmentation in OpenFlow networks,’’ PLoS ONE, vol. 15, no. 5, May 2020, Art. no. e0232574.

[5] Google. (2021). Google IPv6 and Google. Accessed: Sep. 2, 2019. [Online]. Available: https://www.google.com/intl/en/ipv6/statistics.html

[6] L. Ubiedo, T. O’Hara, M. J. Erquiaga, and S. Garcia, ‘‘Current state of IPv6 security in IoT,’’ 2021, arXiv:2105.02710.

[7] T. Narten, E. Nordmark, W. Simpson, and H. Soliman, Neighbor Discovery for IP Version 6 (IPv6), RFC 4861, Sep. 2007.

[8] 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, Apr. 2019, Art. no. e0214518.

[9] E. Mahmood, A. H. Adhab, and A. K. Al-Ani, ‘‘Review paper on neighbour discovery protocol in IPv6 link-local network,’’ Int. J. Services Oper. Inform., vol. 10, no. 1, pp. 65–78, 2019. VOLUME 10, 2022 83661

[10] F. Abusafat, T. Pereira, and H. Santos, ‘‘Roadmap of security threats between IPv4/IPv6,’’ in Proc. IEEE Int. IoT, Electron. Mechatronics Conf. (IEMTRONICS), Apr. 2021, pp. 1–6.

[11] J. L. Shah and H. F. Bhat, ‘‘Towards a secure IPv6 autoconfiguration,’’ Inf. Secur. J., Global Perspective, vol. 29, no. 1, pp. 14–29, Jan. 2020.

[12] M. Tayyab, B. Belaton, and M. Anbar, ‘‘ICMPv6-based DoS and DDoS attacks detection using machine learning techniques, open challenges, and blockchain applicability: A review,’’ IEEE Access, vol. 8, pp. 170529–170547, 2020.