DENIAL OF SERVICE ON DUPLICATE ADDRESS DETECTION USING NDPsec

Mrs . SARANYA E M.E
Assistant Professor
Department Of Computer Science
E.G.S Pillay Engineering College
Nagapattinam,India
saranyaedumban@gmail.com

MOHAMED SAKKEEL M
UG Student
Department Of Computer Science
E.G.S Pillay Engineering College
Nagapattinam,India
sakkeelmohamed69@gmail.com

MOHAMED YASEER M
UG Student
Department Of Computer Science
E.G.S Pillay Engineering College
Nagapattinam,India
yaseercse@gmail.com

PUNNIYAMOORTHI R
UG Student
Department Of Computer Science
E.G.S Pillay Engineering College
Nagapattinam,India
moorthicse17@gmail.com

***Abstract*—**Neighbor Discovery Protocol (NDP) is a stateless protocol used by Internet Protocol Version 6 (IPv6) to find hosts and routers in an IPv6 network.neighbor discovery involves the identification of neighboring nodes for connection and communication.The Edwards-curve Digital Signature Algorithm (EdDSA) was proposed to perform fast public-key digital signatures.the first practical fault attack against EdDSA or Ed25519.Neighbor discovery protocol (NDP) is the core protocol of Internet protocol version 6 (IPv6)A malicious host is able toexpose denial of service or man-in-the-middle attacks by injecting spoofed address in NDP messages.This article revolves around the survey of the vulnerabilities mitigations approaches of NDP.ICMPv6-based Denial of Service (DoS) attacks and its variant form Distributed Denial of Service (DDoS) attack. To detect ICMPv6-based DoS and DDoS attacks as single and hybrid classifiers. Address Resolution (AR) and Duplicate Address Detection (DAD) are considered the most important processes in Neighbour Discovery Protocol (NDP), which occurs frequently from each Internet Protocol version 6 (IPv6) host communicating with other neighbouring hosts. Two NDP messages are used during AR and DAD to communicate with one another in the same IPv6. Neighbour Solicitation (NS) and Neighbour Advertisement (NA) messages.DOS on duplicate address detection proposes an NDP security (NDPsec) mechanism based on the Ed25519 digital signature to authenticate IPv6 hosts to prevent unauthorized devices from joining the network. The proposed NDPsec mechanism is evaluated and compared to Secure NDP (SeND), Match-Prevention, and Trust-ND mechanisms.The optimization of the neighbor discovery to reduce the power consumption in wireless sensor networks.

Keywords - IPv6 link-local Network, NDP, denial of service, DDoS, duplicate address detection, address resolution,Anomaly Detection,authentication.

I. INTRODUCTION

The NDP (Neighbor Discovery Protocol) is a key component of the IPv6 protocol suite. It is responsible for address resolution, neighbor unreachability detection, and router discovery in IPv6 networks.In IPv6, the NDP protocol replaces the functions of the Address Resolution Protocol (ARP) and the Internet Control Message Protocol (ICMP) Router Discovery protocol. The main functions of NDP include: Address Resolution,Address Resolution,Neighbor Unreachability,Duplicate Address Detection.he Neighbor Discovery Protocol (NDP) in IPv6 also provides support for securing network communication using digital signatures. Digital signature algorithms are used to ensure the authenticity and integrity of network traffic, thereby preventing various forms of malicious attacks.ECDSA is used in NDP to provide secure router advertisement and neighbor solicitation messages. These messages are used to discover routers and other devices on the network and to maintain a cache of known network entities. By using ECDSA to sign these messages.To implement ECDSA in NDP, each network entity generates a public-private key pair. The private key is kept secret and is used to sign outgoing messages, while the public key is shared with other network entities to verify the authenticity of incoming messages. The signing and verification process is performed using complex mathematical operations that are computationally efficient, even on resource-constrained devices.The results obtained from the experiments showed that NDPsec successfully prevented cyberattacks, with approximately 144% less processing time and over 50% less traffic overhead compared to SeND (the default security mechanism for NDP protocol)[1].

II. RELATED WORK

A. LITERATURE SURVEY

Detecting ICMPv6-based DoS and DDoS attacks as single and hybrid classifiers.ICMPv6 has been given a vital

role by the designers of IPv6 as compared to its previous version IPv4.. For example, the NDP which uses ICMPv6 messages has been introduced by IPv6 as a new protocol for Stateless Address Auto Confifiguration (SLAAC), discovering link-layer addresses, routers discovery, and Duplicate Address Detection (DAD) processes[2].

Address Resolution (AR) and Duplicate Address Detection (DAD) are considered the most important processes in Neighbour Discovery Protocol (NDP).
Techniques proposed to secure AR and DAD include Secure NDP (SeND) and Trust-NDP (Trust-ND).NDP is a key protocol in the IPv6 network, and it has many processes, such as Address Resolution (AR), Neighbour Unreachability Detection (NUD) and Duplicate Address Detection (DAD). The designer of the IPv6 network presumes that the local area network (LAN) comprises trusted nodes. Therefore, every node inside the LAN is trusted by the NDP. This condition makes the network vulnerable to various attacks, such Denial Of Service (DoS)[10].

A malicious host is able to expose denial of service or man-in-the-middle attacks by injecting spoofed address in NDP messages.The survey of the vulnerabilities mitigations approaches of NDP, since the time of the protocol development[11].

Power consumption is one of the important research concerns in low-power, low-cost communication networks such as sensor networks.The neighbor discovery process becomes a power-consuming task if two neighboring nodes do not know when their partner wakes up and sleeps[7].

NDPsec also present our approach for this task together with the functionalities we provide and the software, NDP that we developed.The need to monitor and manage the associated protocols increases.The exponential growth of the Internet in the nineties brought several problems, due to drawbacks in the IPv4 protocol. To overcome these limits, a new version of the IP protocol, IPv6 was defined, bringing with it advanced builtin services. One of the objectives of IPv6 was to ease the addressing of the hosts, the discovery of network components[9].

B. *NDP sec METHODOLOGY*

Each network entity that wishes to participate in secure NDP must generate a public-private key pair. The private key is kept secret and is used to sign outgoing messages, while the public key is shared with other network entities to verify the authenticity of incoming messages.When a network entity sends a router advertisement or neighbor solicitation message, it signs the message using its private key and includes the resulting digital signature in the message. This ensures that the message has not been tampered with in transit and that its contents are authentic.Verifying Incoming Messages.

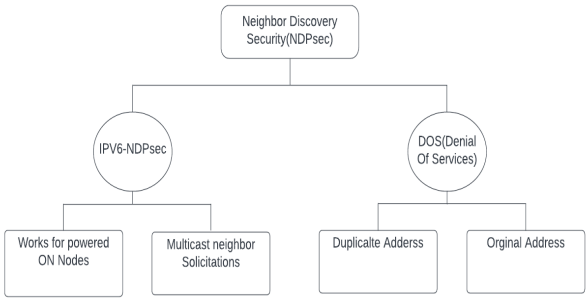

Figure 1.NDPsec

Network entity receives a router advertisement or neighbor solicitation message, it uses the sender's public key to verify the message's digital signature. If the verification process succeeds, the message is considered authentic, and its contents are accepted.Network entities must manage their public-private key pairs carefully to prevent unauthorized access or tampering. This may involve using secure storage mechanisms, such as hardware security modules, to protect the private key.Trust Management: To ensure the security of NDP messages, network entities must trust each other's public keys. This may involve using a trusted third party, such as a certificate authority, to verify the authenticity of public keys.

III. EXISTING METHODOLOGIES

Securing NDP in IPv6 with digital signature algorithms is defined in RFC 3971, "Secure Neighbor Discovery (SEND)". SEND extends the standard NDP protocol by adding support for digital signature algorithms.

Cryptographic Keys: Each network entity generates a public-private key pair for use in signing and verifying NDP messages. The private key is kept secret and is used to sign outgoing messages, while the public key is shared with other network entities to verify incoming messages.

Certificate Management: SEND uses X.509 digital certificates to bind public keys to network entities. Network entities obtain certificates from trusted certificate authorities (CAs) and use them to verify the authenticity of other entities' public keys.

Neighbor Cache Protection: SEND protects the neighbor cache, which stores information about neighboring nodes on the network, from attacks. It does this by including a cryptographic checksum in the neighbor cache entries, which is used to detect any changes made to the entry. Security associations are established between pairs of network entities and are used to protect NDP messages between them.

A. *PROPOSED FRAMEWORK*

NDPsec were used to Each network entity generates an Ed25519 public-private key pair for use in signing and

verifying NDP messages. The private key is kept secret and is used to sign outgoing messages, while the public key is shared with other network entities to verify incoming messages.

Network entities obtain digital certificates from trusted certificate authorities (CAs) and use them to verify the authenticity of other entities' private key.Network entities obtain digital certificates from trusted certificate authorities (CAs) and use them to verify the authenticity of other entities' public key.

The neighbor cache is protected from attacks by including a cryptographic checksum in the neighbor cache entries, which is used to detect any changes made to the entry.Security associations are established between pairs of network entities and are used to protect NDP messages between them., advanced techniques such as multiparty computation or homomorphic encryption.

B. WORKING METHODOLOGIES

IPv6 Neighbor Discovery Protocol (NDP) is used for various tasks, including address resolution, duplicate address detection, and router discovery. Since NDP is a critical component of IPv6, it is essential to secure it from various security threats.

C. EDDSA

EdDSA (Edwards-curve Digital Signature Algorithm) is a modern digital signature algorithm based on the elliptic curve cryptography.

The algorithm is based on the Edwards-curve, a special type of elliptic curve that is resistant to certain types of attacks. EdDSA involves generating a public-private key pair, where the private key is used to sign messages and the public key is used to verify the signature.

The signing process involves a random nonce and a message hash, which together create a signature that is unique to that message.EdDSA uses elliptic curve cryptography, which provides a high level of security with a smaller key size compared to other digital signature algorithms. The key size for EdDSA varies depending on the specific elliptic curve used, but typical key sizes range from 256 bits to 512 bits.

The security of EdDSA depends on the hardness of the elliptic curve discrete logarithm problem (ECDLP). The ECDLP is the problem of finding the scalar value k in the equation P = kG, where P is a point on the elliptic curve, G is a generator point, and k is the scalar value that multiplies the generator point to produce P. The security of EdDSA depends on the difficulty of solving the ECDLP for the specific elliptic curve used.

IV. DUPLICATE ADDRESS DETECTION THREAT

IPv6 link-local network, two types of NDP messages are utilized during the DAD: NS and NA. Verify the uniqueness of an IPv6 local-link network address is necessary when the host joins an IPv6 local-link network, the host creates a tentative IP address.

DAD can be vulnerable to certain types of attacks. Here are some common types of DAD threat attacks:

Address Spoofing attacks: In this type of attack, an attacker spoofs the source IP address in DAD messages, making it appear as if the message is coming from a legitimate device. This can cause confusion and lead to IP address conflicts.

Man-in-the-Middle (MitM) attacks: In this type of attack, an attacker intercepts DAD messages and modifies them before forwarding them on to their destination. This can cause devices to use the wrong IP address, leading to communication problems.

Address Flooding attacks: In this type of attack, an attacker floods the network with a large number of DAD messages, causing devices on the network to become overwhelmed and unable to respond to legitimate DAD requests.

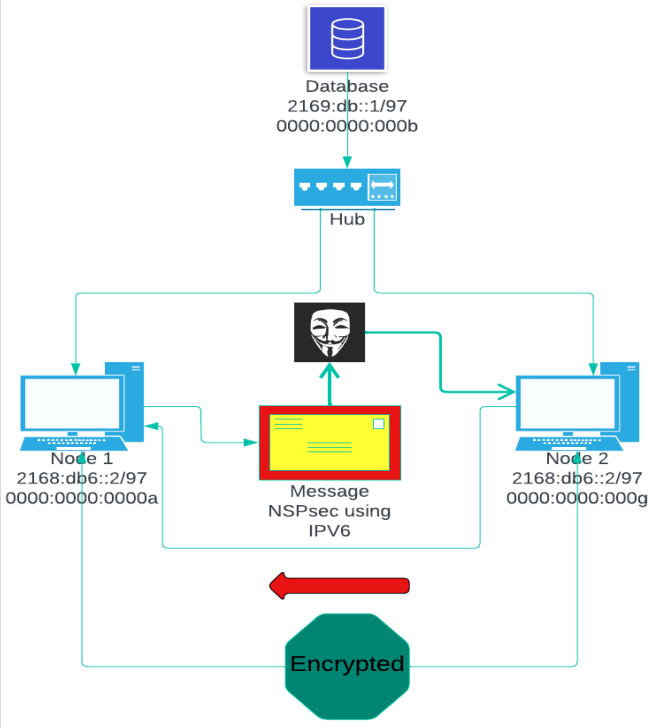

Figure 2.Peer To Peer Encrpytion Attack

Attacker might reply to an NS message by returning a bogus NA response stating that the produced tentative IP address has already been taken thus, it is not unique and cannot be used by the requesting host. Although the IP address is unique, the reply received from the malicious host would prohibit requesting IPv6 host from self-assigning this unique IP address. As a result, the host is unable to join the network and communicate with other hosts. As exhibited in previous studies, this kind of attack is referred to as Denial of Service (DoS) on Duplicate Address Detection (DAD) attacks

A. Secure Neighbor Discovery(SEND)

SEND is an IPv6 extension that provides security for NDP messages. In this methodology, devices use digital signatures to authenticate NDP messages. Each device has a certificate that includes its public key, and the certificate is signed by a trusted third-party certificate authority (CA). When a device sends an NDP message, it signs the message with its private key and includes its certificate.

The recipient device verifies the digital signature using the sender's public key and the CA's public key. This methodology provides end-to-end security for NDP messages and prevents attacks such as spoofing and tampering.

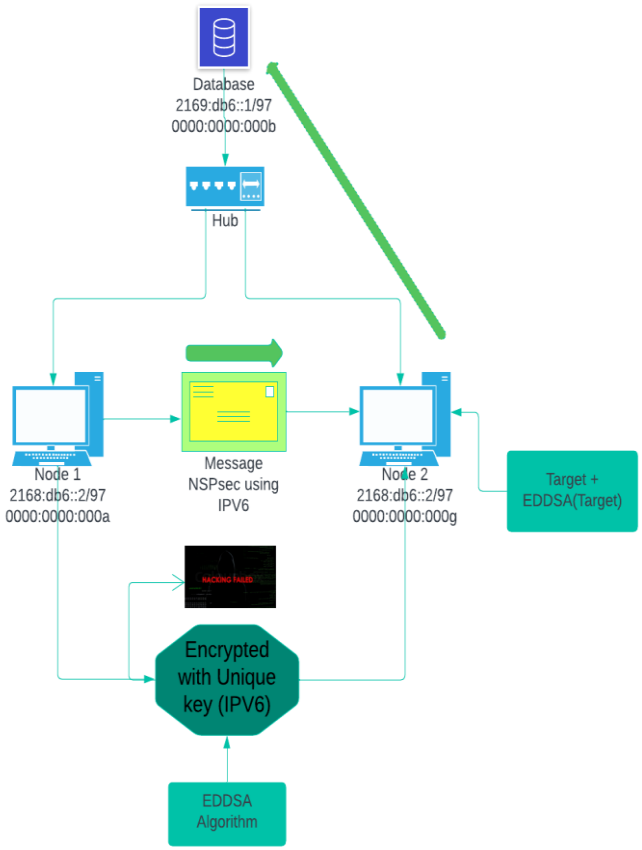

Figure 3.Peer To Peer Security Attack

B. Cryptographically Generated Addresses (CGA)

CGA is a method of generating IPv6 addresses that includes a digital signature. In this methodology, each device generates a public/private key pair and uses the public key to generate its IPv6 address.

The device signs the address with its private key, and the signature is included in the address. When a device sends an NDP message, it includes its CGA address, which includes the digital signature. The recipient device verifies the digital signature using the sender's public key. This methodology provides authentication of the sender's IPv6 address, which prevents address spoofing attacks.

C. ADDRESS RESOLUTION THREAT

The attacker can reply to an NS instead of the real host. So, the victim will send its packets to the attacker instead of the real host. The attack can be even worse when the spoofed node is the default router.

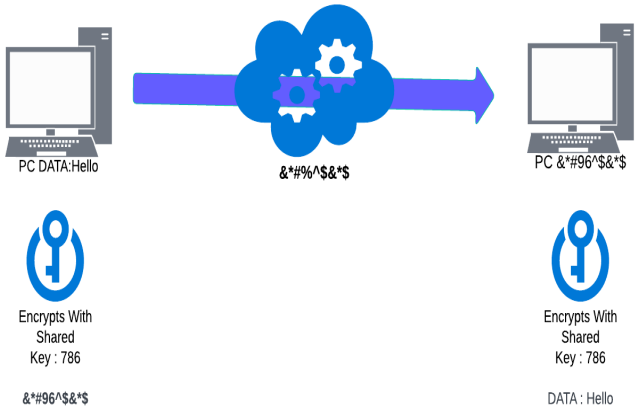

Figure 4.Peer To Peer Key Exchange

D. REDIRECT THREAT

Securing Neighbor Discovery Protocol (NDP) in IPv6 is essential to prevent various network threats, including redirect threats. Redirect threats occur when an attacker sends false router advertisements to redirect traffic to a malicious node, allowing the attacker to intercept, modify or drop packets. Access control policies should be implemented to limit access to the network infrastructure, preventing attackers from sending unauthorized NDP messages.

E. IMPACT OF DOS TABLE

The following table which shows the types of DoS attacks.

Table 1.DoS Attack Types

DoS Attack Type	Impact on DAD using NDPSec
ICMP Flood	NDPSec is designed to detect and prevent DoS attacks, but if the flood is large enough, it may still cause disruption
SYN Flood	NDPSec can detect and prevent SYN Flood attacks, preventing them from impacting DAD
UDP Flood	NDPSec can detect and prevent UDP Flood attacks, preventing them from impacting DAD
Smurf Attack	NDPSec can detect and prevent Smurf attacks, preventing them from impacting DAD

V. CONCLUSION

In conclusion, securing Neighbor Discovery Protocol (NDP) in IPv6 is crucial to prevent various network threats, including redirect threats. NDP plays a vital role in IPv6 networks by enabling hosts to discover and communicate with their neighbors.

However, NDP is vulnerable to various attacks, such as redirect attacks, which can compromise the security of the network.

To secure NDP in IPv6, network administrators should implement various measures, such as securing NDP messages using encryption and authentication, using Secure Neighbor Discovery (SEND), implementing RA guard, implementing access control policies, and monitoring network traffic.

By implementing these measures, network administrators can ensure the security of their IPv6 networks and prevent attackers from intercepting, modifying or redirecting traffic.

VI. FUTURE SCOPE

The importance of securing NDP becomes increasingly critical. Here are some potential future developments in securing NDP in IPv6:Integration with AI and machine learning: With the increasing complexity of network infrastructures and security threats,technology is a distributed ledger that provides secure, transparent, and tamper-proof transactions,Advanced encryption and authentication methods: Researchers are working on advanced encryption and authentication methods to enhance the security of NDP messages.Increased adoption of IPv6 security protocols: There are several IPv6 security protocols, such as SEND, that can secure NDP messages. The increased adoption of these protocols can enhance the security of NDP in IPv6 networks.

REFERENCES

[1]Ayman al-ani1,Ahamed k.al-ani2,Shams a.laghari3,Selvakumar manickam3,Khin wee lai4, (Senior Member, IEEE), And Khairunnisa Hasikin 4, “NDPsec: Neighbor Discovery Protocol Security Mechanism” , NO.3 August 2022.

[2]Mohammad Tayyab,Bahari Belaton,Mohammed Anbar , (Member, IEEE) ,”ICMPv6-Based DoS and DDoS Attacks Detection Using Machine Learning Techniques, Open Challenges, and Blockchain Applicability“,NO.September 28, 2020.

[3]Firas Najjar, Mohammad Kadhum, *Member,IEEE*, Homam El-Taj,” Neighbor Discovery Protocol Anomaly Detection Using Finite State Machine and Strict Anomaly Detection”,No.July 2015.

[4]Yolan Romailler, Sylvain Pelissier ,Kudelski Security Cheseaux-sur-Lausanne,”Practical fault attack against the Ed25519 and EdDSA signature schemes”,NO.2017.

[5]Ayman Al-Ani, Mohammed Anbar*, Shams A. Laghari , Ahmed K. Al-Ani
“Mechanism to prevent the abuse of IPv6 fragmentation in OpenFlow networks”,NO. 2020.

[6]Hua Chun Liu ,Qing Guang Dai,”Design of Security Neighbor Discovery Protocol “,NO.2013.

[7]Amjed Sid Ahmed Mohamed Sid Ahmed,”IPv6 Neighbor Discovery Protocol Specifications, Threats and Countermeasures: A Survey”,NO.August 2017.

[8]Kwun-Hung Li and Kin-Yeung Wong,”Empirical Analysis of IPv4 and IPv6 Networks through Dual-Stack Sites”,NO.14 June 2021.

[9]Frederic Beck, Thibault Cholez, Olivier Festor and Isabelle Chrisment,”Monitoring the Neighbor Discovery Protocol”,NO.2007.

[10]Ahmed K.al-ani,Mohammed Anbar,Ayman al-ani,and Dyalar R.Ibrahim,”Match-Prevention Technique Against Denial-of-Service Attack on Address Resolution and Duplicate Address Detection Processes in IPv6 Link-Local Network “,January 31, 2020.

[11]Sangil Choi 1 and Gangman Yi 2,"Neighbor Discovery Optimization for Big Data Analysis in Low-Power, Low-Cost Communication Networks ",No.26 June 2019.

[12]Demin Gao, *Member, IEEE,* Zhijun Li, *Member, IEEE,* Yunhuai Liu, *Member, IEEE,"*Neighbor Discovery based on Cross-Technology Communication for Mobile Applications ",NO.2020.

[13]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.

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

[15] A. Al-Ani, M. Anbar, A. K. Al-Ani, and I. H. Hasbullah, ''DHCPv6Auth: A mechanism to improve DHCPv6 authentication and privacy,'' Sadhana, Acad. Proc. Eng. Sci., vol. 45, no. 1, Dec. 2020.

[16] A. Al-Ani, M. Anbar, I. H. Hasbullah, R. Abdullah, and A. K. Al-Ani, ''Authentication and privacy approach for DHCPv6,'' IEEE Access, vol. 7, pp. 73144–73156, 2019. Accessed: Jun. 30, 2022.