RUJCST
جامعة الرازي
Al-Razi University
كلية الحاسوب وتقنية المعلومات
ISSN-L 3007-5084
مجلة جامعة الرازي لعلوم الحاسوب وتقنية المعلومات
Al-Razi University Journal of Computer Science and Technology
علمية محكمة تصدر عن كلية الحاسوب وتقنية المعلومات - جامعة الرازي

SURVEY: SECURING IPV6 NEIGHBOR DISCOVERY PROTOCOL

Mohammed Ghaleb M.Ageel
Faculty of Computer and IT
Department of IT
Al- Razi University
Sana'a, Yemen
MohammedAqeel014@gmail.com

Yosef A. Abdulmoghni
Faculty of Computer and IT
Department of IT
Al- Razi University
Sana'a, Yemen
Youssef.almoghni@gmail.com

Yahya Al-Ashmoery
Faculty of Computer and IT
Department of IT - Al- Razi University
Department of Mathematics &
Computer Faculty of Science, Sana'a University
Sana'a, Yemen
Yah.AlAshmoery@su.edu.ye

Abstract: **IPv6 Neighbor Discovery Protocol (NDP) is essential to facilitate communication between local network nodes. However, NDP is vulnerable to various attacks that can disrupt network communication and facilitate malicious activities. This study attempts to identify the major security vulnerabilities to NDP and assess available methods to improve its security. We conducted a systematic literature review to analyze the benefits and limitations of mechanisms such as Cryptographically Generated Addresses (CGA), Secure Neighbor Discovery (SEND), and Attestation-based Neighbor Discovery. Our findings show that these mechanisms significantly reduce the impact of Neighbor Discovery attacks. We recommend an attack detection mechanism to address spoofing of Neighbor Solicitation (NS) and Neighbor Advertisement (NA) messages to improve NDP security in IPv6 networks. These insights can help network administrators and protocol designers implement effective defenses against NDP attacks, thereby enhancing the stability and security of IPv6 deployments. Our research contributes to ongoing efforts to improve IPv6 network reliability by investigating the protocol's structure, the role of ICMPv6, associated security concerns, and potential security solutions.**

Keywords— Neighbor Discovery Protocol (NDP) - Address Resolution Protocol (ARP) - Internet Protocol version 6 (IPv6) - Man in the Middle (MiTM) – Denial of Service (DoS) - Internet Control Message Protocol version 6 (ICMPv6) - NDP security- Secure Neighbor Discovery- Cryptographically Generated Addresses

I. INTRODUCTION

IPv6 was developed to replace IPv4, bringing significant improvements such as a vastly larger address space, which resolves the address shortage issues inherent in IPv4[1, 2]. Furthermore, IPv6 provides improved security characteristics over its predecessor. However, the adoption of IPv6 protocols has generated additional security vulnerabilities, which must be addressed[3]. Studies have explored the delayed adoption of IPv6, revealing that many enterprises do not see the immediate necessity of integrating it into their networks, perceiving it as a complex and challenging technology to deploy[4]. Security concerns have also contributed to the slow uptake of IPv6 [5].

The IPv6 Neighbor Discovery Protocol (NDP) is a critical component that ensures device connection inside Local Area Networks (LANs). It enables devices to discover, recognize, and communicate with neighboring nodes[6]. However, NDP is susceptible to various cyber-attacks, which can compromise the reliability and accuracy of communications mediated by NDP, posing significant security and functional risks to the LAN infrastructure[7].

The neighbor discovery protocol (NDP) is an important protocol and in the IPv6 protocol suite. Its tasks include discovering the MAC address associated with an IPv6, rerouting packets from one router to another, duplicate address identification, finding routers on the network, and address resolution. NDP uses several ICMPv6 message types to conduct its functions, including neighbor solicitation (NS), neighbor advertisement (NA), router solicitation (RS), and router advertisement (RA)[8]. Security is a top priority due to NDP's inherent vulnerabilities in address resolution and auto-configuration, which attackers might exploit to infect devices, intercept traffic, or overload networks. Some of the main risks are traffic hijacking through the marketing of fake network prefixes, MITM attacks that impersonate address resolves, and the flooding of NS or NA messages[9].

Cyber assaults represent a substantial threat to the dependability and accuracy of communications supported by the Neighbor Discovery Protocol (NDP)[10, 11]. These attacks target the vulnerabilities within the NDP, such as Denial of Service (DoS) on Duplicate Address Detection (DAD) attacks, Address Resolution-based attacks, Router Advertisement (RA) based attacks, and Redirect attacks, which can compromise the security of IPv6 hosts and networks[10]. Furthermore, the lack of security mechanisms in the NDP protocol makes it a prime target for various cyber-attacks, leading to potential disruptions in communication and network integrity[11]

RUJCST
جامعة الرازي
Al-Razi University
كلية الحاسوب وتقنية المعلومات
ISSN-L 3007-5084
مجلة جامعة الرازي لعلوم الحاسوب وتقنية المعلومات
Al-Razi University Journal of Computer Science and Technology
علمية محكمة تصدر عن كلية الحاسوب وتقنية المعلومات - جامعة الرازي

Securing NDP in LANs is vital to prevent disruptions in communication and address allocation. Researchers have proposed multiple techniques to enhance NDP security and resilience against cyber threats, such as Secure Neighbor Discovery (SEND), NDPMon, Software Defined Networks (SDN)-based solutions, and innovative cryptographic approaches[12-15]. These solutions aim to mitigate DoS attacks by improving NDP message verification, protecting Neighbor Solicitation (NS) and Neighbor Advertisement (NA) messages, and reducing the risks associated with address spoofing and flooding attacks. Advanced security methods like ABS based on the Blake2 algorithm and novel concepts such as ABS domain have been suggested to prevent rogue nodes from interfering with the automatic configuration process and ensure the uniqueness of IP addresses in local networks[9, 16-19]. Additionally, new algorithms like DH and HMAC have been proposed to enhance security compared to previous systems such as Trust-ND. Digital signatures are also employed to authenticate IPv6 hosts and prevent unauthorized devices from connecting to the network [14, 15, 20]. These solutions collectively aim to bolster the security of IPv6 Neighbor Discovery in LAN environments Over the last two decades, IPv6 security research has made substantial progress, as indicated by a rise in publications and citations, indicating a rising global interest in IPv6 security challenges. The expansive address space of IPv6 compared to IPv4 presents new challenges as attackers develop new tools and strategies, underscoring the importance of adapting tools and monitoring technologies for IPv6[21]. Recent research has proposed innovative solutions such as a unique neighbor discovery mechanism for IPv6 over BLE mesh networks[22]. Similarly, a 2023 study introduced a secure blockchain-based neighbor discovery method that leverages blockchain's immutability and decentralization to enhance the protocol's integrity and reliability[23].Attacks targeting Neighbor Discovery in Internet of Things (IoT) devices within smart home environments highlight the critical need for robust security protocols in IPv6 LAN deployments [24].

Table 1: Summary of attack detection and defense mechanisms.

Mechanisms	Advantages / Limitation
NDPMon	**Advantages:** Real-time monitoring; detects different NDP threats. **Limitation:** ▪ Keep track of any particular assaults, whether they include routers or neighbors. ▪ Efficient at avoiding problems. ▪ Not intelligent and lacks support.
Secure Neighbor Discovery (SEND)	**Advantages:** ▪ The protocol offers cryptographic protection for NDP messages, using Cryptographically Generated Addresses (CGA) to bind IPv6 addresses to public keys. ▪ It prevents replay attacks, supports certificate path validation, and secures message integrity and authenticity. ▪ It also prevents spoofing and address resolution. ▪ It enhances network communication trust, mitigates DoS attacks, and is interoperable with existing IPv6 infrastructure. ▪ It allows granular security policies for different types of NDP messages. **Limitation:** ▪ The cryptography and verification methods demand a large amount of CPU and memory. ▪ Changes to the present NDP (requiring new ICMPv6 messages). ▪ Manage trust anchors and keys at a cost. ▪ DoS attacks pose a hazard. ▪ Compatibility issues with popular operating systems.
Software Defined Networking (SDN)	**Advantages:** Centralized control and flexibility in executing security measures. **Limitation:** Single point of failure; Complex deployment and management
Cryptographically Generated Addresses (CGA)	**Advantages:** Prevents address spoofing and improves security by tying addresses to cryptographic keys. **Limitation:** Computational overhead; difficulty of key management
HMAC (Hash-based Message Authentication Code)	**Advantages**: Efficient; ensures message integrity and authenticity **Limitation**: Requires safe key distribution; restricted to symmetric key settings.
Trust-ND.	**Advantages:** Adaptive security depending on node activity; mitigates insider threats. **Limitation:** ▪ The NDP has been modified by default. ▪ Additional processing resources are required for implementation. ▪ Hash collision attacks are susceptible.
Digital signatures	**Advantages:** High level of security; checks message integrity and sender validity.

RUJCST
جامعة الرازي
Al-Razi University
كلية الحاسوب وتقنية المعلومات
ISSN-L 3007-5084
مجلة جامعة الرازي لعلوم الحاسوب وتقنية المعلومات
Al-Razi University Journal of Computer Science and Technology
علمية محكمة تصدر عن كلية الحاسوب وتقنية المعلومات - جامعة الرازي

	Limitation: High computational expense; requires public key infrastructure.
RA-Guard	**Advantages:** ▪ Improves network security by preventing illegal RA communications. ▪ Prevents RA spoofing, MITM, and DoS attacks. ▪ Compatible with the existing IPv6 infrastructure. ▪ Easily deployable on compatible network devices. **Limitation:** ▪ Only guard the network against malicious router advertisements. ▪ There are potential compatibility issues with RA-Guard, and not all Layer 2 devices (switches) support it. ▪ Evasion and denial-of-service attacks are feasible.
SDN-Based Authentication Mechanism	**Advantages:** Centralized control simplifies security policy management, enabling rapid response to threats. It's scalable, enhances visibility, improves security oversight, reduces manual intervention, and offers context-aware authentication, interoperability, rapid threat mitigation, and efficient network resource use. **Limitation:** ▪ There is a compatibility issue with OpenFlow for network devices. ▪ Destroy SDN's capacity to function as a network controller rather than a network security measure.
Blake2 Algorithm	**Advantages:** ▪ Excellent speed and efficiency. ▪ Strong security, resistant against known assaults. Flexibility with varied hash output sizes and keyed hashing. ▪ Low resource use, ideal for resource-constrained situations. ▪ Open source ensures openness and allows for wider inspection and adoption. ▪ Parallelizable, using multi-core computers to improve speed. **Limitation:** ▪ In comparison to SHA-2 and SHA-3.there has been less adoption and standardization. ▪ Configuration settings may increase the difficulty of implementation. Less optimal hardware support, which may compromise performance on some devices. ▪ Future vulnerabilities might possibly be uncovered. ▪ Integration issues with current NDP protection frameworks.
DH (Diffie-Hellman)	**Advantages:** Secure key exchange; resists eavesdropping. **Limitation:** Vulnerable to man-in-the-middle attacks if not verified. Computational overhead

II. NEIGHBOR DISCOVERY PROTOCOL (NDP)

A. Introduction to NDP:

NDP is an essential component of the IPv6 protocol architecture, performing a variety of important activities required to operate an IPv6 network. This protocol enables IPv6-enabled devices on a LAN to discover, identify, and communicate with nearby network nodes effectively to support basic IPv6 communication operations[25].

The IPv6 Neighbor Discovery Protocol (NDP) is vital for managing communication between devices on a LAN, but it is subject to a number of security threats, including Man-In-The-Middle (MITM) attacks, Denial of Service (DoS) attacks, and address spoofing attacks [26] .

These vulnerabilities are caused by unauthenticated and stateless NDP packets, especially during address resolution, which may compromise network confidentiality, integrity, and availability[25].While Secure Neighbor Discovery (SEND) and other proposed approaches seek to improve NDP security, complexity and resource requirements hinder wider use of the Neighbor Discovery protocol[25, 27].

RUJCST
جامعة الرازي
Al-Razi University
ISSN-L 3007-5084
كلية الحاسوب وتقنية المعلومات
مجلة جامعة الرازي لعلوم الحاسوب وتقنية المعلومات
Al-Razi University Journal of Computer Science and Technology
علمية محكمة تصدر عن كلية الحاسوب وتقنية المعلومات - جامعة الرازي

Recent research has focused on developing novel approaches to authenticating IPv6 hosts and preventing unauthorized access, such as the NDP security (NDPsec) mechanism based on digital signatures, demonstrating superior resilience against cyberattacks while reducing processing time and traffic overhead compared to existing solutions [10, 28, 29].

B. NDP Messages:

Neighbor Discovery Protocol (NDP) messages are important in LAN contexts because they make it easy to map IPv6 addresses to MAC addresses and find neighbors. However, installing NDP on public networks exposes users to major security threats such as address spoofing, denial of service, and man-in-the-middle attacks[25, 30].

Furthermore, transmission failures can have a significant influence on the efficacy of neighbor discovery methods, resulting in longer discovery durations and decreased efficiency[31].

Recent studies have emphasized the need of safeguarding NDP messages in LAN contexts. In this paragraph, we will detail the number of messages that perform NDP-related duties, as well as describe the purpose of each message. In IPv6, NDP makes use of ICMPv6 messages to let nodes locate their neighbors on the same LAN and announce their existence to others. The ICMPv6 messages are[25], as shown in figure 1[32]:

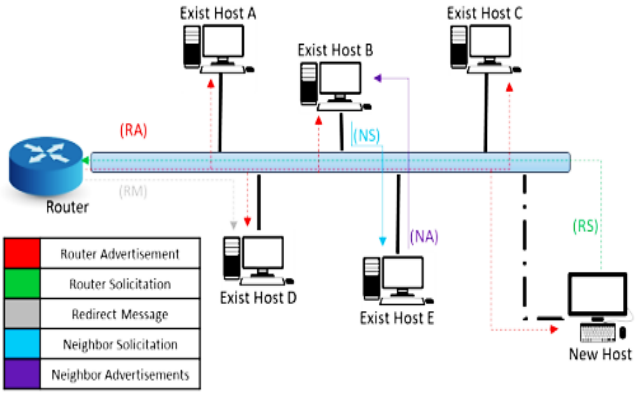


FIGURE 1. NDP five messages

1) Router Solicitation (RS) - Type 133: Hosts send Router Solicitation (RS) messages to detect routers on the same LAN and acquire router information. Routers emit Router Advertisement (RA) messages when they receive packets that are not meant for them, in order to void delaying the next planned timer announcement[33].
2) Router Advertisement (RA) – type 134: The router generates these messages, which are transmitted periodically or in response to router solicitation. Routers use RAs to announce their presence and provide specific features such as the MTU, router prefix, lifetime of each prefix, and hop limits[25, 33]
3) Neighbor Solicitation (NS) – type 135: Hosts send these messages to find the link-layer (MAC) addresses of other nodes on the same LAN or to check the reachability of surrounding nodes[25].
4) Neighbor Advertisement (NA) – type 136 : messages are issued to announce changes in the host MAC address and P address, or to request answers to NS messages[25].
5) Redirect (R) – type 137 : Routers can send redirect messages to one another in order to reroute user traffic[10].

C. NDP in IPv6 environment:

1) Router Discovery: NDP enables IPv6 nodes to find accessible routers on their local network segment[17, 34].
2) Prefix Discovery: NDP allows IPv6 nodes to find available address prefixes that may be used to configure IPv6 addresses on their local network[17, 34].
3) Parameter Discovery: NDP enables IPv6 nodes to learn about many parameters, such as the link MTU (Maximum Transmission Unit) and default hop limit[17, 34].
4) Address Resolution: NDP allows IPv6 nodes to map IPv6 addresses to link-layer (MAC) addresses, analogous to the Address Resolution Protocol (ARP) in Ipv4[17, 34].
5) Neighbor Unreachability Detection: NDP enables IPv6 nodes to detect when an adjacent node becomes inaccessible and take necessary steps, such as initiating a new address resolution process or choosing an alternative next-hop router[17, 34].
6) Duplicate Address Detection: NDP allows IPv6 nodes to ensure that the IPv6 address they are attempting to use is unique on the local network segment, hence avoiding address conflicts[17, 34].

III. ICMPv6 PROTOCOL

A. Introduction to ICMPV6:

As the globe moves closer to broad implementation of the next-generation internet protocol[35], IPv6, the importance of supporting protocols grows. The ICMPv6 is a critical component of IPv6 network communication [36, 37].

ICMPv6 is an important component of the IPv6 protocol suite[9], performing a variety of roles such as error reporting, diagnostic capabilities, and facilitating key IPv6 protocols such as the Neighbor Discovery Protocol (NDP)[25]. This protocol enhances the efficiency and dependability of a local area network (LAN) by enabling IPv6-capable devices to exchange control and informational messages[10].

ICMPv6 is used in LANs. [38]investigated the influences affecting IPv6 adoption and the corresponding ICMPv6 opinions on the influence. In addition, [39] analyzed the security imperative in IPv6, including ICMPv6, but overall we must improve the security of IPv6 networks.

As a result, the ICMPv6 protocol is used for ICMPv6. [40] Implementation of IPv6 in telecommunications

RUJCST
ISSN-L 3007-5084
جامعة الرازي
Al-Razi University
كلية الحاسوب وتقنية المعلومات
مجلة جامعة الرازي لعلوم الحاسوب وتقنية المعلومات
Al-Razi University Journal of Computer Science and Technology
علمية محكمة تصدر عن كلية الحاسوب وتقنية المعلومات - جامعة الرازي

networks, based on telecommunications standards. [41] Finally and on. Eight comprehensive edits on eight security technologies and a few in IPv6 networks, including advanced analysis of ICMPv6-related vulnerabilities and potential countermeasures.

B. ICMPv6 Messages:

The Internet Control Message Protocol version 6 (ICMPv6) is critical for operating and managing IPv6 networks[35]. ICMPv6, the successor to ICMP in IPv4, offers critical error reporting and diagnostic features required for the operation of local area networks (LANs) [42]. ICMPv6 messages are used in IPv6 LANs to provide critical network tasks such as neighbor discovery, path MTU discovery, and fault reporting[43].

Neighbor Discovery Protocol (NDP) messages such as Neighbor Solicitation and Neighbor Advertisement[44] allow hosts to discover neighboring nodes' link-layer addresses[27], whereas Path MTU Discovery (PMTUD) uses the Packet Too Big message to inform senders of the optimal packet size for a given path[45].

Furthermore, ICMPv6 error signals such as Destination Unreachable, Time Exceeded, and Parameter Problem give vital data to hosts and routers on delivery failures, TTL expirations, and header format errors [46]. Below are details of ICMPv6 error messages and information messages as required[47]:

1) ICMPV6 Error Messages:

- Destination Unreachable:

  This indicates that the target IPv6 address cannot be reached. This may be due to routing difficulties, administrative restrictions, or other connectivity issues. It includes a notification code that identifies the reason for the unavailability[47-49].

- Packet Too Big:

  Notifies the sender that the packet is too large to be sent over the route. This initiates Path MTU Discovery (PMTUD) to determine the appropriate MTU size[50]. The message specifies the MTU size that cannot be supported[47-49].

- Time Exceeded:

  The sender is notified that the packet's time to live (TTL) has been exceeded. This often indicates routing loops in the network or difficulties with forwarding. The message contains a code that indicates whether the TTL was exceeded during transfer or during reassembly of the parts[47-49].

- Parameter Problem:

  The sender is notified that there is a problem with the IPv6 packet header parameters[51]. This may include problems such as incorrect field values, absent options, or errors in header formatting. The notice contains a reference to the octet in the IPv6 header where the problem is identified.

2) ICMPV6 Information Messages:

- Echo Request and Echo Reply:

  Echo request messages, similar to ICMP ping in IPv4[52], are used for network diagnosis and troubleshooting. The recipient responds with an echo reply message, which helps verify the connection and measure the round trip time[53].

- Router Solicitation and Router Advertisement:

  Makes it easier to identify IPv6 routers on the local network. Router solicitation messages motivate routers to send router advertising messages. Router announcement messages provide information about accessible routers, prefixes, and other configuration characteristics[8].

- Neighbor Solicitation and Neighbor Advertisement:

  Neighbor Solicitation messages seek a target node's link-layer address, whereas Neighbor Advertisement messages offer it. [54].

IV. IPV6 NDP THREATS

Despite the fact that the NDP is often considered as the most important and critical protocol in IPv6, it lacks a proper security mechanism for checking and authenticating messages delivered between hosts linked across the same network. An attacker with network access can disrupt any of the NDP processes by changing the messages sent between hosts, as well as execute DoS and MITM assaults whenever they want [10, 25, 29].Cyberattacks against NDP services and processes pose a risk to network security:

A. **Neighbor Cache Exhaustion (NCE) attack**, the perpetrator inundates the neighbor cache of the targeted node with numerous fake Neighbor Solicitation (NS) and Neighbor Advertisement (NA) messages. As a consequence, the cache may become overwhelmed, displacing valid entries and causing address resolution issues as well as service interruptions[55].

RUJCST
جامعة الرازي
Al-Razi University
كلية الحاسوب وتقنية المعلومات
ISSN-L 3007-5084
مجلة جامعة الرازي لعلوم الحاسوب وتقنية المعلومات
Al-Razi University Journal of Computer Science and Technology
علمية محكمة تصدر عن كلية الحاسوب وتقنية المعلومات - جامعة الرازي

- **Mechanism of NDP:** The proper functioning of IPv6 relies on the NDP, which plays a crucial role in tasks like address resolution, neighbor discovery, and router discovery. Additionally, it is responsible for managing a neighbor cache that stores relevant information about reachable neighbors[34].
- **Attack Description**: NCE attack involves flooding the victim with a large number of NS packets. These messages instruct the target to resolve multiple IPv6 addresses to the associated link-layer addresses. As the target executes these requests, its neighbor cache fills up with entries, using memory and CPU resources[25].
- **Impact of NCE Attacks:**
  1) Denial of Service (DoS) occurs when a device's neighbor cache reaches its maximum capacity, disrupting network operations and causing communication failures.
  2) Resource exhaustion occurs when attacks exhaust system resources, leading to performance decline and potential system crashes.
  3) Network instability is caused by continuous NCE attacks[56]
- **Mitigation Strategies:**
  1) Rate Limitation: Enforcing rate limits on NDP messages is crucial in avoiding cache depletion by restricting the quantity of NS messages handled in a specific time period[57].
  2) Advanced Neighbor Discovery (AND): Utilizing AND strategies can enhance the effectiveness of neighbor cache administration, guaranteeing that the cache remains manageable[58].
  3) Surveillance and Notifications: Consistent monitoring of NDP traffic and establishment of notifications for abnormal behavior can assist in promptly identifying and addressing NCE assaults[9].
  4) Allocation of Resources: Assigning ample resources for the neighbor cache and utilizing flexible cache sizing can enable the absorption of sudden spikes in NDP traffic without depleting resources[59]

B. **Neighbor Unreachability Detection (NUD) spoofing attacks,** NUD spoofing attacks take advantage of procedures used by IPv6 nodes to evaluate the reachability of surrounding nodes. Here's a thorough analysis of NUD spoofing attacks and their consequences[60]:

- **Mechanism of NUD**: The NUD Mechanism is an essential component of the Neighbor Discovery Protocol (NDP) in IPv6, allowing communication with nearby nodes. When a node transmits a packet to a neighbor, it expects a reply[61]. If no answer is received, NUD processes are initiated to determine if the neighbor is still accessible[54].
- **Attack Description**: In a NUD spoofing attack, an assailant dispatches counterfeit NUD messages to deceive a node into believing that its neighboring node is unreachable. This is accomplished by transmitting fabricated Neighbor Solicitation (NS) or Neighbor Advertisement (NA) messages containing inaccurate information. Consequently, the targeted node may erroneously designate the neighbor as unreachable, leading to communication disruptions[54].
- **Impact of NUD Spoofing Attacks**:
  1) Communication Disruptions: Legitimate nodes could cease transmitting packets to the seemingly unreachable node, leading to interruptions in communication.
  2) Growing Latency: The node might make another attempt to resolve the address, causing delays in communication.
  3) Man-in-the-Middle (MITM) Intrusion: Malicious actors can infiltrate communication by rerouting it through unauthorized nodes, leading to MITM attacks.
  4) Service Denial (DoS): Hackers could flood network resources with numerous address resolutions and verifications, leading to a denial of service**[54, 61]**.
- **Mitigation Strategies**:
  1) Implementing Secure NDP (SEND) can provide cryptographic security to NDP messages, ensuring their authenticity and integrity[28].
  2) Using RA Guard efficiently blocks malicious RA communications, reducing the likelihood of NUD spoofing[62].
  3) Consistently monitoring NDP traffic and establishing alarms for unexpected trends can help detect spoofing efforts quickly[63].
  4) Increasing security by network segmentation might reduce vulnerability to NDP message assaults[62]

RUJCST
جامعة الرازي
Al-Razi University
كلية الحاسوب وتقنية المعلومات
ISSN-L 3007-5084
مجلة جامعة الرازي لعلوم الحاسوب وتقنية المعلومات
Al-Razi University Journal of Computer Science and Technology
علمية محكمة تصدر عن كلية الحاسوب وتقنية المعلومات - جامعة الرازي

C. **Router Advertisement (RA) spoofing attacks**, where an attacker impersonates a legitimate router and sends malicious RA messages. These messages can be used to redirect traffic, perform man-in-the-middle attacks, or enable unauthorized access to network resources[8]:

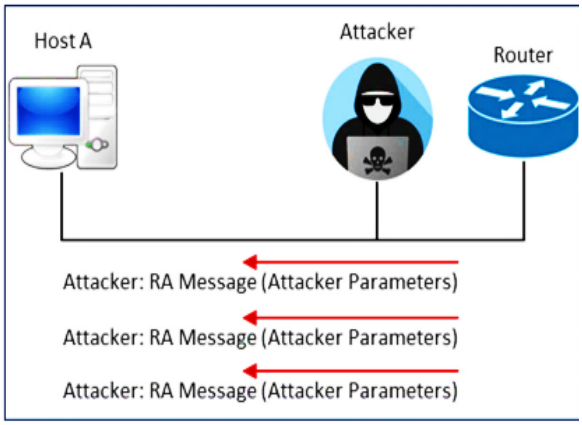
- **Mechanism of RA:** IPv6 routers send out RA messages on a regular basis to announce their availability and share network information such as prefixes, hop limits, and MTU sizes. This information allows nodes to automatically configure their IPv6 addresses and network settings[64].
- **Attack Description:** An RA spoofing attack occurs when an attacker sends fake RA messages. These messages include incorrect network settings or misleading details in the network topology. It helps the attacker by:
  1. It takes on the role of the master router and diverts traffic through itself.
  2. Enters incorrect prefixes, causing address configuration problems.
  3. Reduces the hop limit, resulting in packet loss.
  4. It breaks the connection by adopting non-existent routers or providing wrong details of a spoofed network. as shown in figure 2[10].
  5. 

FIGURE 2. RA flooding attack

- **Impact of RA Spoofing Attacks:**
  1) Attackers have the ability to redirect traffic using a malicious router, enabling them to intercept and potentially alter the traffic, resulting in Man-in-the-Middle (MITM) attacks.
  2) Network misconfigurations and loss of connectivity can occur due to incorrect RA messages, resulting in Denial of Service (DoS) and service disruption.
  3) The instability of the network can be caused by frequent changes in advertised parameters, leading to degraded network performance[44].
- **Mitigation Strategies:**
  1) SEND employs cryptographic mechanisms to validate the source of NDP messages such as RAs, ensuring their legality and security[64].
  2) RA Guard function eliminates illegitimate RA communications, ensuring that only valid ones are handled[65].
  3) Router Advertisement Protection: RAP detects and prevents RA spoofing by monitoring and verifying transmissions[66].
  4) Consistent monitoring and alarms allow for faster reaction to RA spoofing assaults[67]

D. **Neighbor Solicitation / Advertisement Spoofing,** Neighbor Solicitation (NS) and Neighbor Advertisement (NA) spoofing attacks take advantage of weaknesses in the Neighbor Discovery Protocol (NDP) of IPv6 in order to generate inaccurate network mappings and interfere with network communication. Below is an in-depth examination of the methods used in these attacks, the consequences they can have, and the approaches that can be taken to prevent them[10]:

- **Mechanism of Neighbor Solicitation / Advertisement Spoofing:**
  1) Neighbor Solicitation (NS) Spoofing: Malicious persons use spoofing Neighbor Solicitation (NS) to send counterfeit signals to a target, requesting a specific IPv6 address at the link-layer level. In reaction, the victim unintentionally publishes its MAC address, which the attacker can use for malicious purposes[68].
  2) Spoofing Neighbor Advertisement (NA): Adversaries send bogus NA signals to a target, claiming that an IPv6 address corresponds to a certain MAC address. This misled the victim into sending packets to the wrong or malicious device[68].
- **Impact of Neighbor Solicitation/Advertisement Spoofing:**
  1) Traffic Redirection: By modifying IP-to-MAC address mappings, attackers can divert traffic meant for a legal node to themselves, allowing man-in-the-middle attacks[29].
  2) Denial of Service (DoS): If legitimate nodes' IP-to-MAC address mappings are corrupted, a denial of service occurs[8].
  3) Network Disruption: Incorrect mappings can create extensive network disruption because nodes attempt to interact with the incorrect devices[35].
- **Mitigation Strategies:**
  1) Secure Neighbor Discovery: SEND protects NDP communications using Cryptographically Generated Addresses (CGA) and RSA signatures, assuring their authenticity and integrity [69].

RUJCST
جامعة الرازي
Al-Razi University
ISSN-L 3007-5084
كلية الحاسوب وتقنية المعلومات
مجلة جامعة الرازي لعلوم الحاسوب وتقنية المعلومات
Al-Razi University Journal of Computer Science and Technology
علمية محكمة تصدر عن كلية الحاسوب وتقنية المعلومات - جامعة الرازي

2) RA Guard may detect illegal or harmful RA transmissions, lowering the danger of RA spoofing. While primarily intended for RAs, similar filtering algorithms may be used on NS and NA signals[70].
3) Monitoring and Alerts: Using comprehensive network monitoring to detect unexpected patterns or spikes in NDP traffic might assist discover spoofing efforts early on[54].

E. Duplicate Address Detection (DAD) DoS Attacks, Duplicate Address Detection (DAD) is a vital IPv6 mechanism that ensures no two devices on the same network share the same IP address. However, this method may be used to launch a Denial of Service (DoS) assault[23]. Here's a detailed look at how DAD DoS assaults operate, their impact, and how they may be avoided[71].

- **Mechanism of DAD:** When an IPv6 node is set to use a new IPv6 address, it initiates DAD by sending a Neighbor Solicitation (NS) message to the network to see [13]if the requested IP address is already in use[72]. If no Neighbor Advertisement (NA) message is received in response[13], the node considers the address to be unique and assigns it to itself[2].

- **Attack Description:** In a DAD DoS attack, an attacker takes advantage of the DAD mechanism by replying to each NS message with a bogus NA response, suggesting that the requested address is already in use[10]. This inhibits valid devices from correctly setting their IPv6 addresses, causing a denial of service. as shown in figure 3 [54].

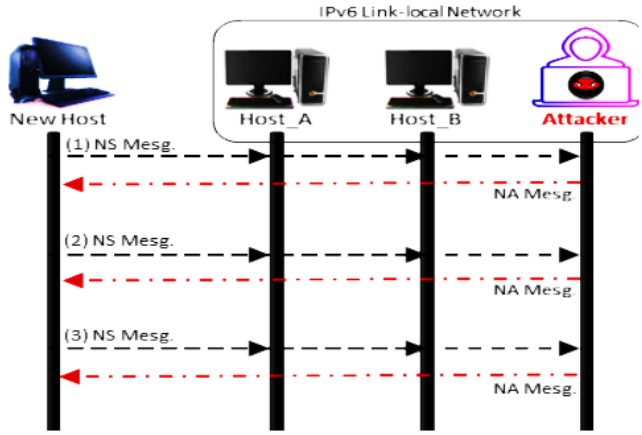


FIGURE 3. DoS-on-DAD attack.

- **Impact of DAD DoS Attacks:**

1) Address Configuration Failure: Legitimate devices cannot receive unique IPv6 addresses, resulting in network connectivity difficulties.
2) Denial of Service (DoS): Failures in persistent address setup can cause substantial disruptions to network services, impacting both client and server operations.
3) Network Instability: Frequent DAD DoS assaults can create significant disruption as devices repeatedly try and fail to set addresses[62].

- **Mitigation Strategies:**

1) Secure Neighbor Discovery: SEND can assist verify NDP communications, allowing only valid devices to participate in the DAD process[10].
2) Implementing rate: restrictions on NDP messages can help to mitigate the impact of Duplicate Address Detection Denial of Service attacks by restricting the amount of NS messages that can be processed in a given time frame.
3) RA Guard: Though designed primarily for router ads, technologies similar to RA Guard may be used to filter and validate NS and NA messages, preventing attackers from sending faked answers[15].
4) Monitoring and Alerts: By continuously monitoring NDP traffic and putting up notifications for unusual activity, DAD DoS assaults may be detected and mitigated early on[54].

F. Address Resolution (AR) DoS Attacks,Address Resolution DoS attacks leverage weaknesses in IPv6's NDP to disrupt the mapping of IP addresses to MAC addresses, causing network disruption and denial of service[73]. Here's a comprehensive review of these assaults, their impact, and mitigating strategies:

- **Mechanism:** In IPv6, NDP is utilized for address resolution instead of ARP, as in IPv4. The NDP comprises messages like Neighbor Solicitation and Neighbor Advertisement for locating and resolving link-layer addresses. An AR DoS attack entails delivering a flood of NS or NA messages to a target in order to deplete its neighbor cache or establish inaccurate IP-to-MAC addresses[20, 73].

- **Attack Description:**

1) Flooding occurs when an attacker sends a high number of bogus NS messages, forcing the victim to complete multiple address resolution queries. This may overflow the target's neighbor cache, resulting in resource exhaustion[25].
2) Spoofing is when an attacker sends fake NA messages that associate wrong MAC addresses with genuine IP addresses. This causes the target to transmit packets to the wrong location, interrupting regular connection[32]. as shown in figure 4[54].

RUJCST
جامعة الرازي
Al-Razi University
كلية الحاسوب وتقنية المعلومات
ISSN-L 3007-5084
مجلة جامعة الرازي لعلوم الحاسوب وتقنية المعلومات
Al-Razi University Journal of Computer Science and Technology
علمية محكمة تصدر عن كلية الحاسوب وتقنية المعلومات - جامعة الرازي

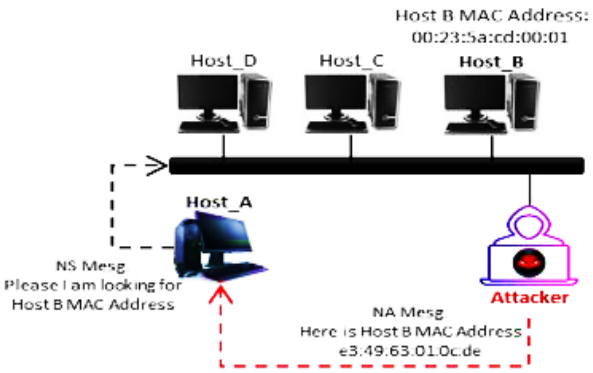


FIGURE 4. DoS-on-AR process

- **Impact of AR DoS Attacks:**

1) Denial of Service (DoS) happens when the target's neighbor cache reaches its capacity, preventing it from resolving new addresses and leading to communication breakdowns.
2) Network Outage: Valid traffic is either redirected incorrectly or disappears, leading to major disruptions in network operations.
3) Resource Exhaustion: The ongoing handling of fake messages drains the CPU and memory resources, which could lead to system crashes or decreased performance**[20, 73].**

- **Mitigation Strategies:**

1) Secure Neighbor Discovery (SEND):
   - SEND secures NDP communications with Cryptographically Generated Addresses (CGA) and RSA signatures.
   - Effectiveness: Prevents spoofing attacks by determining the origin of NDP packets [69].
2) Rate Limiting:
   - Description: Setting rate restrictions on NDP messages minimizes the number of NS and NA messages[25] handled in a given timeframe.
   - Effectiveness: Reduces the severity of flooding assaults by restricting the amount of harmful messages[70] .
3) RA Guard and Similar Mechanisms:
   - RA Guard prevents illegal or harmful NDP communications, including NS and NA messages.
   - Effectiveness: Prevents the introduction of counterfeit NDP messages into the network [70].
4) Monitoring and Alerts:
   - Implementing strong network monitoring to detect unexpected patterns or spikes in NDP traffic can assist detect AR DoS assaults early on.
   - Effectiveness: Allows for proactive actions to reduce assaults before they do serious damage [54].

The following table 2 shows a summary of the security threats and security solutions for IPv6 NDP.

Table 2: Summary of security threats and security solutions for IPv6 NDP

Security threat	Mechanism	Impact	Solutions
NCE	Fake NS/NA messages	Memory exhaustion, services interruption	Determine message rates, AND, monitor, allocate resources
NUD	Fake NS/NA messages	Disconnection, delay, MITM	SEND, RA Guard, Monitoring, Network Segmentation
RA	Fake RA messages	Normally routed traffic, loss of connection	SEND, RA Guard, Ad Protection, Monitoring
NS/NA	Fake NS/NA messages	Traffic redirection, interruption of services	SEND, RA Guard, continuous monitoring
DAD DoS	Fake NA replies	Failed to configure address, interruption of services	SEND, Message Rate Limiting, RA Guard, Continuous Monitoring
AR DoS	Fake NS/NA messages	Interruption of services, exhaustion of resources	SEND, Message Rate Limiting, RA Guard, Continuous Monitoring

V. TECHNICAL TERMINOLOGY

- **Blake2 Algorithm:** The Blake2 algorithm is a cryptographic hash function used in applications that require great performance and security[9, 16-19].
- **SDN (Software Defined Networks):** SDN is a new and superior network design to traditional network architecture in terms of regulating network traffic flows, as well as the elasticity and flexibility to be programmed for effective network administration.
- **Router Advertisement Guard (RA-Guard)** is a method that blocks illegal Router Advertisement (RA) packets on a network, hence avoiding possible attacks that take use of the RA capability of the Neighbor Discovery Protocol (NDP) in IPv6[15].
- **NDPMon** is a network monitoring tool for tracking and analyzing the IPv6 Neighbor Discovery Protocol (NDP). It aids in the detection and alerting of network managers to

RUJCST
جامعة الرازي
Al-Razi University
ISSN-L 3007-5084
كلية الحاسوب وتقنية المعلومات
مجلة جامعة الرازي لعلوم الحاسوب وتقنية المعلومات
Al-Razi University Journal of Computer Science and Technology
علمية محكمة تصدر عن كلية الحاسوب وتقنية المعلومات - جامعة الرازي

aberrant activity and possible NDP assaults, hence improving IPv6 network security[12-15].

- **Trust-ND** is a security enhancement to IPv6's Neighbor Discovery Protocol (NDP) that improves the protocol's trustworthiness. It includes procedures for authenticating NDP messages, guaranteeing that they originate from valid sources and have not been tampered with. Trust-ND tries to mitigate a variety of NDP threats, including spoofing and denial-of-service[14, 15, 20].
- **Cryptographically Generated Addresses (CGA)** bind IP addresses to a public key using cryptography. This binding ensures the validity of the address and prevents address spoofing. CGA is an essential component of the Secure Neighbor Discovery (SEND) protocol, which improves security for IPv6 address setup and Neighbor Discovery procedures.

VI. CONCLUSIONS

IPv6, being the next-generation protocol, offers several benefits that many have yet to understand. However, like a novel protocol, it has security vulnerabilities in addition to its benefits. and there are several NDP-related attacks, including Neighbor Cache Exhaustion (NCE) attacks, Neighbor Unreachability Detection (NUD) spoofing attacks, Router Advertisement (RA) spoofing attacks, Duplicate Address Detection DoS attacks, and Address Resolution DoS attacks. It then presents the mitigation strategies for each of these attacks, such as rate limitation, advanced neighbor discovery techniques, RA Guard, and secure neighbor discovery protocols. The most important protocol is the ICMPv6 that is used by NDP to discover router, network prefix, neighbors and also network parameters.

ACKNOWLEDGMENT

As part of the research community, we would like to extend my deep thanks to Al-Razi University for its continued support of scientific research. we also extend my sincere thanks to the anonymous reviewers who devoted their time and efforts to reviewing our research very carefully. Their valuable contributions have helped improve the quality of our research work and enhance our contributions to scientific knowledge. We again thank Al-Razi University for their continued support in the success and dissemination of scientific research.

REFERENCES

1. Ashraf, Z., et al., *Challenges and Mitigation Strategies for Transition from IPv4 Network to Virtualized Next-Generation IPv6 Network.* Int. Arab J. Inf. Technol., 2023. **20**(1): p. 78-91.
2. Song, G., et al., *: A Fast, Efficient, and Comprehensive Global Active IPv6 Address Detection System.* IEEE/ACM Transactions on Networking, 2024.
3. Al-Azzawi, A. and G. Lencse, *Analysis of the Security Challenges Facing the DS-Lite IPv6 Transition Technology.* Electronics, 2023. **12**(10): p. 2335.
4. Dahabiyeh, L., *Factors affecting organizational adoption and acceptance of computer-based security awareness training tools.* Information & Computer Security, 2021. **29**(5): p. 836-849.
5. Igulu, K., F. Onuodu, and T.P. Singh, *IPV6: Strengths and Limitations*, in *Communication Technologies and Security Challenges in IoT: Present and Future*. 2024, Springer. p. 147-172.
6. Kumar, A., A. Prasad, and T.P. Singh, *Communication Technologies and Security Challenges in IoT: An Introduction*, in *Communication Technologies and Security Challenges in IoT: Present and Future*. 2024, Springer. p. 1-20.
7. Isizoh, A., O. Okechukwu, and A. Ani, *ANALYSES OF THE MIGRATION TO INTERNET PROTOCOL VERSION SIX (IPv6).* International Journal of Computing, Science and New Technologies (IJCSNT), 2024. **2**(1): p. 11-23.
8. Hasan, A.H., M. Anbar, and T.A. Alamiedy, *Deep learning approach for detecting router advertisement flooding-based DDoS attacks.* Journal of Ambient Intelligence and Humanized Computing, 2023. **14**(6): p. 7281-7295.
9. Hamarsheh, A., *An Adaptive Security Framework for Internet of Things Networks Leveraging SDN and Machine Learning.* Applied Sciences, 2024. **14**(11): p. 4530.
10. Al-Ani, A., et al., *NDPsec: Neighbor Discovery Protocol Security Mechanism.* IEEE Access, 2022. **10**: p. 83650-83663.
11. Puhl, Z.T. and J. Guo, *Securing IPv6 Neighbor Discovery Address Resolution with Voucher-Based Addressing.* 2024.
12. Song, G., J. Hu, and H. Wang, *An Anti-DoS Duplicate Address Detection Model.* Engineering Letters, 2022. **30**(2).
13. Seth, A.D., S. Biswas, and A.K. Dhar, *DADCNF: Diagnoser design for duplicate address detection threat using conjunctive Normal form.* Computer Networks, 2023. **222**: p. 109539.
14. Al-Shareeda, M.A., et al. *IPv6 Link-Local Network SLAAC Attack Detection Mechanisms: A Review*. in *2022 Fifth College of Science International Conference of Recent Trends in Information Technology (CSCTIT)*. 2022. IEEE.
15. Shah, J.L. and H.F. Bhat, *Towards a secure IPv6 autoconfiguration.* Information Security Journal: A Global Perspective, 2020. **29**(1): p. 14-29.
16. Abdullah, S.A. and A.A. Al Ashoor, *Ipv6 security issues: A systematic review following prisma guidelines.* Baghdad Science Journal, 2022. **19**(6 (Suppl.)): p. 1430-1430.

RUJCST
جامعة الرازي
Al-Razi University
كلية الحاسوب وتقنية المعلومات
ISSN-L 3007-5084
مجلة جامعة الرازي لعلوم الحاسوب وتقنية المعلومات
Al-Razi University Journal of Computer Science and Technology
علمية محكمة تصدر عن كلية الحاسوب وتقنية المعلومات - جامعة الرازي

17. Machana, J.R. and G. Narsimha, *Optimization of ipv6 neighbor discovery protocol.* Journal of Interconnection Networks, 2022. **22**(Supp01): p. 2141025.
18. Park, W.-S. and C.-S. Park, *Securing 6LoWPAN neighbor discovery.* IEEE Internet of Things Journal, 2021. **8**(17): p. 13677-13689.
19. Talukder, M.S.H., et al. *An enhanced method for encrypting image and text data simultaneously using AES algorithm and LSB-based steganography*. in *2022 International Conference on Advancement in Electrical and Electronic Engineering (ICAEEE)*. 2022. IEEE.
20. Assotally, N.A. *Review of IPv6 Mitigation Techniques for Enterprise Local Area Networks*. in *2023 International Conference on Engineering and Emerging Technologies (ICEET)*. 2023. IEEE.
21. Ubiedo, L., et al., *Current state of IPv6 security in IoT.* arXiv preprint arXiv:2105.02710, 2021.
22. Luo, B., et al., *Neighbor discovery for IPv6 over BLE mesh networks.* Applied Sciences, 2020. **10**(5): p. 1844.
23. El Ghazouani, M., et al., *A Blockchain-based Method Ensuring Integrity of Shared Data in a Distributed-Control Intersection Network.* International Journal of Advanced Computer Science and Applications, 2023. **14**(10).
24. Kumar, R. and N. Agrawal, *Software defined networks (SDNs) for environmental surveillance: A Survey.* Multimedia Tools and Applications, 2024. **83**(4): p. 11323-11365.
25. Najjar, F., Q. Bsoul, and H. Al-Refai, *An Analysis of Neighbor Discovery Protocol Attacks.* Computers, 2023. **12**(6): p. 125.
26. Han, Y., et al., *Research on the Security of IPv6 Communication Based on Petri Net under IoT.* Sensors, 2023. **23**(11): p. 5192.
27. Pragya, B. Kumar, and G. Kumar, *Optimized Duplicate Address Detection for the Prevention of Denial-of-Service Attacks in IPv6 Network.* IETE Journal of Research, 2024: p. 1-26.
28. Usman, M., et al. *Enhance Neighbor Discovery Protocol Security by Using Secure Hash Algorithm*. in *2021 International Conference on Innovative Computing (ICIC)*. 2021. IEEE.
29. Zhang, L., et al. *Petri Net Model of MITM Attack Based on NDP Protocol*. in *International Conference on Networking and Network Applications (NaNA)*. 2022. IEEE.
30. Al-Sadhan, A.A., *Detecting Distributed Denial of Service Attacks in IPV6 by Using Artificial Intelligence Techniques*. 2020: Liverpool John Moores University (United Kingdom).
31. Moreira, D., K. Wagemann, and S. Céspedes. *IPv6 Neighbor Discovery for Vehicular Networks*. in *VII Taller del Grupo de Trabajo de Ingeniería de Internet/Argentina (IETF Day 2021)-JAIIO 50 (Modalidad virtual)*. 2021.
32. Amlak, G.M.H., F.Q. Kamal, and A.K. Al-Ani, *Denial of Service Attack on Neighbor Discovery Protocol Processes in the Network of IPv6 Link-Local.* International Journal of Electrical and Electronic Engineering & Telecommunications, 2020. **9**(4): p. 247-251.
33. Al-Shareeda, M.A., et al., *Proposed security mechanism for preventing fake router advertisement attack in IPv6 link-local network.* Indones. J. Electr. Eng. Comput. Sci, 2023. **29**: p. 518-526.
34. Liu, R., et al., *Addressless: enhancing IoT server security using IPv6.* IEEE Access, 2020. **8**: p. 90294-90315.
35. Saad, R.M., et al., *Neighbor discovery protocol anomaly-based detection system using neural network algorithm.* International Journal of Information Security, 2024: p. 1-17.
36. Elejla, O.E., et al., *Deep-learning-based approach to detect ICMPv6 flooding DDoS attacks on IPv6 networks.* Applied Sciences, 2022. **12**(12): p. 6150.
37. Kenyon, A., L. Deka, and D. Elizondo, *Are public intrusion datasets fit for purpose characterising the state of the art in intrusion event datasets.* Computers & Security, 2020. **99**: p. 102022.
38. Nayak, P.K., & Jha, R. K. , *Factors influencing the adoption of IPv6 in organizations.* International Journal of Communication Systems, 2023. **36**(5): p. e4973.
39. Shan, Z., Wang, W., Lyu, J., & Yang, Y., *Security analysis and enhancement mechanisms for IPv6 protocol.* Computers & Electrical Engineering, 2021. **93**: p. 107258.
40. Zhao, L., Wang, X., & Li, Y., *Challenges and solutions for IPv6 deployment in enterprise networks.* IEEE Transactions on Network and Service Management, 2024. **21**(2): p. 123-138.
41. Ranjbar, A., Hosseini, S. M., & Sadeghiyan, B., *A comprehensive survey on ICMPv6 security threats and mitigation techniques.* IEEE Communications Surveys & Tutorials, 2021. **23**(2): p. 1144-1175.
42. Shen, Y., & Zhang, J., *Mitigating ICMPv6 Error Message Attacks in IPv6 Networks.* IEEE Transactions on Network and Service Management, 2022. **19**(3): p. 2234-2247.
43. Cheng, Y., Jiang, F., & Guo, X, *Optimizing Path MTU Discovery in IPv6 Networks.* IEEE Access, 2020. **8**: p. 54494-54505.
44. Nixon, J.S. and M. Amenu, *Investigating security issues and preventive mechanisms in IPv6 deployment.* Int. J, 2022. **2**: p. 1-20.
45. Prasad, P., T. Mohammad, and P. Sainio, *Enhancing Security in Software-Defined Networking (SDN)*

RUJCST
جامعة الرازي
Al-Razi University
كلية الحاسوب وتقنية المعلومات
ISSN-L 3007-5084
مجلة جامعة الرازي لعلوم الحاسوب وتقنية المعلومات
Al-Razi University Journal of Computer Science and Technology
علمية محكمة تصدر عن كلية الحاسوب وتقنية المعلومات - جامعة الرازي

based IP Multicast Systems: Challenges and Opportunities. 2024.

46. Shen, Y., & Zhang, J., *Mitigating ICMPv6 Error Message Attacks in IPv6 Networks.* IEEE Transactions on Network and Service Management, 2022. **19**(3): p. 2234-2247.
47. Alghuraibawi, A.H.B., et al., *Detection of ICMPv6-based DDoS attacks using anomaly based intrusion detection system: A comprehensive review.* International Journal of Electrical and Computer Engineering, 2021. **11**(6): p. 5216.
48. Bdair, A.H., et al. *Brief of intrusion detection systems in detecting ICMPv6 attacks*. in *Computational Science and Technology: 6th ICCST 2019, Kota Kinabalu, Malaysia, 29-30 August 2019*. 2020. Springer.
49. Manickam, S., et al., *Labelled Dataset on Distributed Denial-of-Service (DDoS) Attacks Based on Internet Control Message Protocol Version 6 (ICMPv6).* Wireless Communications and Mobile Computing, 2022. **2022**(1): p. 8060333.
50. Hussain, I. and J. Bashir, *Dynamic MTU: A smaller path MTU size technique to reduce packet drops in IPv6.* Journal of King Saud University-Computer and Information Sciences, 2022. **34**(9): p. 7070-7088.
51. Rahouma, K.H., M.S. Abdul-Karim, and K.S. Nasr. *TCP/IP network layers and their protocols (A Survey)*. in *Internet of Things—Applications and Future: Proceedings of ITAF 2019*. 2020. Springer.
52. Yaibuates, M. and R. Chaisricharoen. *A combination of ICMP and ARP for DHCP malicious attack identification*. in *2020 Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunications Engineering (ECTI DAMT & NCON)*. 2020. IEEE.
53. Feng, X., et al. *{Off-Path} Network Traffic Manipulation via Revitalized {ICMP} Redirect Attacks*. in *31st USENIX Security Symposium (USENIX Security 22)*. 2022.
54. Al-Ani, A.K., et al., *Match-prevention technique against denial-of-service attack on address resolution and duplicate address detection processes in IPv6 link-local network.* IEEE Access, 2020. **8**: p. 27122-27138.
55. Bahashwan, A.A., et al., *Flow-based approach to detect abnormal behavior in neighbor discovery protocol (NDP).* IEEE Access, 2021. **9**: p. 45512-45526.
56. Fereidouni, H., O. Fadeitcheva, and M. Zalai, *IoT and Man-in-the-Middle Attacks.* arXiv preprint arXiv:2308.02479, 2023.
57. Nowak, P., *Aggregation & Analysis of IPv6 Prefixes at Internet-Scale*. 2024, Technische Universität Wien.
58. Garzón, C., et al., *P4 Cybersecurity Solutions: Taxonomy and Open Challenges.* IEEE Access, 2023.
59. Varma, I.M. and N. Kumar, *A comprehensive survey on SDN and blockchain-based secure vehicular networks.* Vehicular Communications, 2023: p. 100663.
60. Al-Shareeda, M.A., et al., *Sadetection: Security mechanisms to detect slaac attack in ipv6 link-local network.* Informatica, 2023. **46**(9).
61. Boufenneche, Y., et al., *Selfishness in secure internet of things networks: 6TiSCH case study.* Wireless Networks, 2021. **27**(6): p. 3927-3946.
62. Kumar, G. and Pragya, *IPv6 addressing with hidden duplicate address detection to mitigate denial of service attacks in the internet of drone.* Concurrency and Computation: Practice and Experience, 2024: p. e8131.
63. Tajdini, M. and H. Kolivand, *IPv6 Common Security Vulnerabilities and Tools: Overview of IPv6 with Respect to Online Games.* Encyclopedia of Computer Graphics and Games, 2024: p. 1008-1019.
64. Mönnich, M., et al. *Mitigation of IPv6 Router Spoofing Attacks with P4*. in *Proceedings of the Symposium on Architectures for Networking and Communications Systems*. 2021.
65. Bouyeddou, B., et al., *Detecting network cyber-attacks using an integrated statistical approach.* Cluster Computing, 2021. **24**: p. 1435-1453.
66. Fonseca, O., et al., *Identifying networks vulnerable to IP spoofing.* IEEE Transactions on Network and Service Management, 2021. **18**(3): p. 3170-3183.
67. Rani, P., S. Singh, and K. Singh, *Cloud computing security: a taxonomy, threat detection and mitigation techniques.* International Journal of Computers and Applications, 2024. **46**(5): p. 348-361.
68. Bahashwan, A.A., M. Anbar, and S.M. Hanshi. *Overview of IPv6 based DDoS and DoS attacks detection mechanisms*. in *Advances in Cyber Security: First International Conference, ACeS 2019, Penang, Malaysia, July 30–August 1, 2019, Revised Selected Papers 1*. 2020. Springer.
69. Jacome, C., et al., *A more secure IPv6 neighborhood process.* arXiv preprint arXiv:2004.14993, 2020.
70. Arjuman, N.C., S. Manickam, and S. Karuppayah. *An improved secure router discovery mechanism to prevent fake ra attack in link local IPv6 network*. in *International Conference on Advances in Cyber Security*. 2021. Springer.
71. Kumar, B. *Duplicate Address Detection: Significance, Attacks and its Solutions*. in *4th International Conference on Advances in*

RUJCST
جامعة الرازي
Al-Razi University
كلية الحاسوب وتقنية المعلومات
ISSN-L 3007-5084
مجلة جامعة الرازي لعلوم الحاسوب وتقنية المعلومات
Al-Razi University Journal of Computer Science and Technology
علمية محكمة تصدر عن كلية الحاسوب وتقنية المعلومات - جامعة الرازي

Computing, Communication Control and Networking (ICAC3N). 2022. IEEE.

72. Li, X., et al. *Fast IPv6 network periphery discovery and security implications*. in *2021 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. 2021. IEEE.

73. Jamil, F., H. Jamil, and A. Ali, *Spoofing Attack Mitigation in Address Resolution Protocol (ARP) and DDoS in Software-Defined Networking.* 2022.

RUJCST
جامعة الرازي
Al-Razi University
كلية الحاسوب وتقنية المعلومات
ISSN-L 3007-5084
مجلة جامعة الرازي لعلوم الحاسوب وتقنية المعلومات
Al-Razi University Journal of Computer Science and Technology
علمية محكمة تصدر عن كلية الحاسوب وتقنية المعلومات - جامعة الرازي

استبيان: تأمين بروتوكول اكتشاف الجيران في IPv6

محمد غالب م. عقيل
كلية علوم الحاسوب وتكنولوجيا المعلومات
قسم تقنية المعلومات – جامعة الرازي
صنعاء، اليمن
MohammedAqeel014@gmail.com

يوسف ع. عبدالمغني
كلية علوم الحاسوب وتكنولوجيا المعلومات
قسم تقنية المعلومات – جامعة الرازي
صنعاء، اليمن
Youssef.almoghni@gmail.com

يحيى الأشموري
كلية علوم الحاسوب وتكنولوجيا المعلومات
قسم تقنية المعلومات – جامعة الرازي
قسم الرياضيات والحاسوب – كلية العلوم، جامعة صنعاء
صنعاء، اليمن
Yah.AlAshmoery@su.edu.ye

الملخص

بروتوكول اكتشاف الجيران (NDP) في IPv6 ضروري لتسهيل التواصل بين عقد الشبكة المحلية. ومع ذلك، فإن NDP معرض لهجمات مختلفة يمكن أن تعطل التواصل في الشبكة وتسهّل الأنشطة الخبيثة. تحاول هذه الدراسة تحديد الثغرات الأمنية الرئيسية في NDP وتقييم الطرق المتاحة لتحسين أمانه. أجرينا مراجعة منهجية للأدبيات لتحليل الفوائد والقيود للآليات مثل العناوين المولدة تشفيرياً (CGA)، اكتشاف الجيران الآمن (SEND)، واكتشاف الجيران المعتمد على الشهادات. تُظهر نتائجنا أن هذه الآليات تقلل بشكل كبير من تأثير هجمات اكتشاف الجيران. نوصي بآلية لاكتشاف الهجمات لمعالجة تزوير رسائل استعلام الجيران (NS) وإعلانات الجيران (NA) لتحسين أمان NDP في شبكات IPv6. يمكن لهذه الأفكار أن تساعد مسؤولي الشبكة ومصممي البروتوكولات على تنفيذ دفاعات فعالة ضد هجمات NDP، مما يعزز استقرار وأمان نشرات IPv6. تساهم أبحاثنا في الجهود المستمرة لتحسين موثوقية شبكة IPv6 من خلال التحقيق في هيكل البروتوكول، دور ICMPv6، القضايا الأمنية المرتبطة، والحلول الأمنية المحتملة.

الكلمات المفتاحية: بروتوكول اكتشاف الجيران - (NDP) بروتوكول حل العناوين - (ARP) الإصدار السادس من بروتوكول الإنترنت - (IPv6) الرجل في الوسط - (MiTM) هجمات الحرمان من الخدمة - (DoS) بروتوكول التحكم برسائل الإنترنت الإصدار السادس - (ICMPv6) أمان - NDP اكتشاف الجيران الآمن – العناوين المولدة تشفيرياً