computers

MDPI

Article

An Analysis of Neighbor Discovery Protocol Attacks

Firas Najjar *, Qusay Bsoul and Hasan Al-Refai

Information Security and Cybersecurity, Philadelphia University, Amman 19392, Jordan;
qbsoul@philadelphia.edu.jo (Q.B.); halrefai@philadelphia.edu.jo (H.A.-R.)
* Correspondence: fnajjar@philadelphia.edu.jo

Abstract: Neighbor Discovery Protocol (NDP) is a network protocol used in IPv6 networks to manage communication between neighboring devices. NDP is responsible for mapping IPv6 addresses to MAC addresses and discovering the availability of neighboring devices on the network. The main risk of deploying NDP on public networks is the potential for hackers or attackers to launch various types of attacks, such as address spoofing attacks, denial-of-service attacks, and man-in-the-middle attacks. Although Secure Neighbor Discovery (SEND) is implemented to secure NDP, its complexity and cost hinder its widespread deployment. This research emphasizes the potential hazard of deploying IPv6 networks in public spaces, such as airports, without protecting NDP messages. These risks have the potential to crash the entire local network. To demonstrate these risks, the GNS3 testbed environment is used to generate NDP attacks and capture the resulting packets using Wireshark for analysis. The analysis results reveal that with just a few commands, attackers can execute various NDP attacks. This highlights the need to protect against the potential issues that come with deploying IPv6 on widely accessible public networks. In addition, the analysis result shows that NDP attacks have behavior that can be used to define various NDP attacks.

Keywords: NDP attacks; IPv6 security; flooding attacks

1. Introduction

Internet Protocol Version 4 (IPv4) [1] specifies the guidelines that regulate computer communication across the internet. Each device on the internet must have a unique IPv4 address in order to communicate with other devices. As the most commonly used IP protocol, IPv4 plays a crucial role in directing data packets through the internet. However, the significant increase in Internet users has resulted in the depletion of available IPv4 addresses, forcing the Internet Assigned Number Authority (IANA), which is the main organization for the allocation of Internet numbering resources, to begin utilizing the Internet Protocol version 6 (IPv6) [2], which enables a vast number of IP addresses. IPv6 addresses are 128-bit numbers, which provides a much larger address space than IPv4, which uses only 32-bits for addressing. This means that there are enough IPv6 addresses for every device on the planet and more. IPv6 also includes a number of other features that are not present in IPv4, such as improved security and support for mobile devices. Despite IPv6 being designed with security in mind and as a successor to IPv4, IPv6 is susceptible to security vulnerabilities inherited from the Neighbor Discovery Protocol (NDP) [3]. NDP lacks authentication and registration mechanisms, leaving it open to attacks.

In IPv6 networks, any connected node can configure its own IP address and communicate with other nodes without authentication or registration. This makes it vulnerable to attackers, who can flood the network with fake NDP messages. Hosts inside the same network must respond to these messages, and they must blindly accept and process them. This can lead to exhaustion of system resources and an eventual system freeze, often requiring rebooting to clear fake addresses from memory.

The original NDP specifications called for the use of IPsec to protect NDP messages. However, the RFCs do not provide detailed instructions on how to use IPsec for this

check for updates

Citation: Najjar, F.; Bsoul, Q.; Al-Refai, H. An Analysis of Neighbor Discovery Protocol Attacks. *Computers* **2023**, *12*, 125. https://doi.org/10.3390/computers12060125

Academic Editor: Paolo Bellavista

Received: 23 May 2023
Revised: 11 June 2023
Accepted: 16 June 2023
Published: 19 June 2023

purpose. In this particular application, IPsec can only be used with a manual configuration of security associations. This is due to bootstrapping problems in using IKE, which is the protocol used to establish IPsec security associations. Additionally, the number of manually configured security associations needed for protecting NDP can be very large, making this approach impractical for most purposes. To address this challenge, Secure Neighbor Discovery (SEND) [4] was developed as a protocol extension to add security features to NDP. SEND uses Cryptographically Generated Addresses (CGA) to encrypt NDP messages. CGAs are generated using a public-key infrastructure (PKI), which allows nodes to verify the authenticity of each other's CGAs. This prevents attackers from spoofing NDP messages or launching other attacks against the NDP. However, the SEND is not widely deployed due to several reasons:

- Compatibility: SEND is not backward compatible with existing IPv6 devices and networks. Therefore, deploying it requires a complete overhaul of the network infrastructure;
- Complexity: The implementation of SEND is complicated and requires additional resources and expertise. This can increase the cost of deployment and maintenance;
- Lack of awareness: Many network administrators and users are not aware of the vulnerabilities present in the NDP protocol. They also do not know about the benefits of using the SEND protocol;
- Limited support: The current operating systems and network devices do not fully support the SEND protocol. This reduces the willingness to adopt it;
- Cost: Deploying SEND requires additional resources, such as public key infrastructure (PKI), which adds to the cost of implementation.

Nowadays, many commercial enterprises offer free public internet access to their customers, making the internet network available and reachable to everyone, such as Wi-Fi hotspots in coffee shops, airports, hotels, and other locations. This opens up the possibility of NDP attacks. It is simply possible for anyone connected to these networks to perform NDP denial-of-service attacks with little experience using networks and limited command-line knowledge. These attacks caused significant disruption to businesses and organizations that rely on the internet. The economic loss of the NDP attack can be measured in terms of lost revenue, productivity, and reputational damage. Businesses that are unable to operate due to a denial-of-service attack can lose significant revenue. Moreover, businesses that are the target of a denial-of-service attack can suffer damage to their reputation.

This research aims to investigate the effects of NDP attacks and analyze their behavior. By studying the behavior of these attacks, researchers can develop effective solutions to secure IPv6 without adding unnecessary complexity or vulnerabilities to the protocol.

The rest of this paper is organized as follows: Section 2 presents the background of the NDP. Section 3 describes the related work. Section 4 describes the testing and analysis of NDP attacks. Finally, the conclusion is covered in Section 5.

2. NDP Background

The Neighbor Discovery Protocol (NDP) mechanism enables connected nodes to configure their own IP addresses and gateways as well as communicate with neighboring nodes without requiring authentication or authorization within the local site [5]. However, this makes it vulnerable to attackers, who can impersonate any node in the network and launch various attacks. While NDP does include IPsec in its original specification to secure Neighbor Discovery Protocol (NDP) messages [6], there are no instructions on how to use IPsec or automatically exchange keys, making it impractical for most use cases [7].

In IPv6, NDP uses ICMPv6 messages to allow nodes to identify their neighbors on the same LAN and advertise their presence to other neighbors. The ICMPv6 messages are [8]:

- Router Solicitation (RS): Hosts generate these messages at system startup to request router information;
- Router Advertisement (RA): The router generates these messages and sends them periodically, or the router sends them in response to router solicitation. Routers use

RAs to advertise their presence and send specific parameters such as MTU, router prefix, lifetime for each prefix, and hop limits;

- Neighbor Solicitation (NS): Hosts generate these messages to discover the link-layer addresses of other nodes on the same local link or to verify the reachability of neighboring nodes;
- Neighbor Advertisement (NA) messages are sent to advertise the changes of the host MAC address and IP address or solicit responses to NS messages;
- Redirect messages are used to redirect traffic from one router to another.

The absence of NDP authentication gives the attackers the opportunity to easily flood or spoof the IPv6 network with fake NDP messages. The NDP flooding and spoof message attacks can be categorized as follows [9]:

- The RA Flooding attack sends a huge number of RA messages to a specific host or to all multi-cast nodes (FE02::1). Therefore, most hosts blindly accept and process all RA messages, thereby, exhausting the system resources of these hosts, which may lead to freezing them, and eventually rebooting is required to clear the memory of thousands of fake addresses;
- The RS Flooding attack sends a huge number of RS messages targeting routers inside the local area network (LAN); it sends all these messages to the all-routers multicast group (FE02::2), keeping the routers busy answering all RS messages and, consequently, preventing routers from completing other requests;
- NA Flooding attacks flood the network with a huge number of NA messages trying to exhaust the kernel memory of neighboring node cashes; furthermore, systems that do not enforce limitation policies in node caches end in kernel panic;
- NS Flooding attacks flood IPv6 networks with a huge number of NS messages, causing target nodes to remove saved entries from their neighbor caches, and try to poison the neighbor cache by sending Neighbor Solicitation;
- Redirect Flooding Attack: send a large number of data redirected to an existing node, which exhausts the node's resources and leads to a DoS attack;
- Neighbor Spoofing: In this attack, an attacker impersonates a legitimate neighbor by sending fake NDP messages with the spoofed IP or MAC address. This can lead to the attacker redirecting legitimate traffic to a malicious destination, causing a denial of service;
- Router Advertisement Spoofing: An attacker sends Router Advertisement messages with false information, which can redirect traffic to a malicious router or network;
- Rogue Router: An attacker can pretend to be a legitimate router and send malicious Router Advertisement messages to the network, leading to a man-in-the-middle attack.

3. Related Works for Securing NDP

NDP lacks authentication and is stateless, which exposes it to attacks [10,11]. Even IPsec is used in the original design of IPv6 to secure it; however, IPsec needs manual configuration, which makes it limited to small networks with known hosts [12].

There are two main approaches to overcoming the limitations of NDP: securing NDP and monitoring NDP. Securing NDP solutions typically involves making changes to the original design of the protocol, which can increase its complexity. Monitoring NDP solutions, on the other hand, does not modify the original design of the protocol. Instead, they detect any violations of the protocol's predefined normal behavior and alert system administrators.

Some examples of securing NDP solutions include SEND [13] and Cryptographically Generated Addresses (CGAs) [14]. SEND and CGAs are the best choices for securing IPv6 networks where IPsec is not practical. However, they have not been widely implemented or deployed due to their high complexity and other issues, such as intellectual property claims and licensing terms.

Another example of a secure NDP solution is the use of digital signatures [15]. This solution is less complex than CGAs, but it cannot detect all types of NDP attacks. Another solution is to use a highly randomized technique for address generation. This solution protects node privacy and ensures address uniqueness on the link [16].

The main limitation of all NDP security solutions is that they increase the complexity of the protocol. In contrast, monitoring NDP solutions does not increase the complexity of the protocol. Instead, their main role is to alert system administrators of any violations of NDP's normal behavior.

There are two types of monitoring solutions: passive and active. Passive monitoring solutions track changes in MAC-IP pairings. Any changes trigger alerts to system administrators. In addition, rules-based detection techniques are used to detect any violation of the network configuration or the fragmentation of RA messages and extension headers [17–19]. The main drawback of passive monitoring is that the training phase must be free of any compromised nodes; otherwise, the detection process will fail [20,21]. For that, [22,23] suggest dynamically updating the rules whenever a legitimate change on the network appears.

Active monitoring solutions use probe packets to gather additional observations [24,25]. One example of an active monitoring solution is Multicast Listener Discovery (MLD) probing [26]. MLD probing reduces the amount of traffic generated by active monitoring. Another example is a host-based IDPS that verifies any changes made to its neighbor cache by sending Neighbor Solicitations (NS) probes [27].

The main limitation of active monitoring is that it generates overhead traffic. This traffic can be used by attackers to perform denial-of-service attacks by flooding nodes with fake MAC-IP address pairs.

In conclusion, there are a number of challenges to securing the NDP. Securing NDP solutions increases the complexity of the protocol, while monitoring NDP solutions does not. However, monitoring NDP solutions can generate overhead traffic that can be used by attackers to perform denial-of-service attacks.

4. NDP Attacks: Effect and Analysis

Nowadays, NDP attacks can affect networks and operating systems by causing network downtime, packet loss, data theft, and unauthorized access. They can also be exploited to launch more complex attacks, such as sniffing or spoofing. These attacks can compromise the integrity, confidentiality, and availability of the networks and operating systems, leading to a significant loss of time and revenue for an organization. It is essential to have proper security controls in place to protect against NDP attacks. The main aim of this paper is to highlight and analyze the effects of these attacks on networks and operating systems. Analyzing the attack behavior provides hints on how to mitigate it and helps in defining features to detect it.

4.1. NDP Attack Generation

In order to analyze the NDP attacks, a testbed was created. As shown in Figure 1, different tools are used to generate and capture NDP packets.

To ensure that the testbed accurately mirrors an actual IPv6 network, the tools selected emulate those found in a real-world scenario. The primary tools utilized to create NDP packets consist of:

- Graphical Network Simulator GNS3 Network Tool is open-source software that provides a graphical network simulator to emulate computer networks by connecting real and virtual devices together. This helps in simulating complex networks easily and quickly [28];
- Wireshark is a packet analyzer for networks that captures network packets and translates them into easily understandable formats. Traditionally, such packet analyzers were costly, but Wireshark now offers an open-source, free solution that assists with network troubleshooting, traffic analysis, and communication protocol development [29];

- THC-IPv6 is a toolkit that allows you to test the security of an IPv6 network by executing attacks against it. This toolkit includes a variety of tools that can be used to discover IPv6 hosts on a network, perform reconnaissance, and launch attacks [30];
- Oracle Virtual Machine (VM) is a free, open-source program that allows multiple operating systems and applications to run on the same physical hardware simultaneously. In simpler terms, it enables a single machine to function like many computers [31].

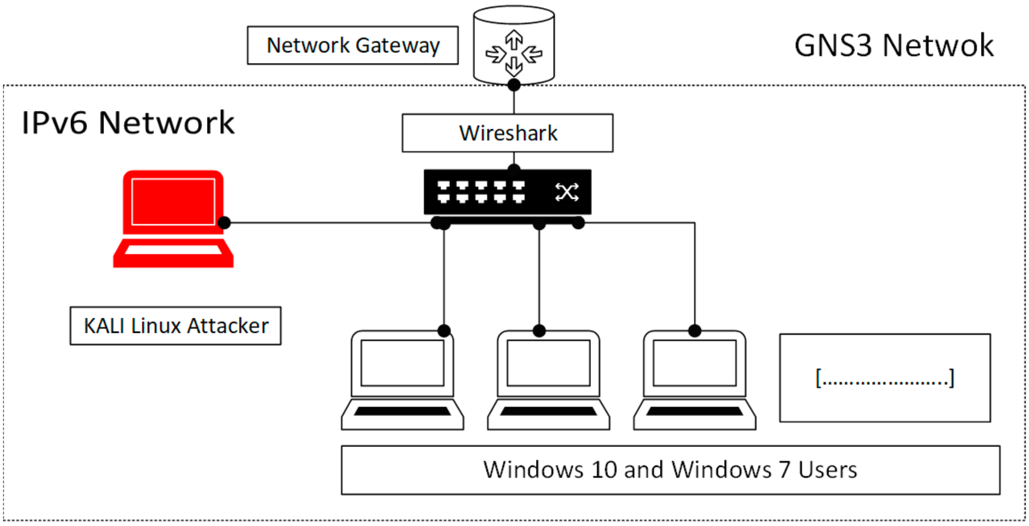


Figure 1. Testbed architecture.

The infrastructure for testing includes virtual machines that are linked together using the GNS3 Network tool. These machines include Windows 10, Windows 7, and Kali Linux stations. Kali Linux is equipped with thc-ipv6 toolkits to execute NDP attacks, and Wireshark is used to record, decode, filter, and convert data packets into another format in order to analyze them.

In the normal behavior of NDP, when a testbed is launched, neighboring nodes start to exchange messages to discover and maintain their presence and availability. Routers periodically send RA messages to inform neighboring nodes of their presence and availability. These messages may also include options such as prefix information, the default gateway address, and other configuration parameters. Moreover, nodes can send RS messages to request immediate RA messages from routers instead of waiting for periodic messages. This can be useful in scenarios where the node is just joining the network and needs configuration parameters. In addition, nodes send NS messages to discover the link-layer address of a neighboring node, and the latter responds with an NA message. These messages are essential for building and maintaining the neighbor cache, which is used to forward packets to other nodes.

All normal behavior messages are captured and recoded using the Wireshark tool. Additionally, the resources used by nodes during normal activity are observed to compare them later with resources used during attacks. This helps us understand how attacks affect nodes inside IPv6 networks.

4.2. NDP Attacks Effects

As previously mentioned, there are no authentication mechanisms for NDP nodes in an IPv6 environment. Consequently, every node will accept and process all NDP packets regardless of the source's validity. For example, in Figure 2, an attacker using the thc-IPv6 toolkit can flood an IPv6 network with thousands of NDP packets.

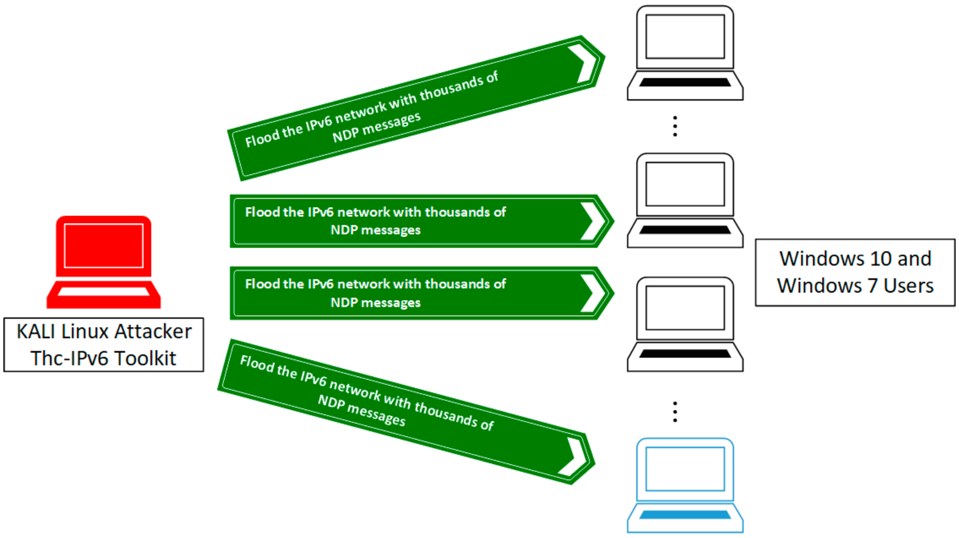

Flood the IPv6 network with thousands of NDP messages
Flood the IPv6 network with thousands of NDP messages
Flood the IPv6 network with thousands of NDP messages
Flood the IPv6 network with thousands of NDP messages
KALI Linux Attacker
Thc-IPv6 Toolkit
Windows 10 and
Windows 7 Users

Figure 2. NDP flooding attack scenario.

The Flood-Route6 attack tool, for instance, can send thousands of RA packets with random prefixes to every network node. These packets are blindly accepted, and every node generates a new IPv6 address using the phony prefix. This leads to the depletion of crucial resources such as CPU and memory, as illustrated in Figure 3.

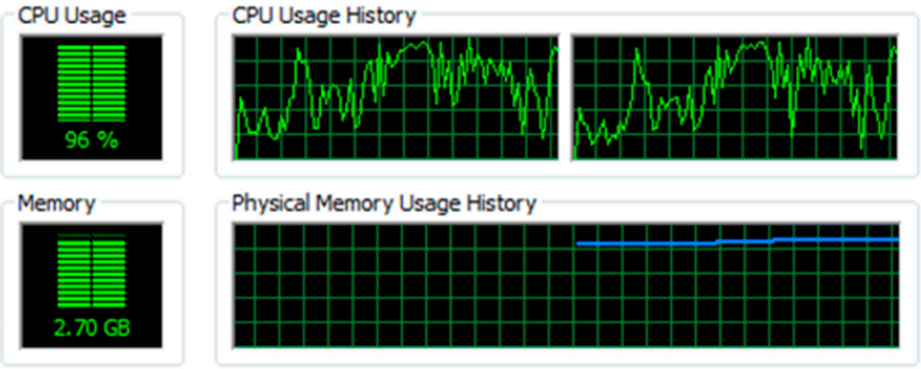
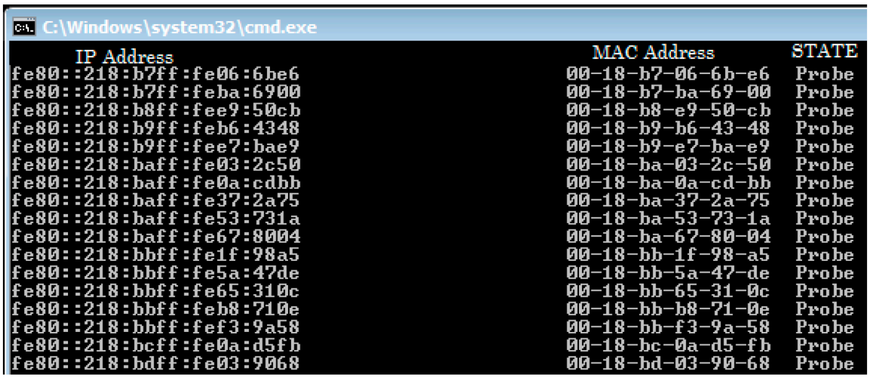


Figure 3. Resource consumption under the Flood-Route6 attack scenario.

Additionally, the Flood-Solicitate6 attack tool floods the network with random NS messages. Upon receiving a fake NS message, a victim node will fill its neighbor cache with new entries, as depicted in Figure 4. Further, the attacker can overwhelm the victim node with NA messages, overburdening its resources unless the victim sets a limit for its cache size.

NDP attacks require the attacker to be located within the same broadcast domain as the target devices. This limits the scope of the attack to a specific network. Moreover, NDP attacks have a high impact on the targeted devices, including network disruptions and resource depletion, which may compel device restarts. Given that the internet has become a crucial service for many hospitality businesses, NDP attacks can be exploited to undermine the trust and reputation of targeted businesses. It is also possible for such attacks to be launched by insiders, disrupting regular business operations. In critical cases, these types of attacks can disturb critical activities such as universities' online exams.



```
        IP Address                                          MAC Address        STATE
fe80::218:b7ff:fe06:6be6                              00-18-b7-06-6b-e6   Probe
fe80::218:b7ff:feba:6900                              00-18-b7-ba-69-00   Probe
fe80::218:b8ff:fee9:50cb                              00-18-b8-e9-50-cb   Probe
fe80::218:b9ff:feb6:4348                              00-18-b9-b6-43-48   Probe
fe80::218:b9ff:fee7:bae9                              00-18-b9-e7-ba-e9   Probe
fe80::218:baff:fe03:2c50                              00-18-ba-03-2c-50   Probe
fe80::218:baff:fe0a:cdbb                              00-18-ba-0a-cd-bb   Probe
fe80::218:baff:fe37:2a75                              00-18-ba-37-2a-75   Probe
fe80::218:baff:fe53:731a                              00-18-ba-53-73-1a   Probe
fe80::218:baff:fe67:8004                              00-18-ba-67-80-04   Probe
fe80::218:bbff:fe1f:98a5                              00-18-bb-1f-98-a5   Probe
fe80::218:bbff:fe5a:47de                              00-18-bb-5a-47-de   Probe
fe80::218:bbff:fe65:310c                              00-18-bb-65-31-0c   Probe
fe80::218:bbff:feb8:710e                              00-18-bb-b8-71-0e   Probe
fe80::218:bbff:fef3:9a58                              00-18-bb-f3-9a-58   Probe
fe80::218:bcff:fe0a:d5fb                              00-18-bc-0a-d5-fb   Probe
fe80::218:bdff:fe03:9068                              00-18-bd-03-90-68   Probe
```

Figure 4. Updating the host cache with fake IP and MAC addresses.

This paper analyzes the behavior of each attack and its effectiveness on IPv6 network traffic. Analyzing attack behavior can help us mitigate attacks and define features for detecting them. The types of attacks used in this paper can be categorized into three categories based on their harmful effects.

4.2.1. Flooding Attacks

NDP flooding attacks consume network bandwidth and node processing resources by processing a large number of NDP messages. Two flooding attacks were used in this paper: the first flooding attack is called Flood_RA, where the network is flooded with thousands of RA messages. Figure 5 shows the number of NDP messages per second while the system is under attack.

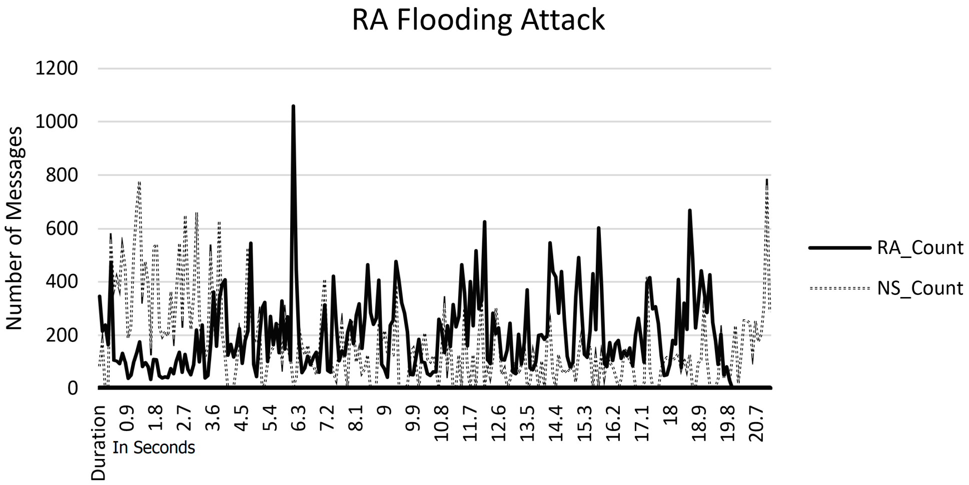


Figure 5. NDP messages counts under RA flooding attack.

The attack increases the number of RA and NS messages sent by a host, while the number of other types of messages remains the same. The generated RA messages cause the host's operating system to create new IPv6 addresses in response to every packet it receives. The host then uses these new addresses to send NS messages in response to the Duplicate Address Detection (DAD) process. Additionally, the host consumes more CPU time as the Stateless Address Autoconfiguration (SLAAC) process attempts to configure the new addresses [32].

Here is a more detailed explanation of each of the steps involved in the attack:

- The attacker sends a large number of RA messages to the target host;
- The RA messages cause the host's operating system to create new IPv6 addresses;
- The host then uses these new addresses to send NS messages in response to the DAD process;

- The DAD process is used to verify that the new addresses are not already in use by another host on the network;
- The SLAAC process is used to configure the new addresses on the host;
- The SLAAC process consumes CPU time, which can slow down the host.

The attack can be used to disrupt network communication or gain unauthorized access to a network.

The second flooding attack used is called Flood_NS. It sends a large number of NS messages to a specific node. It is prohibited to use the all-nodes address (FF02:1) as a target address for this attack. Figure 6 shows the number of NDP messages per second while the system is under NS flooding attack. The attack affects the number of NS and NA messages, while the other types of messages are unaffected. The attacker forces the victim's node to respond to each NS message by sending NA messages.

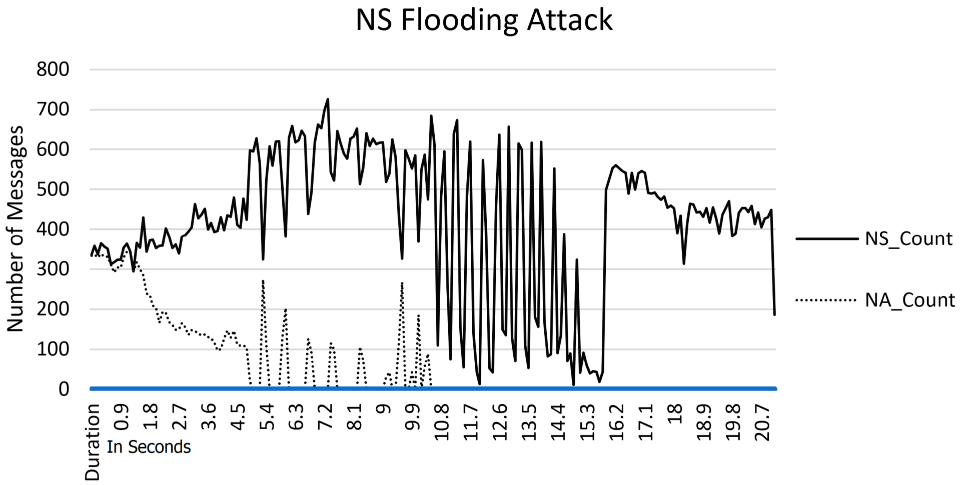


Figure 6. NDP messages counts under NS flooding attack in seconds.

The figure shows that there are no NA messages after the 10th second. This is because the attacker is using NS messages with fake addresses. The victim first responds to NS messages by sending NA messages to the fake IPs. The victim then adds these fake IPs to its cache and changes the status of the IPs to stale. To confirm the reachability of the IPs, the victim starts to send NS to all fake addresses and changes the status of these addresses to probe. As there is no response from the fake addresses, the victim sends three NS messages to all of them.

Here is a more detailed explanation of each of the steps involved in the attack:

- The attacker sends a large number of NS messages to the target node;
- The NS messages cause the victim's node to respond by sending NA messages;
- The victim's node adds the fake IPs to its cache and changes the status of the IPs to stale;
- The victim's node starts to send NS to all fake addresses and changes the status of these addresses to probe;
- As there is no response from the fake addresses, the victim's node sends three NS messages to all of them.

Flooding attacks have a big effect on the number of NDP messages compared to the original normal counts. Figure 7 shows the counts of NDP messages over 24 h under normal behavior.

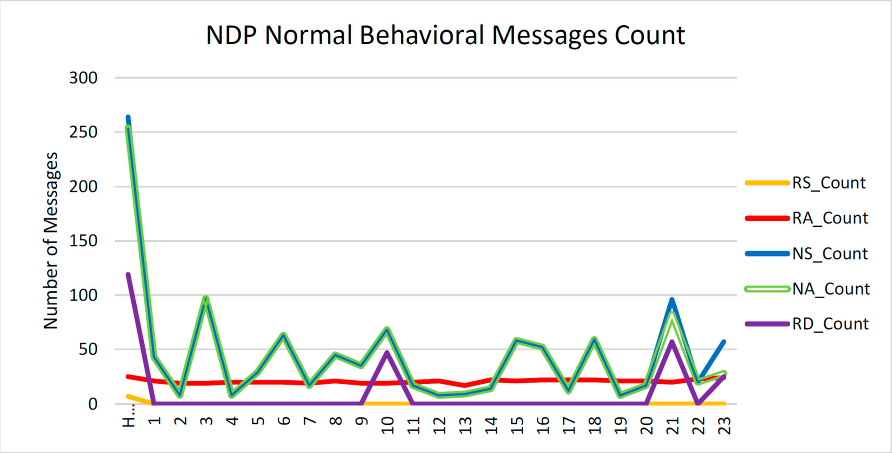


Figure 7. Normal behavior NDP message count in normal hours.

When analyzing normal NDP behavior, RS messages appear on the first connection because they are only generated when a host boots up. The number of these messages is limited because RA messages are periodically generated over time, as shown in the same Figure 7. In normal behavior, the router sends RA messages periodically to all hosts in the multicast group or in response to RS messages.

NS messages are used in address resolution and NUD processes. The receiver of a NS message must respond by sending a NA message. Therefore, it is clear from the figure that the number of NS messages and NA messages is approximately equal over time. Redirect messages are sent by the router to advertise a better hop.

Here is a more detailed explanation of each of the messages mentioned:

- Router Advertisement (RA) messages are used by routers to advertise their presence on a network and to provide information about the network, such as the network prefix and the default gateway;
- Neighbor Solicitation (NS) messages are used by hosts to request information about a neighbor, such as the neighbor's link-layer address;
- Neighbor Advertisement (NA) messages are used by hosts to respond to NS messages and to advertise their own link-layer address;
- Redirect messages are used by routers to inform hosts that a better next hop exists for a particular destination.

The number of each type of message can vary depending on network activity. For example, the number of RA messages will increase if there are new hosts joining the network. The number of NS and NA messages will increase if hosts are communicating with each other. The number of redirect messages will increase if hosts are using a suboptimal route to reach a destination.

4.2.2. DoS Attack

A DoS attack is any attempt to disrupt the normal functioning of a network by overwhelming it with traffic. In the context of IPv6, a DoS attack can be carried out by sending fake RA messages containing incorrect configuration data. This can lead to the router becoming unreachable for legitimate nodes. To mitigate this attack, it is important to have a network security profile that defines the legitimate configuration data for RA messages.

4.2.3. MITMA Attacks

A MITMA attack is a type of attack where an attacker is able to intercept and modify traffic between two parties. In the context of IPv6, a MITMA attack can be carried out by sending unsolicited NA messages. These messages are used to advertise the link-layer address of a node. By sending unsolicited NA messages, an attacker can change the default router information in the host's cache. This can allow the attacker to intercept and modify traffic between the host and the router. To mitigate this attack, it is important to verify the source of NA messages before updating the host's cache.

Another way to carry out a MITMA attack is to send solicited NA messages with the default router MAC address changed to the attacker's MAC address. This will cause the host to believe that the attacker is the default router. To detect this attack, it is important to check whether the solicited NA message is generated in response to a NS message. If it is not, then the message is likely from an attacker.

4.3. Result Discussion

The designers of IPv6 assumed that all users on a local area network were trusted. However, this is not always the case. Public users, such as those in an airport or coffee shop, should not be trusted. In addition, employees have been shown to be a significant source of attacks. Therefore, it is important to study and analyze NDP attacks in order to take steps to mitigate them and protect networks.

In order to study and analyze the normal behavior of the protocol, Testbed uses both Windows and Linux operating systems to simulate the normal behavior of NDP protocols. This is important because all modern operating systems must support the IPv6 protocol. The captured network packets are filtered using the Wireshark tool to separate the NDP packets from other protocol packets. This is necessary to concentrate on the NDP's behavior and message flow. Once the NDP packets have been captured, they are compared against the expected behavior of the protocol as outlined in the protocol RFC. This proves that both the Windows and Linux operating systems adhere to the expected protocol specifications.

NDP attacks are limited in scope to a specific network, as the attacker must be situated within the same broadcast domain as the target device. However, NDP attacks have a significant impact on targeted devices and can be performed using simple tools available online. These attacks affect the business's reputation and have a significant impact on normal business operations. Moreover, the consequences of NDP attacks can be far-reaching and even disrupt critical activities such as university online exams. NDP attacks utilize standard protocol messages, which makes them difficult to detect. However, such attacks deviate from typical protocol behavior. Under normal circumstances, an IPv6 node sends a message every second. However, an attacker can send thousands of messages in less than a second during an NDP attack, depleting network resources.

To produce abnormal behavior in NDP, the thc-ipv6 toolkit was utilized in the testbed. Studying flooding attacks has revealed that they create packet patterns that are distinct from typical protocol behavior. By identifying and analyzing these patterns, we can accurately identify NDP flooding attacks. This is because any deviation from the expected protocol behavior is a clear indication of an attack, particularly when the behavior is significantly different from what is considered normal. However, it becomes more challenging to detect DoS and MITMA attacks as these attacks use legitimate protocol processes. In such cases, it is necessary to create a network profile to define legitimate network service providers, such as routers. A change in the protocol standard may also add complexity and reduce its simplicity.

5. Conclusions

IPv6 is the successor to IPv4, the current version of the Internet Protocol. IPv6 was developed to address the problem of IPv4 address exhaustion. IPv6 provides a much larger address space; therefore, it is becoming more widely adopted.

IPv6 is secure by design. It uses a number of security features, such as IPsec, to protect data from unauthorized access. However, most proposed solutions for securing IPv6 increase the protocol overhead and complexity; therefore, they are not widely implemented or deployed. As IPv6 adoption continues, it is important to be aware of the security implications. Therefore, this paper highlights the effect of NDP attacks on the network and operating systems.

In this paper, a testbed is used to analyze the impact of NDP attacks on networks and operating systems. The results of these tests show that with simple commands, attackers can affect the network and operating systems by causing network downtime, packet loss, data theft, and unauthorized access. These attacks can compromise the integrity, confidentiality, and availability of the network and operating systems, leading to a significant loss of time and revenue for an organization. It is essential to have proper security controls in place to protect against NDP attacks.

Having an IPv6 network that allows for digital signatures during the IPv6 neighbor discovery process can effectively prevent attacks like the falsification of RA and NS messages. Nonetheless, implementing this approach may not be practical for networks with a large number of users or that are publicly accessible. To compensate for this, it is crucial to monitor network activity to identify any deviations from the normal behavior of the NDP protocol, such as blocking messages that are outside of the protocol's expected behavior. To achieve this, network tools can be utilized to detect and prevent potential attacks, such as firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS). However, these network tools must be configured, probably because misconfiguration could impact the normal behavior of the protocol.

Any business that decides to start using IPv6 networks should know about the security issues related to NDP. They should make sure that their network has the proper tools and professionals who support IPv6 to keep it secure. In addition, policies and procedures need to be in place to prevent any NDP attacks without making the network more complex. NDP attack results indicate that NDP attacks have a unique way of sending packets. This highlights the need for further investigation into how network tools can precisely determine the behavior of the protocol. One potential solution is to apply machine learning techniques to identify the specific features of the protocol. By doing so, abnormal behavior can be more accurately detected and identified.

Author Contributions: Conceptualization, F.N. and H.A.-R.; methodology, F.N.; software, Q.B.; validation, F.N., Q.B. and H.A.-R.; formal analysis, F.N.; investigation, F.N. and H.A.-R.; resources, Q.B.; writing—original draft preparation, F.N.; writing—review and editing, F.N.; visualization, F.N. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Deanship of Scientific Research at Philadelphia University.

Data Availability Statement: For data supporting reported results, please contact fnajjar@philadelphia.edu.jo.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Postel, J. Internet Protocol. RFC 791. DARPA Internet Program Protocol Specification. 1981. Available online: https://www.rfc-editor.org/rfc/rfc791 (accessed on 5 January 2023).
2. Najjar, F.; El-Taj, H. Ipv6 Change Threats Behavior. *Int. J. Adv. Comput. Sci. Appl.* **2015**, *6*, 63–68. [CrossRef]
3. Narten, T.; Nordmark, E.; Simpson, W.; Soliman, H. Neighbor Discovery for IP Version 6 (IPv6). RFC 4861. 2007. Available online: https://www.rfc-editor.org/rfc/rfc4861 (accessed on 10 January 2023).
4. Arkko, J.; Kempf, J.; Zill, B.; Nikander, B. Secure Neighbor Discovery (SEND). RFC 3971. 2005. Available online: https://www.rfc-editor.org/rfc/rfc3971 (accessed on 10 January 2023).
5. Narten, T.; Thomson, S.; Jinmei, T. IPv6 Stateless Address Autoconfiguration. RFC 4862. Internet Engineering Task Force. 2007. Available online: https://www.rfc-editor.org/rfc/rfc4862 (accessed on 10 January 2023).
6. Kent, S.; Seo, K. Security Architecture for the Internet Protocol. RFC4301. 2005. Available online: https://www.rfc-editor.org/rfc/rfc4301 (accessed on 10 January 2023).
7. Frankel, S.; Graveman, R.; Pearce, J.; Rooks, M. *Guidelines for the Secure Deployment of IPv6. NIST Special Publication 800-119*; NIST Special Publication 800-119; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2010; 188p. Available online: https://csrc.nist.gov/publications/detail/sp/800-119/final (accessed on 10 January 2023).
8. Conta, A.; Gupta, M.; Deering, S. Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification. RFC4443. 2006. Available online: https://www.rfc-editor.org/rfc/rfc4443 (accessed on 10 January 2023).

9. Najjar, F.; Kadhum, M.M.; El-Taj, H. Detecting neighbor discovery protocol-based flooding attack using machine learning techniques. In *Advances in Machine Learning and Signal Processing: Proceedings of MALSIP 2015*; Springer International Publishing: Cham, Switzerland, 2016. [CrossRef]
10. Nikander, P.; Kempf, J.; Nordmark, E. IPv6 Neighbor Discovery (ND) Trust Models and Threats. RFC 3756. 2004. Available online: https://www.rfc-editor.org/rfc/rfc3756 (accessed on 11 January 2023).
11. Jankiewicz, E.; Loughney, J.; Narten, T. IPv6 Node Requirements. No. RFC6434. 2011. Available online: https://www.rfc-editor.org/rfc/rfc6434 (accessed on 11 January 2023).
12. Agarwal, A.; Bhadauria, S. A comparative study of VPN Protocols (PPTP Vs L2TP Vs SSTP Vs IKEV2 Vs OPENVPN). *Int. J. Eng. Comput. Sci.* **2017**, *6*, 23209–23214. [CrossRef]
13. Gagliano, R.; Krishnan, S.; Kukec, A. Subject Key Identifier (SKI) SEcure Neighbor Discovery (SEND) Name Type Fields. RFC 6495. 2012. Available online: https://www.rfc-editor.org/rfc/rfc6495 (accessed on 11 January 2023).
14. Bagnulo, M.; Arkko, J. Cryptographically Generated Addresses (CGA) Extension Field Format. RFC 4581. 2006. Available online: https://www.rfc-editor.org/rfc/rfc4581 (accessed on 11 January 2023).
15. Hassan, R.; Ahmed, A.S.; Osman, N.E. Enhancing Security for IPv6 Neighbor Discovery Protocol Using Cryptography. *Am. J. Appl. Sci.* **2014**, *11*, 1472–1479. [CrossRef]
16. Shah, J.L.; Parvez, J. Optimizing Security and Address Configuration in IPv6 SLAAC. *Procedia Comput. Sci.* **2015**, *54*, 177–185. [CrossRef]
17. Al-Shareeda, M.A.; Manickam, S.; Saare, M.A.; Arjuman, N.C. Proposed security mechanism for preventing fake router advertisement attack in ipv6 link-local network. *Indones. J. Electr. Eng. Inform.* **2022**, *46*, 31–38. [CrossRef]
18. Kaur, H.; Kaur, A. An empirical study of aging related bug prediction using cross project in cloud oriented software. *Informatica* **2022**, *46*, 105–120. [CrossRef]
19. Al-Shareeda, M.A.; Manickam, S.; Laghari, S.A.; Jaisan, A. Replay-attack detection and prevention mechanism in industry 4.0 landscape for secure secs/gem communications. *Sustainability* **2022**, *14*, 15900. [CrossRef]
20. Beck, F.; Cholez, T.; Festor, O.; Chrisment, I. Monitoring the neighbor discovery protocol. In Proceedings of the 2007 International Multi-Conference on Computing in the Global Information Technology (ICCGI'07), Guadeloupe, French Caribbean, 4–9 March 2007. [CrossRef]
21. Al-Shareeda, M.A.; Manickam, S.; Saare, M.A.; Bin Omar, N. SADetection: Security Mechanisms to Detect SLAAC Attack in IPv6 Link-Local Network. *Informatica* **2022**, *46*, 31–38. [CrossRef]
22. Al-Shareeda, M.A.; Manickam, S. Msr-dos: Modular square root-based scheme to resist denial of service (dos) attacks in 5g-enabled vehicular networks. *IEEE Access* **2022**, *10*, 120606–120615. [CrossRef]
23. SBourougaa-Tria, S.; Mokhati, F.; Tria, H.; Bouziane, O. Spubbin: Smart public bin based on deep learning waste classification an iot system for smart environment in algeria. *Informatica* **2022**, *46*, 41–66. [CrossRef]
24. Barbhuiya, F.A.; Bansal, G.; Kumar, N.; Biswas, S.; Nandi, S. Detection of neighbor discovery protocol based attacks in IPv6 network. *Netw. Sci.* **2013**, *2*, 91–113. [CrossRef]
25. Barbhuiya, F.A.; Biswas, S.; Hubballi, N.; Nandi, S. A host based DES approach for detecting ARP spoofing. In Proceedings of the 2011 IEEE Symposium on Computational Intelligence in Cyber Security (CICS), Paris, France, 11–15 April 2011; pp. 114–121. [CrossRef]
26. Bansal, G.; Kumar, N.; Nandi, S.; Biswas, S. Detection of NDP based attacks using MLD. In Proceedings of the Fifth International Conference on Security of Information and Networks, Jaipur, India, 25–27 October 2012. [CrossRef]
27. Kumar, N.; Bansal, G.; Biswas, S.; Nandi, S. Host based IDS for NDP related attacks: NS and NA Spoofing. In Proceedings of the 2013 Annual IEEE India Conference (INDICON), Mumbai, India, 13–15 December 2023; pp. 1–6. [CrossRef]
28. GNS3. 2023. Available online: https://www.gns3.com/ (accessed on 1 February 2023).
29. Wireshark. 2023. Available online: https://www.wireshark.org/ (accessed on 1 February 2023).
30. Thc-IPv6 Toolkit. 2023. Available online: https://www.kali.org/tools/thc-ipv6/ (accessed on 1 February 2023).
31. Virtual Box. 2023. Available online: https://www.virtualbox.org/ (accessed on 1 February 2023).
32. Shah, J.L.; Bhat, H.F. Towards a Secure IPv6 Autoconfiguration. *Inf. Secur. J. A Glob. Perspect.* **2020**, *29*, 14–29. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.