ENHANCED TRUST-ND PROTOCOL TO PREVENT TEMPORAL DENIAL-OF-SERVICE VULNERABILITIES ON IPV6 LINK-LOCAL NETWORK

IZNAN HUSAINY BIN HASBULLAH

UNIVERSITI SAINS MALAYSIA

2023

ENHANCED TRUST-ND PROTOCOL TO PREVENT TEMPORAL DENIAL-OF-SERVICE VULNERABILITIES ON IPV6 LINK-LOCAL NETWORK

by

IZNAN HUSAINY BIN HASBULLAH

Thesis submitted in fulfilment of the requirements
for the degree of
Master of Science

September 2023

ACKNOWLEDGEMENT

First and foremost, all praise is due to Allah SWT, and His Peace and Blessings be upon His Final Messenger, his pure family, his noble Companions, and all those who follow them with righteousness until the Day of Judgment.

None deserved the most gratitude after Allah SWT than my parents, Hasbullah bin Hussin and Nik Ismah Wan Adnan, for their continuous encouragement and countless prayers and supplications – many during their *qiamullail* before twilight. My other half, Hasanah Haron, and family for being patient and supportive by my side. My supervisor, Dr. Mohamed Anbar, and co-supervisors, Prof Dr. Rosni Abdullah and Ms. Chong Yung-Wey, for guidance throughout the long journey. The knowledge and wisdom imparted are plenty. May all of them be counted as 'beneficial knowledge' that lasts till the end of time. Special mention goes to Prof Dr. Supriyanto of Universitas Sultan Ageng Tirtayasa (UNTIRTA), who is also the field supervisor of this research. His Ph.D. work is the starting point of this research. Not forgetting my first supervisor, Dr. Mohammed Khadum, who started the ball rolling. The Director of National Advanced IPv6 Centre (NAv6), Assoc. Prof Dr. Selvakumar, for the push and nudge in the right direction. Not forgetting the admins and staff of the Centre, current and former, for the help and encouragement along the way.

'Stay hungry, stay humble.'

Iznan H. Hasbullah, Seberang Jaya

TABLE OF CONTENTS

LIST OF TABLES

Page

LIST OF FIGURES

Page

LIST OF ABBREVIATIONS

3GPP	3rd Generation Partnership Project
6LoWPAN	Low-Power Wireless Personal Area Networks
ARSSI	Average Received Signal Strength Indicator
AT	Attacking Host
Bash	Bourne Again Shell
BGP	Border Gateway Protocol
BU	Bandwidth Utilization
CGA	Cryptographically Generated Address
DAD	Duplicate Address Detection
DDoS	Distributed Denial of Service
DHCPv6	Dynamic Host Control Protocol Version 6
DNS	Domain Name System
DPSR	DoS Prevention Success Rate
DoS	Denial of Service
EH	Existing Host
I-D	Internet Draft
IETF	Internet Engineering Task Force
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
IDE	Integrated Development Environment
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IP	Internet Protocol
IPS	Institute of Postgraduate Studies
IPSec	Internet Protocol Security
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
LAN	Local Area Network
LDoS	Low-rate Denial of Service

MAC	Medium Access Control
MAD	Message Authentication Data
MitM	Man-in-the-Middle
NA	Neighbor Advertisement
NAv6	National Advanced IPv6 Centre
NDP	Neighbor Discovery Protocol
NH	New Host
NS	Neighbor Solicitation
NTP	Network Time Protocol
OS	Operating System
PAWS	Protection Against Wrapped Sequences
PTP	Precision Timestamping Protocol
QoS	Quality of Service
RFC	Request for Comments
RPL	Routing Protocol for Low-Power and Lossy Networks
RTTM	Round-Trip Time Measurement
SA	Security Associations
SEND	Secure Neighbor Discovery
SHA-1	Secure Hash Algorithm 1
SLAAC	Stateless Address Autoconfiguration
SNMA	Solicited Node Multicast Address
TAI	*Temps Atomique International* (International Atomic Time)
Trust-NC	Trust Neighbor Cache
Trust-ND	Trust Neighbor Discovery
USM	Universiti Sains Malaysia
UTC	Coordinated Universal Time
UTP	Unshielded Twisted Pair
WSN	Wireless Sensor Network

LIST OF APPENDICES

PROTOKOL TRUST-ND DIPERTINGKAT UNTUK MENCEGAH KERENTANAN NAFI KHIDMAT TEMPORAL PADA RANGKAIAN IPV6 PAUTAN SETEMPAT

ABSTRAK

Trust-ND ialah mekanisme keselamatan berasaskan kepercayaan teragih untuk memastikan keselamatan rangkaian pautan setempat IPv6 sebagai alternatif kepada protokol Penemuan Jiran Selamat (SEND) yang sangat kompleks. Walau bagaimanapun, analisis teori dan eksperimen yang dijalankan mendapati reka bentuk cap masa protokol Trust-ND mendedahkan ia kepada serangan nafi perkhidmatan (DoS) temporal yang berpunca daripada rujukan, format dan sais medan, dan peraturan pengesahbetulan cap masa. Penyelidikan ini bertujuan untuk mencegah kerentanan DoS temporal pada rangkaian pautan setempat IPv6 dengan mempertingkat Trust-ND tanpa mengubah struktur paket asalnya untuk mengekalkan kelebihan atas SEND. Versi Trust-ND dipertingkat yang dicadangkan, dipanggil eTrustND, menangani kerentanan melalui tiga tahap: (i) Formulasi Cap Masa, (ii) Trust-ND Dipertingkat, dan (iii) Mekanisma verifikasi berasakan peraturan. Tahap pertama merubah rujukan masa daripada waktu sistem kepada UTC, format waktu 24-jam dalam bentuk perenambelasan kepada saat epok dalam bentuk integer, dan meningkatkan kejituan daripada per seratus kepada per sepuluh ribu saat. Tahap kedua menggunakan medan *Reserved* Trust-ND untuk nilai sub-saat dan menukar jenis data bagi medan cap masa daripada bait kepada *IntField.* Tahap ketiga mencadangkan satu mekanisma verifikasi berasaskan peraturan untuk menangani situasi waktu komputer tak-segerak bagi mencegah kerentanan DoS temporal. Keputusan eksperimen pada tapak uji menunjukkan bahawa eTrustND mencegah kerentanan DoS berasaskan temporal

tanpa mengubah struktur mesej Trust-ND asal dan tidak meningkatkan overhed (pengkomputeran dan penggunaan lebar jalur). Kadar Kejayaan Pencegahan DoS bagi eTrustND adalah 100 % untuk kedua-dua senario Kondisi DoS (rujukan cap masa dan kejituan) berbanding Trust-ND (0 %). Di samping itu, walaupun kecil, eTrustND telah memperbaiki masa pemprosesan bagi proses DAD tanpa dan bersama konflik alamat IP berbanding Trust-ND sebanyak 0.07092 ms (1.26 %) and 0.055755 ms (0.66 %), masing-masing. Penyelidikan ini menyerlahkan kepentingan pertimbangan teliti apabila mereka bentuk mekanisme atau protokol keselamatan yang bergantung pada cap masa.

ENHANCED TRUST-ND PROTOCOL TO PREVENT TEMPORAL DENIAL-OF-SERVICE VULNERABILITIES ON IPV6 LINK-LOCAL NETWORK

ABSTRACT

Trust-ND is a trust-based distributed security mechanism to secure IPv6 link-local networks as an alternative to the highly complex Secure Neighbor Discovery (SEND) protocol. However, theoretical analysis and experimental research revealed that the Trust-ND protocol is susceptible to temporal Denial-of-Service vulnerabilities due to timestamp reference, field size and format, and verification rule. This research aims to prevent temporal DoS vulnerabilities on IPv6 link-local networks by enhancing Trust-ND without jeopardizing its original structure to retain its advantages over SEND. The proposed enhanced version of Trust-ND, called eTrustND, addresses the vulnerabilities in three stages, (i) Timestamp Formulation, (ii) Enhanced Trust-ND, and (iii) Rule-based verification mechanism. The first stage changes the reference time from system time to UTC, the 24-hour time format in hexadecimal to epoch second in integer. It also increases the precision from one hundredth to one ten-thousandth second. The second stage utilizes the Trust-ND's Reserved field for the sub-second value and changes the timestamp field data type from *byte* to *IntField*. The third stage proposes a rule-based verification mechanism to handle out-of-sync computer clocks, preventing temporal DoS vulnerabilities. The experiment results on a testbed demonstrate that eTrustND prevents temporal-based DoS vulnerabilities without jeopardizing the original Trust-ND packet structure and adding overheads (computation and bandwidth). The eTrustND's DoS Prevention Success Rates are 100 % for both DoS Condition scenarios (timestamp reference and precision) vs. the

existing Trust-ND (0 %). Besides, although marginal, eTrustND improved the total processing time of the DAD process without and with an IP address conflict compared to Trust-ND by 0.07092 *ms* (1.26 %) and 0.055755 *ms* (0.66 %), respectively. This research highlights the importance of careful consideration when designing security mechanisms or protocols that rely on timestamps.

CHAPTER 1

INTRODUCTION

This chapter presents the thesis context, where the research background is described in Section 1.1, followed by Section 1.2, describing this research's motivation. Sections 1.3, 1.4, and 1.5 present the research problem, objectives, and scopes. Next, Sections 1.6 and 1.7 describe this research's contributions and the steps. Finally, Section 1.8 highlights the overall thesis organization.

1.1 Overview

The Internet has revolutionized the way we communicate, work, and live our daily lives. It has become an indispensable tool for businesses and individuals, enabling us to access information and services anywhere in the world. The exponential growth of Internet-facing devices demands more Internet Protocol (IP) addresses that the current IP version cannot support, leading to the development of Internet Protocol version Six (IPv6). IPv6 provides a significantly larger address space than Internet Protocol version Four (IPv4).

A 32-bit address space of IPv4 can support a maximum of 2^{32} (4,294,967,296) or roughly 4.3 billion IP addresses. In contrast, IPv6 uses a 128-bit address space, which provides 3.4 x 10^{38} unique IP addresses or approximately 340 undecillion. This vast address space ensures that there are more than enough addresses to meet the needs of the growing number of devices and users on the Internet.

The "Google IPv6 Statistics" graph (Google, 2022) provides a visual overview of the uptrend of Global IPv6 adoption, as shown in Figure 1.1.

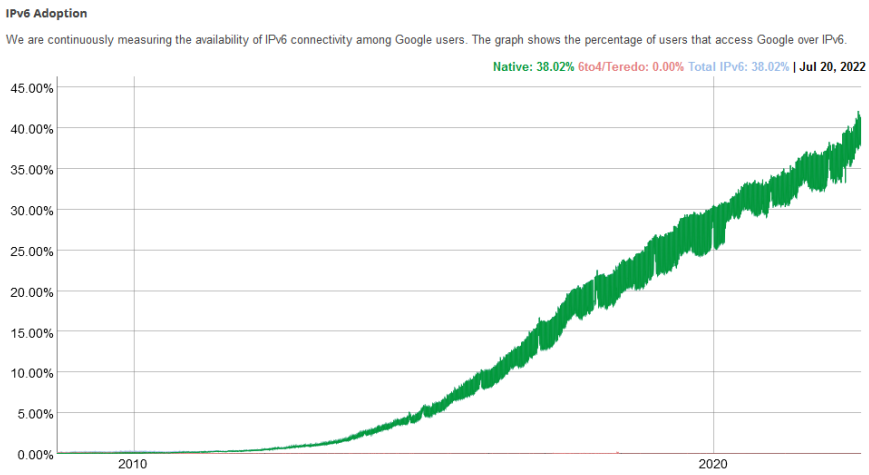

Figure 1.1 Google IPv6 statistics (Google, 2022)

Figure 1.1 shows the trend of Google's IPv6 traffic volumes over the last decade, where nearly ten-fold growth occurred in the latter half. It also shows that as of 20th July 2022, almost 40 % of Google users are on IPv6 networks.

Mobile service providers are among the earliest adopters of IPv6 since 2009 after the 3rd Generation Partnership Project (3GPP) standard organization mandated wireless service providers to enable IPv6 on their 4G wireless infrastructures in 3GPP Specification 8 (3GPP, 2009). The result of the mandate is evident today in the number and percentage of IPv6 adoption among mobile device users. For example, the New T-Mobile, the largest mobile service provider in the US after a merger with Sprint in April 2020, with more than 98 million subscribers in the US alone and 230 million subscribers globally, had close to 100 % IPv6 adoption in 2020 (HexaBuild Inc, 2020).

Even though dual-stack networks, where IPv4 and IPv6 coexist in the same network, still dominate the network world, especially in corporate and enterprise settings, the shift to IPv6-only networks is inevitable simply because the existing IPv4 can no longer provide enough IP addresses for the global need.

1.2 Background

This section provides a brief explanation of IPv6 (Section 1.2.1), Neighbor Discovery Protocol (NDP) (Section 1.2.2), Trust Neighbor Discovery (Trust-ND) with its security issues (Section 1.2.3), and temporal denial-of-service (DoS) vulnerability in (Section 1.2.4).

1.2.1 IPv6

IPv6 is the latest version of the Internet protocol, first proposed in December 1998 by the Internet Engineering Task Force (IETF) as the successor to IPv4 with an Internet Draft (I-D) RFC 2460. It was accepted as an Internet standard in July 2017 as RFC 8200 (Deering & Hinden, 2017). It introduces several changes to IPv4, notably in the addressing capabilities, header format simplification, supporting extensions and options, flow labeling, and adding authentication and privacy features.

Many governments have already issued mandates for IPv6-only networks or supports, such as in China and The United States (Office of the Central Cyber Security and Informatization Committee, 2021; Vought, 2020). Similarly, in the corporate world, especially among the Big Tech, such as Microsoft (McKillop, 2019), Google (Babiker et al., 2011), Cisco (Oswal, 2015), and Amazon, there are already policies and initiatives toward IPv6-only networks. In June 2021, AWS announced “continued commitment and innovation towards the enablement of IPv6 on AWS.” A year later, they launched Amazon Virtual Private Cloud (VPC) with IPv6-only architecture for their clients (Santhanam & Aswani, 2022).

At the end of 2021, there were 25 billion internet-connected devices, and Ericsson projected the number to exceed 40 billion by 2027, as visualized by Ericsson Mobility Visualizer (Ericsson, 2022), shown in Figure 1.2. Connected devices include

mobile phones, wide-area IoT, short-range IoT, vehicles, machines, meters, sensors, point-of-sale terminals, consumer electronics, and wearables.

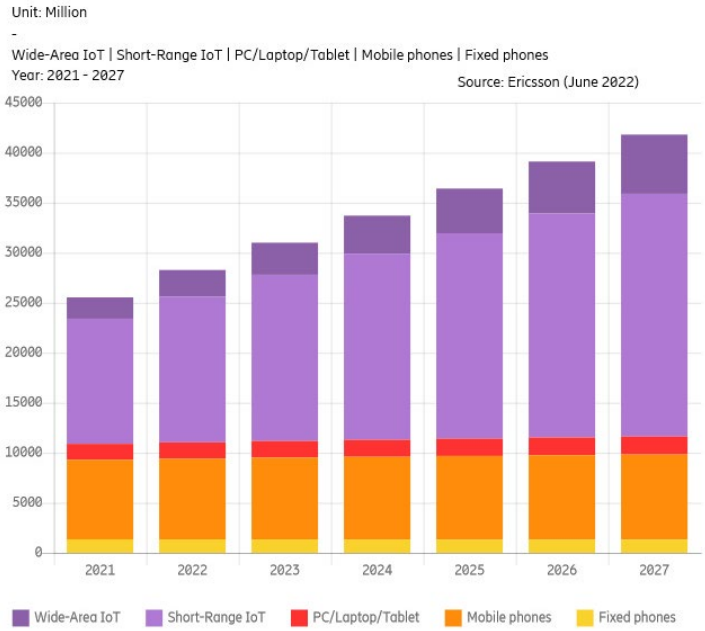

Figure 1.2 Total number of connected devices in 2021 and projection until 2027 (Ericsson, 2022)

According to data from GSMA Intelligence, at the end of 2020, 5.2 billion people subscribed to mobile services, representing 67% of the global population (GSM Association, 2021).

The US government has mandated that at least 80 % of IP-enabled assets on the US Federal network operate in IPv6-only environments by the end of 2025. The US Office of Management and Budget (OMB) issued a mandate on 19th November 2020 via memorandum M-21-07, "Completing the Transition to Internet Protocol Version 6 (IPv6)." The memo outlined the Federal government's strategic intent "to deliver its information services, operate its networks, and access the services of others using only IPv6" (Vought, 2020). Meanwhile, China will no longer allow new networks to use IPv4 by 2023 (Office of the Central Cyber Security and Informatization Committee, 2021). These government mandates or policies will

influence network equipment manufacturers, service providers, and other countries to follow and thus will increase the number of IPv6-only networks and expedite IPv6 adoption globally.

The changes and new capabilities added to IPv6 require updating or creating new protocols, and one of the newly introduced protocols in IPv6 is the NDP.

1.2.2 NDP

NDP is one of the core protocols of IPv6, which is essential for many processes and functionalities involving IPv6 nodes' communication within the local network. It introduced five Internet Control Message Protocol for IPv6 (ICMPv6) messages to perform its operations.

Unfortunately, the transmission of NDP messages is in plain text (Conta & Deering, 2006). Besides, the NDP standard only provides rudimentary security protection using the IPv6 address scope to limit the exposure of the local network to external threats (Haberman et al., 2005).

The lack of a robust default security mechanism in the NDP exposes the local IPv6 network to many threats and vulnerabilities (Mahmood et al., 2019; Zhang & Wang, 2016), not only from the malicious act of adversaries or agents but also from unintentional misconfiguration by users or administrators (Chown & Venaas, 2011). Therefore, the NDP standard recommends two security mechanisms for insider attacks, Secure Neighbor Discovery (SEND) and IP Security (IPsec). However, IPSec is unsuitable for securing a link-local network due to an issue with bootstrapping (Gelogo et al., 2011; Supriyanto et al., 2013), and SEND is heavily criticized for being computationally intensive and having a high bandwidth overhead (Alsa'deh & Meinel, 2012; An et al., 2007; Pohl, 2007).

1.2.3 Trust-ND

Supriyanto proposed Trust-ND, a security mechanism that secures the NDP using a comprehensive, integrated, and decentralized approach, as an alternative to SEND (Supriyanto, 2015). Trust-ND employs distributed trust approach using a probabilistic trust model based on the beta reputation function (Josang & Ismail, 2002) to classify trusted or untrusted IPv6 nodes.

Trust-ND obtained its favorable characteristic by relying on soft and "hard" security combinations, not complex encryption. Trust-ND positioned itself as an alternative to SEND as a lightweight security mechanism for NDP by avoiding complex encryption methods and combining soft and hard security methods. Soft security models expect the presence of unwanted intruders in the system or network. So, instead of adding protective security layers with complex measures, such as access control, program verification, and symmetrical or asymmetrical encryption, it strives to identify and prevent harmful actions to legitimate users (Rasmusson & Jansson, 1996).

The soft security approach adopted by Trust-ND is a distributed trust management approach using a probabilistic trust model based on the beta reputation function (Josang & Ismail, 2002) to identify and classify IPv6 nodes as trusted or untrusted. On the other hand, traditional hard security approaches, such as encryption, authentication, and access control, are proven, widely deployed, and have been extensively studied and scrutinized. Therefore, Trust-ND mainly uses a hybrid approach instead of relying exclusively on hard security to maintain an acceptable level of protection with reduced complexity.

Trust-ND uses a cryptographic (unkeyed) hash function as the hard security mechanism, which ensures data or message integrity with lesser computation demand

and lower overhead than SEND's key-based cryptographic mechanism. In addition, the hash function is widely used in information security protocols or applications to ensure the integrity of messages in transit (Menezes et al., 1997).

Trust-ND introduced a new security measure using a distributed trust approach to ensure secure link-local communication in IPv6 networks. However, there are still weaknesses and vulnerabilities inherent within Trust-ND, such as temporal denial-of-service (DoS) vulnerabilities (Hasbullah et al., 2016) and SHA-1 hash collision (A. K. Al-Ani, Anbar, Manickam, Wey, et al., 2019).

The hash collision issue is easily solvable by switching the hashing algorithm from SHA-1 to a non-vulnerable algorithm, such as SHA-3 (A. K. Al-Ani, Anbar, Manickam, & Al-Ani, 2019) and UMAC (Rehman & Manickam, 2017). However, the issue with temporal DoS vulnerability requires more effort and steps to resolve, which is the subject of this research.

1.2.4 Temporal Denial-of-Service Vulnerability

Temporal denial of service (DoS) vulnerability is a type of security weakness in a network or system exploitable by an attacker to disrupt the timing behavior of a protocol and cause network performance issues or even render the system or network unavailable.

The vulnerability is called "temporal" because it involves exploiting the timing aspects of a protocol, which are critical to its proper functioning. A temporal DoS attack can target various timing-related mechanisms, such as the timestamp or the lack of it and the synchronization of clocks between devices.

The attack involves manipulating the timing aspect of the protocol used to coordinate and sequence the various events that occur within a network protocol to cause disruption and potentially render the network, system, or service unavailable.

The attacker's manipulation of the timestamps can cause chaos within the protocol, disrupting the normal flow of communication, and causing packet drop or delay, resulting in various problems, including slow network performance, connection timeouts, and even complete network failures. There are several ways that this vulnerability can be exploited, including the following:

Exploiting the lack of timestamps: Some network protocols do not include timestamps, which can make them vulnerable to temporal DoS attacks. Without timestamps, it can be challenging to determine packet order or detect anomalies in the protocol's timing behavior. An attacker could exploit this vulnerability by injecting packets into the network strategically, disrupting the protocol's normal operation and causing network performance issues or even system crashes.

Manipulating timestamps: Attackers can also exploit network protocol vulnerabilities in the timestamp generation or verification process. By altering timestamps, attackers can influence the timing behavior of the protocol, causing packet delay or drop, or process out of order, disrupting the network, and leading to degraded network performance or even network failure.

Exploiting clock synchronization issues: Many network protocols rely on clock-synchronized devices to ensure accurate and consistent timing. However, clock synchronization can sometimes be vulnerable to exploitation. For example, an attacker could introduce a clock synchronization error, causing network devices to become out of sync and disrupting the protocol's timing behavior, leading to network performance issues, dropped packets, or even system crashes.

Preventing the exploitation of these vulnerabilities requires network protocols to be designed with robust timing mechanisms that include timestamps and other measures to detect and mitigate temporal DoS attacks.

1.3 Research Motivation

Although most IP networks today still operate on a dual-stack configuration, they will not remain so and will eventually become IPv6-only networks.

Many hardware vendors and current operating systems have supported IPv6 since it became a Draft Standard in 1995 (Hagen, 2007). Additionally, the proliferation of connected devices via the Internet of Things (IoT) and Wireless Sensor Networks (WSN) further exacerbates the need for IP addresses, which, unfortunately, is beyond the current IPv4 capacity, which paves the way for IPv6.

NDP is one of the new protocols introduced by IPv6 based on ICMPv6, and it is crucial for the proper operation of IPv6 networks. NDP enables various vital functions for IPv6-enabled nodes on a link-local network, making it impossible to be disabled like ICMPv4 despite many concerns about its security (Ahmed et al., 2015; Barbhuiya et al., 2011; Zhang & Wang, 2016). Consequently, securing it becomes a high priority, and the IETF has proposed several security mechanisms to ensure NDP security, such as SEND and IPSec. However, many well-known issues with them, such as bootstrapping, susceptibility to DoS due to complexity, and high protocol overhead led to the birth of Trust-ND as an alternative.

Unfortunately, Trust-ND is also susceptible to various security issues and vulnerabilities, such as temporal DoS. Therefore, it must be addressed for Trust-ND to be viable as the alternative security mechanism to secure IPv6 link-local networks. This research attempts to fill the gaping hole left by existing studies in NDP security related to temporal DoS vulnerabilities, specifically those caused by faulty design of Trust-ND protocol.

In conclusion, link-local networks are an indispensable part of IPv6 networking, including the Internet, which is experiencing rapid adoption. As such,

research into the security of IPv6 link-local networks is more critical than ever before, given the significant role that IPv6 will play in the future of networking and the Internet.

1.4 Research Problem

NDP is inherently insecure and vulnerable to various attacks (Arkko et al., 2005; Nikander et al., 2004) and misconfigurations (Chown & Venaas, 2011). This insecurity and vulnerability are due to NDP's reliance on the plain-text ICMPv6 messages void of a robust built-in security mechanism (Elejla et al., 2017). In addition, unlike ICMPv4, it cannot be disabled or blocked without breaking the network due to its essential nature to IPv6. Consequently, the vital role of ICMPv6 in the operations of IPv6 networks creates a new enticing attack vector for malicious actors to target.

Temporal DoS or DDoS attacks target the inherent weaknesses of the NDP protocol in dealing with threats that manipulate the timing or rate of attacks, such as temporal lensing technique in pulsing DoS (Rasti et al., 2015), replay (Nikander et al., 2004), and high- or low-rate DoS attacks (Bhuyan et al., 2015). As a result, many researchers have proposed various approaches to tackle the threat of temporal DoS and DDoS on NDP (Barbhuiya et al., 2013; Elejla et al., 2017; Tayyab et al., 2020). The most efficient attack prevention approach is preventative, which addresses the inherent weaknesses of the protocol itself (Mirkovic & Reiher, 2004), such as SEND and Trust-ND. However, SEND is highly complex due to its dependency on public key cryptography and digital signatures to verify the authenticity of messages exchanged between nodes, making it vulnerable to DoS and DDoS attacks (Alsa'deh & Meinel, 2012; Supriyanto et al., 2013). Therefore, Supriyanto proposed Trust-ND (Supriyanto, 2015) as an alternative security mechanism to SEND.

However, theoretical analysis and experimental research (A. Al-Ani et al., 2022; A. K. Al-Ani, Anbar, Manickam, Al-Ani, et al., 2019; Rehman & Manickam, 2017; Thulasiraman & Wang, 2019) on the Trust-ND protocol revealed that it is susceptible to several vulnerabilities due to its design decisions. These vulnerabilities expose Trust-ND to security issues, including temporal DoS.

The problem statements are as follows:

- **Timestamp reference:** The existing Trust-ND use of the local system clock as the timestamp reference time could cause a considerable difference in the Trust-ND packets' sending and receiving times, failing verification. A computing device with a different time zone or daylight-saving settings will have a different system time than the rest (Klyne & Newman, 2002). This situation is plausible if the device is from outside the region or country or is the target of malicious actors that manipulate its clock subsystem (Langer et al., 2019; Tripathi & Hubballi, 2021).

- **Precision:** The existing Trust-ND's timestamp field size (4 bytes) and format (hexadecimal) limit the precision or granularity. A 32-bit timestamp cannot provide sufficient resolution to differentiate consecutive packets on a high-speed network (Orosz & Skopko, 2010) and run for a long time without overflowing, resulting in a rollover or wraparound (Micheel et al., 2001). The hexadecimal timestamp format used by Trust-ND requires a *string* or *char* data type, reducing the timestamp precision further.

- **Vulnerable verification rule:** Trust-ND's existing timestamp verification rule is vulnerable to DoS due to out-of-sync clocks, clock rollover or wraparound, and insufficient precision. The out-of-sync condition could occur due to DoS,

clock subsystem misconfiguration or malfunction, time zone differences, and clock drift. Using a 24-hour time format exposes Trust-ND to clock rollover or wraparound every midnight when the time changes from 23:59:59.99 to 00:00:00.00 (Mizrahi T. et al., 2020). Meanwhile, coupled with Trust-ND's inadequate precision and high-speed networks, its verification rule cannot distinguish two timed events that occur in a shorter period than the precision, leading to packet drop. On a link with full 1 Gbps speed, the timestamp difference between two consecutive 64-byte frames, which is the smallest Ethernet frame length, claims nanosecond (10^{-9}) precision resolution, notably 608 ns, while the largest frame length (1518-byte) is in the microsecond's domain (Orosz & Skopko, 2010).

1.3 Research Objectives

The primary goal of this research is to enhance Trust-ND to prevent temporal DoS vulnerabilities on IPv6 link-local networks. The following objectives are defined to facilitate achieving the goal.

1. To propose a new Trust-ND timestamp reference with enhanced timestamp format and precision (RO1).

2. To propose a mechanism to precisely represent the timestamp in the enhanced Trust-ND message that accommodates the new timestamp without jeopardizing the original Trust-ND packet structure (RO2).

3. To propose a rule-based timestamp verification mechanism to prevent temporal DoS vulnerabilities on IPv6 link-local networks (RO3).

1.5 Research Scope and Limitations

The scope of the research is limited to prevent temporal DoS vulnerabilities resulting from the faulty design of the Trust-ND's timestamp and its utilization on IPv6 link-local networks. Table 1.1 lists the rest of the scope and limitations of this research.

Table 1.1 Research scope and limitations

Scope	Limitation
Environment	IPv6 link-local network
Vulnerability	Temporal DoS vulnerability
Vulnerability Classification	DoS, Bug exploitation, internal attack
Protocol and Messages	Trust-ND (Trust-NA and Trust-NS messages)
Trust-ND Process	Duplicate Address Detection (DAD)
OSI Target Layer	Network Layer

1.6 Research Contributions

The main contribution of this research is an enhanced Trust-ND protocol to prevent temporal DoS vulnerabilities on IPv6 link-local networks due to improper design and utilization of Trust-ND's timestamp. The contributions of this research to the body of knowledge are as follows:

1. A new Trust-ND timestamp reference with enhanced timestamp format to prevent temporal DoS vulnerabilities. The proposed timestamp utilizes UTC as a reference instead of the system clock, allowing the timestamp format to change from human-readable hexadecimal to machine-readable integer, which is more efficient.

2. A proper packet structure of the enhanced timestamp with increased precision by increasing the timestamp field size via repurposing the Reserved field in Trust-ND to avoid jeopardizing the original Trust-ND packet structure.

3. A rule-based timestamp verification mechanism that considers time differences to prevent temporal DoS vulnerabilities of the Trust-ND protocol.

Table 1.2 maps the research problems, objectives, and contributions.

Table 1.2 Mapping between research problems, research objectives, and research contributions

Problems	**Research objectives**	**Research contribution**
Using local system time as the timestamp reference could cause unsynchronized clocks with considerable differences between the timestamps of Trust-ND packets and arrival times, resulting in temporal DoS vulnerabilities. In addition, using 12-hour or 24-hour timestamp subjected Trust-ND timestamp to clock rollover or wraparound.	RO1	RC1
Trust-ND cannot distinguish two subsequent packets in a high-speed network due to insufficient timestamp precision caused by the size of the timestamp field (4-byte) and its format (hexadecimal).	RO2	RC2
The Trust-ND's timestamp verification rule is susceptible to DoS vulnerabilities when involving unsynchronized clocks.	RO3	RC3

RO = Research Objective, RC= Research contribution

1.7 Research Steps

This section outlines the process undertaken in this research to achieve the stated objectives. This research comprises five steps, as explained below and visualized in Figure 1.4.

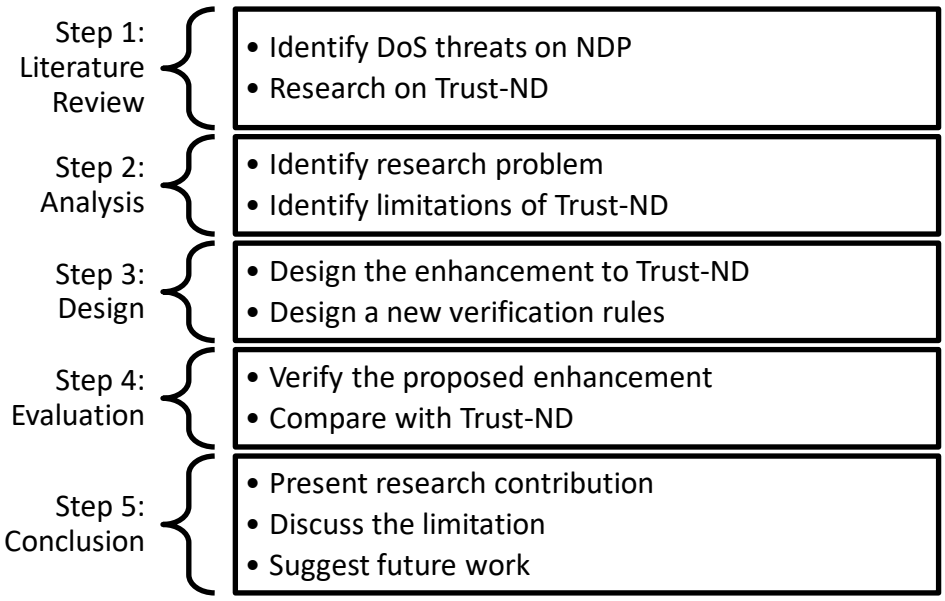

Figure 1.3 Research Steps

Step 1: Literature Review involves a background study related to the Trust-ND, such as an overview of the IPv6, NDP, and SEND. Also covered in the study are some common attacks against the NDP processes, the DAD process, some timestamping formats in different protocols, common issues with the timestamp, and existing solutions to timestamp issues.

Step 2: Analysis dissects, analyzes, and discusses the Trust-ND mechanisms in securing the IPv6 link-local communication, focusing on timestamp utilization. This step identifies the advantages and limitations of Trust-ND to provide insights into areas needing fixing or enhancement.

Step 3: Design enhances the Trust-ND security to protect IPv6 hosts exposed to temporal DoS vulnerabilities in IPv6-only link-local networks.

Step 4: Evaluation measures or calculates and compares the proposed mechanism's performance against Trust-ND for processing time, bandwidth utilization, and susceptibility to DoS vulnerabilities.

Step 5: Conclusion presents the research findings, suggestions for future research, and the known limitations of the proposed mechanism.

1.8 Thesis Organization

This thesis comprises six chapters. Chapter 1 introduces the research topic, and the organization of the subsequent chapters is as follows:

Chapter Two critically reviews existing literature on security mechanisms and techniques used or proposed to secure NDP, focusing on the soft security approach.

Chapter Three discusses the methodology of the proposed mechanism and elaborates on its requirements.

Chapter Four analyses the proposed mechanism, its mechanisms, and its conceptual design and implementation.

Chapter Five compares the performance of the enhanced Trust-ND with the original Trust-ND and the standard NDP.

Chapter Six summarizes the findings of this thesis. The chapter also suggests several recommendations for future work and lists a few known limitations of the proposed eTrustND.

CHAPTER 2

LITERATURE REVIEW

This chapter presents the background of the research (Section 2.1), reviews related works in the literature (Section 2.2), and critically analyzes the existing approaches for weaknesses and security issues (Section 2.3) to identify research gaps (Section 2.4). Finally, the last section (Section 2.5) summarizes this chapter.

2.1 Background

This section provides the background of Neighbor Discovery Protocol, SEND, Trust-ND, different timestamp formats by network protocols with its issues, and the existing solution to those issues.

2.1.1 NDP

NDP was first described in RFC2461 and updated by RFC4861 in 2007 (Narten et al., 2007). It is one of the core IPv6 protocols supporting the essential processes and functionalities that rely on IPv6 nodes' communication within IPv6 link-local networks. For example, it enables local IPv6 nodes to find routers, discover each other's presence, generate their IP addresses and ensure their uniqueness, determine their link-layer addresses, and keep track of active neighbors' reachability status. NDP utilizes five ICMPv6 messages to perform its operations: Router Solicitation (RS), Router Advertisement (RA), Neighbor Solicitation (NS), Neighbor Advertisements (NA), and Redirect messages. Table 2.1 lists the five ICMPv6 messages utilized by NDP.

Table 2.1 ICMPv6 messages utilized by NDP

Message	Message Type	Description
Router Solicitation (RS)	133	IPv6 hosts use RS to inquire about router(s) in a link-local network.
Router Advertisement (RA)	134	Routers periodically send RA to advertise their presence in the link-local network or respond to RS sent by hosts. Also used by routers to propagate network parameters, such as prefixes,
Neighbor Solicitation (NS)	135	IPv6 nodes send NS messages to request a target node's link-layer address while providing their link-layer address to the target.
Neighbor Advertisement (RA)	136	IPv6 nodes send NA messages to respond to NS messages. Nodes also use unsolicited NA messages to propagate new information to neighbors quickly.
Redirect	137	A router sends a Redirect packet to inform the IPv6 host of a better first-hop node on the path to a destination or inform a host that the destination is its Neighbor.

Unfortunately, the NDP standard has no default security mechanism except for the IPv6 address scope (Haberman et al., 2005) to prevent external threats. However, without a security mechanism to protect the network from insider threats, the local IPv6 nodes remain exposed to various attacks, such as DoS and DDoS, MiTM, replay, and spoofing (Mohamed Sid Ahmed et al., 2017; Nikander et al., 2004; Supriyanto, 2012; Supriyanto et al., 2013).

Unlike ICMPv4 messages in IPv4, disabling NDP messages is not an option without breaking the IPv6. Therefore, to deal with insider threats, the NDP standard recommends Secure Neighbor Discovery (SEND) (Arkko et al., 2005) or IPSec (Frankel & Krishnan, 2011). However, bootstrapping problem restricts the use of IPSec to small IPv6 networks with a few hosts since it requires manual configuration of each host's Security Associations (SA), which is tedious and unrealistic for extensive networks (Alsa'deh & Meinel, 2012; Anbar et al., 2017).

2.1.1(a) NDP Duplicate Address Detection Process

One of the vital NDP processes is the Duplicate Address Detection (DAD) process, which ensures that no network interfaces in a local network are assigned duplicate unicast IPv6 addresses. All IPv6 nodes must perform this process before an interface is assigned any unicast address, regardless of whether via stateless autoconfiguration (SLAAC), DHCPv6, or manual configuration.

A node using SLAAC runs the DAD process before assigning the address to its interface. Meanwhile, a manually assigned node uses the DAD process to verify that the address is not used on the local link. However, a DHCPv6 client may request that the DHCPv6 server perform DAD on the assigned address on its behalf.

However, the specification lists three exceptions: First, when an interface's DupAddrDetectTransmits variable is zero. Second, anycast addresses (note that it is impossible to distinguish anycast addresses from unicast addresses syntactically). Third, each node SHOULD test each unicast address for uniqueness. It is worth noting that some implementations only perform DAD for the link-local address and not the global address that shares the same interface with the link-local address for performance optimization. Although the NDP specification does not recommend such implementations, it does not prevent it either, but new implementations must not do such optimization (Thomson Narten T. and T. Jinmei, 2007).

A node executes the DAD process only once using a single NS message for each IPv6 address it attempts to assign to its interface. If there is no response to the NS message within 1 second, as per RFC4862 (Thomson Narten T. and T. Jinmei, 2007), the address is considered unique, and the node assigns it to its interface. Once the address is assigned successfully, the DAD process is not run again for that particular address unless the address is removed from the interface and reassigned later.

2.1.1(b) Common Attacks Against the NDP Process

The lack of a robust default security mechanism for NDP exposes local IPv6 networks to many threats and attacks, such as DoS and DDoS, spoofing, masquerading, redirect, replay, and Man-in-the-Middle (MitM) attacks (A. K. Al-Ani, Anbar, Manickam, Wey, et al., 2019; Najjar et al., 2015; Nikander et al., 2004; Supriyanto, 2012). However, malicious user or agent is not the only source of threats but also unintentional misconfiguration by users or administrators, leading to many rogue router incidents that resulted in the publication of RFC6104 (Chown & Venaas, 2011) titled "Rogue IPv6 Router Advertisement Problem Statement."

DoS attack is the second most common attack recorded in the Common Vulnerabilities and Exposure (CVE®) database since 1999 after code execution (44,266 vs. 28,960 incidents). More than half (52 %) of reported software vulnerabilities listed in the MITRE's 2022 Top 25 Most Dangerous Software Weaknesses (CWE™ Top 25) list (MITRE, 2022) could cause DoS, affecting the availability of applications and services. CWE™ Top 25 lists the most common and impactful software weaknesses that are usually easy to find and exploit. These weaknesses could lead to exploitable vulnerabilities that allow adversaries to break into the system, steal data, or force the software to stop functioning.

Temporal DoS vulnerability allows adversaries to exploit the protocol's time component or absence to disrupt the computer system or network. An adversary could manipulate the timing of certain events, actions, or behavior of the protocol, such as in the case of temporal lensing DoS (Rasti et al., 2015) and low- and high-rate DoS (Bhuyan et al., 2015) attacks. The vulnerabilities could be due to malicious activity, the inability of network devices to handle an extreme load (Ramanauskaite & Cenys, 2011), or the exposure of a poorly designed network protocol (Handley et al., 2006).

2.1.2 Secure Neighbor Discovery (SEND)

The NDP standard explicitly recommends SEND, described in RFC3971 (Arkko et al., 2005), as one of the security mechanisms for securing NDP, making it the standard security benchmark for IPv6 link-local networks. It enhances NDP security by introducing a message integrity function, an address ownership proof, and a new router authorization mechanism (AlSa'deh et al., 2013; Shah, 2019).

SEND specified four new Neighbor Discovery options to provide all those enhancements: Cryptographically Generated Address (CGA), RSA Signature, Timestamp, and Nonce. It also introduced a new mechanism to protect router discovery operations by introducing a trusted anchor concept, which relies on two new messages: Certification Path Solicitation (CPS) and Certification Path Advertisement (CPA).

SEND's computational complexity and deployment challenges are well-documented and extensively studied (Gelogo et al., 2011). For example, researchers discovered, empirically and theoretically, that the CGA generation and RSA signature processes are the sources of SEND's complexity (Alsa'deh & Meinel, 2012; An et al., 2007), exposing it to CPU exhaustion attacks (Pohl, 2007). In addition, adding new options to the existing NDP messages affects the protocol overhead and bandwidth utilization since the four newly introduced SEND options increase each NDP message by at least 368 bytes (An et al., 2007; Supriyanto, 2012).

2.1.2(a) SEND Timestamp Option

SEND introduced the Timestamp Option to ensure unsolicited advertisements and redirects are not replayable, preventing some DoS, MiTM, and replay attacks.

The SEND's Timestamp Option consists of four fields: Type, Length, Reserved, and Timestamp. The Timestamp field is a 64-bit unsigned integer, which

holds the value of epoch seconds, or seconds since 00:00:00 UTC on 1 January 1970, in a fixed-point format and is divided into two parts. The first 48 bits contain the second's value, and the remaining 16 bits represent the 1/64K fractions of a second. Figure 2.8 depicts the four fields in the SEND's Timestamp Option structure.

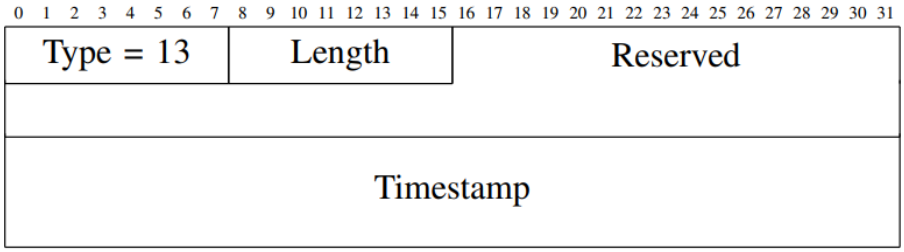

Figure 2.1 SEND Timestamp Option structure

2.1.2(b) SEND Timestamp Verification

SEND specification dictates receivers define a timestamp Delta (δ) value, a "fuzz factor" for comparisons, and an allowed clock drift parameter. The default value for δ is 300 seconds or 5 minutes; for the fuzz factor is 1 second; for clock drift, 1 % of the fuzz factor, or 0.01 second (Arkko et al., 2005).

SEND requires receivers to check the Timestamp option after receiving a message from a new peer for the received timestamp, TS_{new}, and accept it if the timestamp is recent enough to the packet's reception time, RD_{new}.

$$-\delta < RD_{new} - TS_{new} < +\delta$$

The receiving host SHOULD store the RD_{new} and TS_{new} values in the cache as RD_{last} and TS_{last}.

2.1.3 Trust-ND

The high complexity of SEND leads Supriyanto to propose Trust-ND (Supriyanto, 2015) as a comprehensive, integrated, and decentralized security mechanism to secure NDP.

2.1.3(a) Trust-ND Improvement to SEND

As mentioned in Section 2.1.1(a), SEND is well known to demand high computational resources due to its complexity – a fact readily admitted by SEND authors themselves (Arkko et al., 2005). Trust-ND eliminates the sources of SEND complexity, which are the CGA and RSA Signature options. Removing SEND's RSA Signature option is necessary since its generation and verification are the primary sources of computationally expensive operations in SEND.

Additionally, the confidentiality of the node's IPv6 address is unnecessary for the operation of NDP. The NDP message content should be transparent for neighbors to consume, especially for neighbor discovery, router discovery, and duplicate address detection processes.

Trust-ND replaced the cryptographic-based options in SEND with Secure Hash Algorithm 1 (SHA-1), an unkeyed hash function, to ensure the integrity of its messages. However, it retained two SEND options, Timestamp and Nonce, but represented them differently as fields within the Trust Option instead of separate individual options. This format sheds off several hundred bytes from the SEND packet and thus reduces the protocol overhead and bandwidth utilization for Trust-ND while benefiting from timestamp and Nonce.

Removing and replacing four SEND options (368 bytes) with a single 32-byte Trust Option reduces each NDP packet's size by 336 bytes, significantly reducing protocol overhead and bandwidth utilization for Trust-ND compared to SEND (Supriyanto, 2015).

2.1.3(b) Trust-ND Packet Structure

Trust Option follows the format of the ICMPv6 option in the form of the Type-Length-Value convention. Figure 2.2 illustrates the complete structure of the Trust-ND packet with IPv6 and NDP headers.

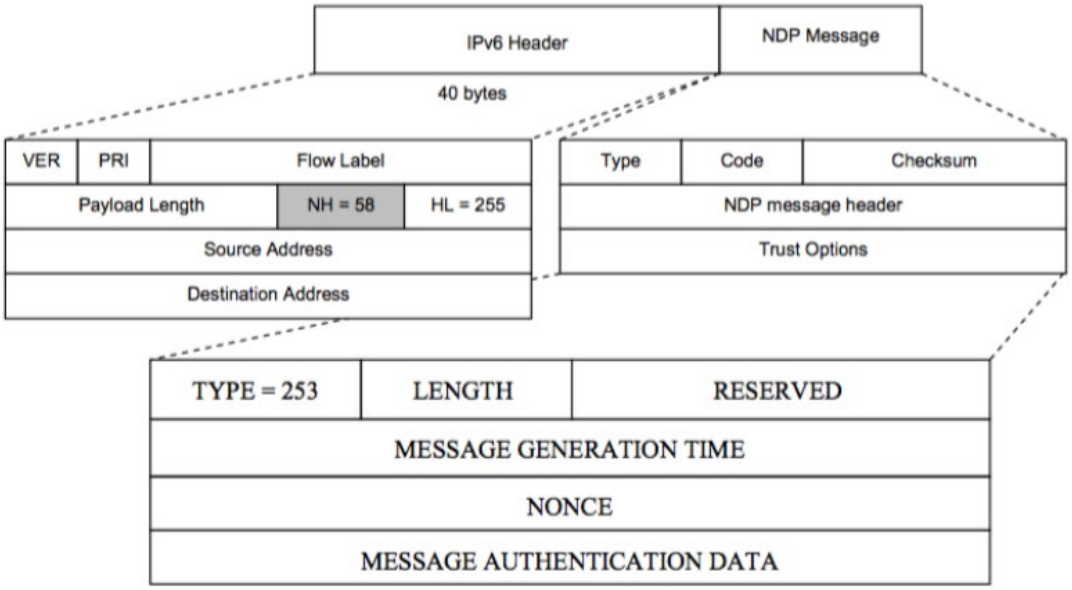

Figure 2.2 Trust-ND packet with IPv6 and NDP headers (Supriyanto, 2015).

Figure 2.3 shows the structure of the Trust Option incorporated into all Trust-ND messages.

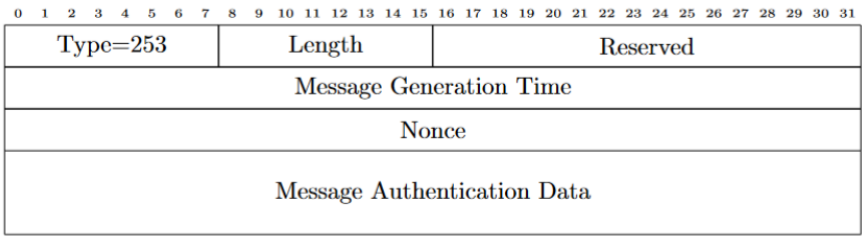

Figure 2.3 Trust-ND's Trust Option structure

The TYPE field is a 1-octet identifier indicating the type of ICMPv6 option the NDP message carries. Trust-ND uses a value of 253 since this is an officially allocated