THE DYNAMIC HOST CONFIGURATION PROTOCOL VERSION 6 SECURITY AND PRIVACY MECHANISM

AYMAN KHALLEL IBRAHIM

UNIVERSITI SAINS MALAYSIA

2020

THE DYNAMIC HOST CONFIGURATION PROTOCOL VERSION 6 SECURITY AND PRIVACY MECHANISM

by

AYMAN KHALLEL IBRAHIM

Thesis submitted in fulfillment of the requirements
for the degree of
Doctor of Philosophy

June 2020

ACKNOWLEDGEMENT

I thank all who in one way or another contributed in the completion of this research. First, I give thanks to "Allah" for protection and the ability to do this research. I would like to give sincere thanks to the lecturers and collegemates at the National Advanced IPv6 Center, the librarians, and other workers of the Center for their kind help during my Ph.D. journey, without you all, I will not be able to achieve this research.

My special and heartily thanks to my research supervisor, Dr. Mohammed Anbar, and co-supervisors Professor Dr. Rosni Abdullah. Without their assistance and dedicated involvement in every step throughout the process, this research would have never been accomplished. I would like to thank you very much for your support and understanding over these past three years.

Getting through my research required more than academic support, and I have many, many people to thank for to and, at times, having to tolerate me over the past three years. I cannot begin to express my gratitude and appreciation for their friendship. For many memorable evenings out and in, I must thank; Dr. Kamal Alieyan, Dr. Abdullah Shirari, and Dr. Shams alearifin have been unwavering in their personal and professional support during the time I spent at the USM university.

Most importantly, none of this could have happened without my family. My life-coach "My Father" Prof. Khallel Ibrahim. Al-Ani, I really do not have any word to explain my thanks for your assistance to make me where I am now, without you, Dad, I am literally nothing. My lightness in this life "My Mother," who encouraged me and prayed for me throughout the time of my research. And lastly, thanks to my brothers Dr. Ahmed Al-Ani and Fahad Al-Ani and my lovely three sisters. I love you all…

Finally, I would like to express my thanks to the unknown soldier who supports me without notice. May the Almighty God richly bless all of you. I dedicate this work to all of you.

Ayman Khallel Al-Ani, Penang Malaysia, 2020.

TABLE OF CONTENTS

LIST OF TABLES

Page

LIST OF FIGURES

LIST OF ABBREVIATIONS

AES	Advanced Encryption Standard
APSR	Attack Prevention Success Rate
AEAD	authenticated encryption with associated data
ADD	Authorization Delegation Discovery Mechanism
ACDA	Auto-configuration Detecting Attacks
Avg.	Average
BYOD	Bring-Your-Own-Device
CPU	Central Processing Unit
CBC	Cipher Block Chaining
CPK	Client Public Key
CGAs	Cryptographically Generated Address
DAP	Delayed Authentication Protocol
DoS	Denial-of-Service
DSAUDC	DHCP Server Authentication Using Digital Certificates
DUID	DHCP unique identifier
DHCPv6Sec	DHCPv6 Security
DPK	DHPCv6 Public Key
DDoS	Distributed Denial of Service
DNS	Domain Name System
DHCPv4	Dynamic Host Configuration Protocol version 4
DHCPv6	Dynamic Host Configuration Protocol version 6
ECB	Electronic Code Book
ECDH	Elliptic Curve Diffie-Hellman

E	Encrypted
GCM	Galois Counter Mode
GRK	Generator Reconfigure Key
HMAC	Hash Message Authentication Code
IANA	Internet Assigned Numbers Authority
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPSec	IP security
KDA	Key Distribution and Authentication
MITM	man-in-the-middle
Max	Maximum
MTU	maximum transmission unit
Min	Minimum
NAv6,	National Advanced IPv6 Centre
NIST	National Institute of Standards and Technology
NFG	Network Flow Guard
NIC	Network interface card
NTP	Network Time Protocol
PM	Pervasive Monitoring
P-DHCP	Protect DHCP
RK	Reconfigure Key
RKAP	Reconfigure Key Authentication Protocol
RIRs	Regional Internet Registries
RD	Replay Detection
RFC	Request for Comments

RSA	Rivest–Shamir–Adleman
RA	Router Advertisement
SEND	Secure neighbor discovery protocol
SDUC	Secure-DHCPv6 Using CGAs
SDURA	Secure-DHCPv6 Using RSA Authentication
SIP	Session Initiation Protocol
SAVI	Source Address Validation Improvement
SD	standard deviation
THC	The Hackers Choice
USD	United States dollar
USM	Universiti Sains Malaysia
UDP	User Datagram Protocol

LIST OF APPENDICES

MEKANISME KESELAMATAN DAN PRIVASI PROTOKOL KONFIGURASI HOS DINAMIK VERSI 6

ABSTRAK

Protokol Internet versi 6 (IPv6) merupakan versi IP terkini yang bertujuan menampung ratusan ribu alamat IP yang unik untuk peranti dalam rangkaian pautan tempatan yang sama. Dalam rangkaian pautan rangkaian tempatan IPv6, Protokol Konfigurasi Hos Dinamik untuk IPv6 (DHCPv6) digunakan untuk memperuntukkan dan mengedarkan alamat IPv6 dan parameter konfigurasi rangkaian kepada pelanggan DHCPv6. Walau bagaimanapun, protokol DHCPv6 telah dibangunkan tanpa pendekatan keselamatan yang baik menyebabkan ia terdedah kepada pelbagai ancaman, seperti serangan pelayan DHCPv6 jahat dan serangan pasif. Dua isu DHCPv6 yang dimaklumi adalah ketiadaan mekanisme penyahihan yang membolehkan penyerang menyuntik parameter konfigurasi rangkaian palsu ke dalam rangkaian tanpa dikesan; dan isu privasi kerana tiada perlindungan terhadap maklumat pelanggan atas talian. Untuk menangani isu-isu ini, beberapa pendekatan telah dicadangkan oleh penyelidik untuk menyediakan perlindungan penyahihan dan privasi untuk DHCPv6. Walau bagaimanapun, kebanyakan pendekatan tidak mempunyai mekanisme untuk mengedarkan watikah penyahihan pelayan; dan mengabaikan isu privasi pelanggan. Tesis ini bertujuan menangani isu-isu tersebut di atas dengan mencadangkan DHCPv6Sec. DHCPv6Sec mempunyai tiga peringkat: penjanaan kekunci pelayan awam dan persendirian DHCPv6; saling berhubung menggunakan mesej DHCPv6Sec; dan proses mesej *Reconfiguration* DHCPv6Sec. DHCPv6Sec telah dinilai dan dibandingkan dengan pendekatan Secure-DHCPv6 dari segi keupayaan pencegahan pelayan DHCPv6 jahat, perlindungan privasi, masa pemprosesan, overhed trafik, masa komunikasi, dan had saiz mesej DHCPv6. Prestasi

setiap pendekatan dinilai menggunakan senario eksperimen yang berbeza. Keputusan eksperimen menunjukkan bahawa DHCPv6Sec lebih unggul dalam semua aspek yang diukur. DHCPv6Sec menjimatkan masa pemprosesan sehingga 25.15 milisaat semasa proses mendapatkan alamat IPv6 dan sehingga 6.21 milisaat semasa pemprosesan mesej *Reconfiguration* berbanding pendekatan Secure-DHCPv6. Selanjutnya, DHCPv6Sec mengurangkan masa konfigurasi sebanyak 27.27% berbanding pendekatan Secure-DHCPv6. Pendekatan DHCPv6Sec tidak meletakkan had pada saiz mesej DHCPv6, bukan seperti pendekatan Secure-DHCPv6. DHCPv6Sec juga mempunyai overhed trafik yang lebih rendah (4068 KB) berbanding dengan Secure-DHCPv6 (1036 KB).

THE DYNAMIC HOST CONFIGURATION PROTOCOL VERSION 6 SECURITY AND PRIVACY MECHANISM

ABSTRACT

Internet Protocol version 6 (IPv6) is the most recent IP version that aims to accommodate hundreds of thousands of unique IP addresses for devices in the network. In IPv6 network, Dynamic Host Configuration Protocol version IPv6 (DHCPv6) is used to allocate and distribute IPv6 addresses and network configuration parameters to DHCPv6 clients. However, the DHCPv6 protocol was developed without a proper security mechanism making it vulnerable to various threats, such as rogue DHCPv6 server attack and passive attack. Two well-known issues of DHCPv6 are lack of verification mechanism that allows attackers to inject fake network configuration parameters into the network undetected; and privacy concerns due to lack of protection of client information in transit. In order to address these issues, several mechanisms were proposed by researchers to provide authentication and privacy protection for DHCPv6. However, most mechanisms lack the method to distribute the server authentication credentials; and ignore the client's privacy issue. This thesis intends to address the above mentioned issues by proposing DHCPv6Sec mechanism. DHCPv6Sec was evaluated and compared to Secure-DHCPv6 mechanism in terms of rogue DHCPv6 server prevention capability, privacy protection, processing time, traffic overhead, communication time, and message size limitation. The experiment results showed that DHCPv6Sec is superior in all aspects measured. DHCPv6Sec reduced processing time by 57%, and 136% during obtain IPv6 address and processing of Reconfigure message, respectively, compared to Secure-DHCPv6 mechanism. More, DHCPv6Sec reduced configuration time by 27% compared to Secure-DHCPv6 mechanism. DHCPv6Sec mechanism did not put a limit on the

DHCPv6 message size, unlike Secure-DHCPv6 mechanism. The DHCPv6Sec also has less traffic overhead 1036 Kb compared to Secure-DHCPv6 4068 Kb.

CHAPTER 1

INTRODUCTION

1.1 Overview

Nowadays, the Internet is widely used in various fields such as industries, education, marketing, and medicine (Fierro, Cardona Arbelaez, & Gavilanez, 2017). The Internet is the largest system ever built by humans, and it has become an important part of daily life. It provides access to information anytime and anywhere. In addition, it allows people to communicate with one another (Sameera & Vishwakarma, 2019; Zhao, 2018). The Internet makes life easier and more comfortable now more than before. Consequently, the number of Internet users has exponentially grown over the last five years. Recent research shows that more than 4.39 billion people are connected to the Internet (Reichelt, 2019).

The number of Internet security issues keeps increasing and becoming more damaging due to the growing number of Internet users and the advantages of connecting online (Elavarasi & Elango, 2017). Internet security issues could cost millions or billions of dollars depending on the size and target of the attack. According to BofA Merill Lynch Global Research, Internet security issue costs the global economy up to USD 575B annually (Rahman et al., 2017). The report indicates that in a potential worst-case 2020 “Cybergeddon” scenario, Internet security issue could extract up to a fifth of the value created by the Internet (Symantec, 2015).

The unexpected growth of the number of Internet users has resulted in the exhaustion of the Internet Protocol version 4 (IPv4) address pool. Therefore Internet Protocol version 6 (IPv6) is proposed to overcome the IPv4 address exhaustion issue

(Ren et al., 2019; Samad et al., 2018). The following section presents the background of IPv6.

1.2 Background

IPv4 has been used since the beginning of the Internet era to uniquely identify each node on the Internet. However, the recent exponential increase in the number of Internet-facing devices has resulted in all Regional Internet Registries (RIRs) to run out of allocatable IPv4 addresses (Pickard et al., 2017, 2018) . IPv6 is the upcoming version of Internet Protocol that will replace IPv4. Reports in 2018 of Internet trends reveal a substantial increase in IPv6 usage (Internet Society, 2018). Google statistic shows that IPv6 usage had increased from 6% in 2015 to around 26% in April 2019, indicating an upward trend of IPv6 usage that will surpass IPv4 usage in the future. Figure 1.1 shows the percentage of Internet users that access Google services using IPv6 compared to IPv4 (Pickard et al., 2019).

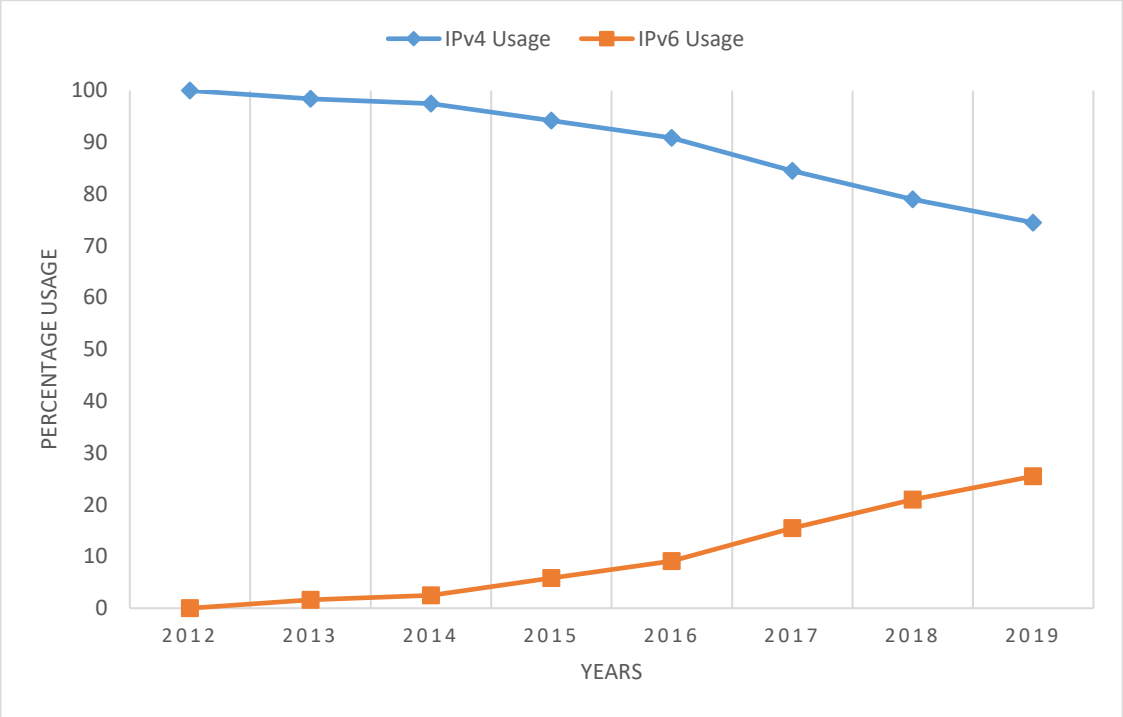

Figure 1.1: Percentage of IPv6 Traffic Accessing Google Services.

IPv6 slightly improves the security of the network, as well as service quality. It brings improvements in terms of simplicity, routing speed, quality of service, and security over IPv4 (Kristadi & Sucahyo, 2017). However, IPv6 also introduces new security issues that need to be solved. One of these security issues is related to the Dynamic Host Configuration Protocol version 6 (DHCPv6).

IPv6 has two standard mechanisms to configure IPv6 address of the client which are DHCPv6 and stateless auto-configuration (SLAAC) (Ruiz et al., 2017; Yousheng et al., 2018). However, DHCPv6 provides the network administrator with more control on the network compared to SLAAC mechanism (Anbar et al., 2018). The following section highlights the security issues related to DHCPv6.

1.2.1 Dynamic Host Configuration Protocol version 6 (DHCPv6)

In IPv6 network, DHCPv6 server is typically deployed to assign IPv6 addresses and distribute network configuration parameters, such as Network Time Protocol

(NTP) server address, Session Initiation Protocol (SIP) server address, and Domain Name System (DNS) server address to DHCPv6 clients (Barreto, 2015). DHCPv6 is similar to Dynamic Host Configuration Protocol version 4 (DHCPv4) in the IPv4 network in term of functionalities. However, the message formats are different, and both are vulnerable and susceptible to different types of attacks. For example, DHCPv4 is susceptible to starvation attack but not DHCPv6 because of the availability of a huge amount of IPv6 addresses at its disposal (Huitema et al., 2016). Besides, DHCPv6 treats client privacy differently than DHCPv4. DHCPv6 client uses the client's DHCP unique identifier (DUID), which has potential privacy issues, whereas DHCPv4 is optional to use it (Krishnan, Mruthe galski, & Jiang, 2016). Therefore, most of DHCPv4 security mechanisms cannot be applied directly to DHCPv6.

DHCPv6 has two modes of operation: stateful and stateless. The stateful mode is utilized to allocate and assign IPv6 addresses and distribute other network configuration parameters. Whereas, the stateless mode is used to only distribute the network configuration parameters. Therefore, DHCPv6 plays a vital role to serve the host in IPv6 link-local network, and it is widely used and deployed nowadays (L. Li et al., 2018). The following section highlights the most common security issues of DHCPv6 such as a rogue DHCPv6 server and privacy.

1.2.1(a) Rogue DHCPv6 Server Issue

As mentioned above, DHCPv6 server is responsible to assign IPv6 address and distribute network configuration parameters to clients that are connected to IPv6 link-local network (Abdullah, 2019). The client configures its own network interface card (NIC) with IPv6 address and other network configuration based on the information in the DHCPv6 server message it receives without any verification to check whether the

message originated from legitimate source or not, such as from a rogue DHCPv6 server. A malicious node located on the same network could masquerade as a DHCPv6 server by responding to client messages with incorrect network configuration parameters, such as fake DNS and NTP addresses. Since the client does not have any mechanism to verify the legitimacy of DHCPv6 server messages, the client will unknowingly configure its NIC with incorrect network information that is received from the network. This kind of attack is called a rogue DHCPv6 server attack (Abdulla, 2017; L. Li et al., 2018). As a result, the attackers could redirect the client's traffic to rogue servers such as DNS and NTP servers or conduct Denial-of-Service (DoS) attack.

Furthermore, DHCPv6 also provides the server with Reconfigure message that allows the server to reconfigure the client with new network configuration parameters. However, the attacker could also exploit this feature to reconfigure the client anytime. Therefore, the authentication of DHCPv6 server message is a very important feature in the IPv6 network.

1.2.1(b) DHCPv6 Client's Privacy Issue

All DHCPv6 messages are transmitted in plain text, which may put the privacy of the client at risk by disclosing personal information. This information includes several identifiers such as Client's DHCP Unique Identifier (DUID) and hostname. By monitoring the DHCPv6 messages, the attacker can use these identifiers as a stable identifier to the DHCPv6 client for tracking and profiling users and their activities over time. A stable identifier is an immutable unique information that does not change over time, and it can be used to distinguish one client from another.

Moreover, this information can be used to digitally fingerprint a client as it reveals the device type, the vendor name or the operating system type and version. This information could be used by attackers to track their victims and to learn of the potential vulnerabilities of the device or the operating system for exploitation. Besides, attackers that monitor DHCPv6 traffic through passive monitoring could obtain the hostname, the operating system, and vendor name of all DHCPv6 clients in the network. They could correlate such information with other information, such as from those extracted from traffic analysis and other sources that could potentially reveal the device, its properties, and user. Additionally, the DHCPv6 message could also be used to discover the networks that had been visited by the device previously. Therefore, the client's privacy is disclosed due to DHCPv6 messages being transmitted in plain text (Krishnan et al., 2016). Therefore, the privacy of the DHCPv6 client is extremely important in the IPv6 network.

1.3 Problem Statement

DHCPv6 protocol is used to configure IPv6 addresses of IPv6 hosts (clients) and distribute network configuration parameters. In the protocol standard, no effective authentication mechanism exists to allow IPv6 client to verify the messages it received originated from a legitimate server or not, thereby leaving the client vulnerable to rogue DHCPv6 server attack (Mrugalski et al., 2018). Furthermore, DHCPv6 messages are transmitted in plain text, thus could disclose critical and identifiable information related to the client, such as DUID which may expose the client's privacy (Krishnan et al., 2016).

Several mechanisms have been proposed to prevent rogue DHCPv6 server attack and to protect the client's privacy. Generally, these mechanisms can be

categorized into two groups: authentication and privacy. Most authentication mechanisms such as (Jiang & Shen, 2012) and (Su et al., 2011) lack a method to manage and distribute server authentication credentials, thus are forced to distribute the credentials manually which make the management and deployment difficult in large-scale networks. Furthermore, due to the importance of authentication of Reconfigure message, which allows the server to reconfigure the client anytime, the standard DHCPv6 provides an mechanism called Reconfigure Key Authentication Protocol (RKAP) to authenticate Reconfigure DHCPv6 message (Mrugalski et al., 2018). However, the authentication credential is transmitted in plaintext, similar to the DHCPv6 Reconfigure message, which exposes the authentication process to hijacking and spoofing.

Meanwhile, there are two privacy mechanisms: Anonymity Profile and Secure-DHCPv6. Anonymity Profile protects client's privacy by anonymizing DHCPv6 client in the network (Huitema et al., 2016). It protects client privacy by randomizing the client's DUID and not using some DHCPv6 options to deny an attacker the ability to track and profile DHCPv6 clients. However, Anonymity Profile reduces some of the DHCPv6 functionalities, such as troubleshooting and providing proper configuration to clients, thus making it unsuitable in many situations.

Due to the limitation and drawback of Anonymity Profile, Li, and et al. proposed Secure-DHCPv6 to provide authentication and to protect the privacy of DHCPv6 clients (L. Li et al., 2018) by anonymizing DHCPv6 clients to the attackers. The Secure-DHCPv6 mechanism also provides a method to distribute server authentication credential by using two extra DHCPv6 messages. However, these extra messages increase the configuration time for the host to obtain an IPv6 address. Secure-DHCPv6 also increases computational complexity and puts a limit on the size of DHCPv6

message as this mechanism utilizes asymmetric key encryption algorithm, which has high computational complexity and not designed to encrypt a big message (Asaduzzaman et al., 2015; Rahouma, 2016, 2017).

The problems can be summarized as follows:

1. Most server authentication mechanisms do not provide an authentication credential distribution method thus require manual distribution.
2. The credential to authenticate Reconfigure message is transmitted in plaintext.
3. The privacy mechanisms either reduce some DHCPv6 functionalities or increase the computational complexity, configuration time, and limit the DHCPv6 message size.

1.4 Research Objectives

The main goal of this research is to propose an mechanism to improve the DHCPv6 security and privacy in IPv6 link-local network. The following objectives are identified to achieve the main goal of this research:

- To propose an efficient way to distribute and manage server authentication credential
- To propose a method to prevent rogue DHCPv6 server attack and protect the client's privacy.
- To improve the authentication method of the DHCPv6 Reconfigure message.

1.5 Research Contribution

IPv6 is considered as the backbone of the future Internet; however, it is prone to rogue DHCPv6 server attack because the client does not have any means to verify the source of a DHCPv6 server message. Furthermore, the DHCPv6 message may expose client information that could lead to a violation of the client's privacy. This research contributes to the prevention of rogue DHCPv6 server attack and protection of the client's privacy in the following manner:

- A method to distribute server authentication credential to DHCPv6 clients without using extra DHCPv6.
- A method to prevent rogue DHCPv6 server attack and protect the client's privacy with improved performance in term of processing time, traffic overhead and without putting a limit to DHCPv6 message size.
- An improved authentication method of the DHCPv6 Reconfigure message.

1.6 Research Scope and Limitations

In this research, the research scope of the designed security mechanism is limited to the protection of IPv6 link-local network against rogue DHCPv6 server attack and protection of the client's privacy as depicted in Table 1.1.

Table 1.1: Research Scope and Limitations

Items	Scope of Research
Architecture	Traditional network
Network	IPv6 link-local network that used DHCPv6 in stateful mode
Attack Type	A rogue DHCPv6 server attack Passive monitor attack
Router Advertisement (RA) Message	Secured

1.7 Research Steps

To achieve the objectives of this research, numerous research steps have been followed. Figure 1.2 presents the main steps in this research study. These steps are:

1) Identifying Problem. This step covers the background of DHCPv6 and its main function in addition to a detailed analysis of the DHCPv6 and its threats.
2) Literature Review. This step discusses and analyzes the major mechanisms that are used to secure DHCPv6 and identifies the advantages and limitations of each mechanism. Hence, it provides a better understanding of current solutions limitations, research problem, and scope, which gives the knowledge to outline the proposed solution.
3) Research Methodology: This step discusses the proposed mechanism stages and its steps. Further, It explains the mechanisms used to achieve the objectives of this research.
4) Implementation: This step discusses the Implementation of the proposed mechanism and tools and programming language used in the implementation.

This step also explains the testbed and experiment scenarios used for evaluation.

5) Evaluation. In this step, a real-world case study is used to evaluate the efficiency of the proposed mechanism in terms of processing time, configuration time, traffic overhead. Furthermore, this step also tests the ability of the proposed mechanism to prevent rogue DHCPv6 server and protect the client's privacy. The proposed mechanism is validated by comparing it with other existing mechanisms in terms of accuracy and to ensure its usefulness.

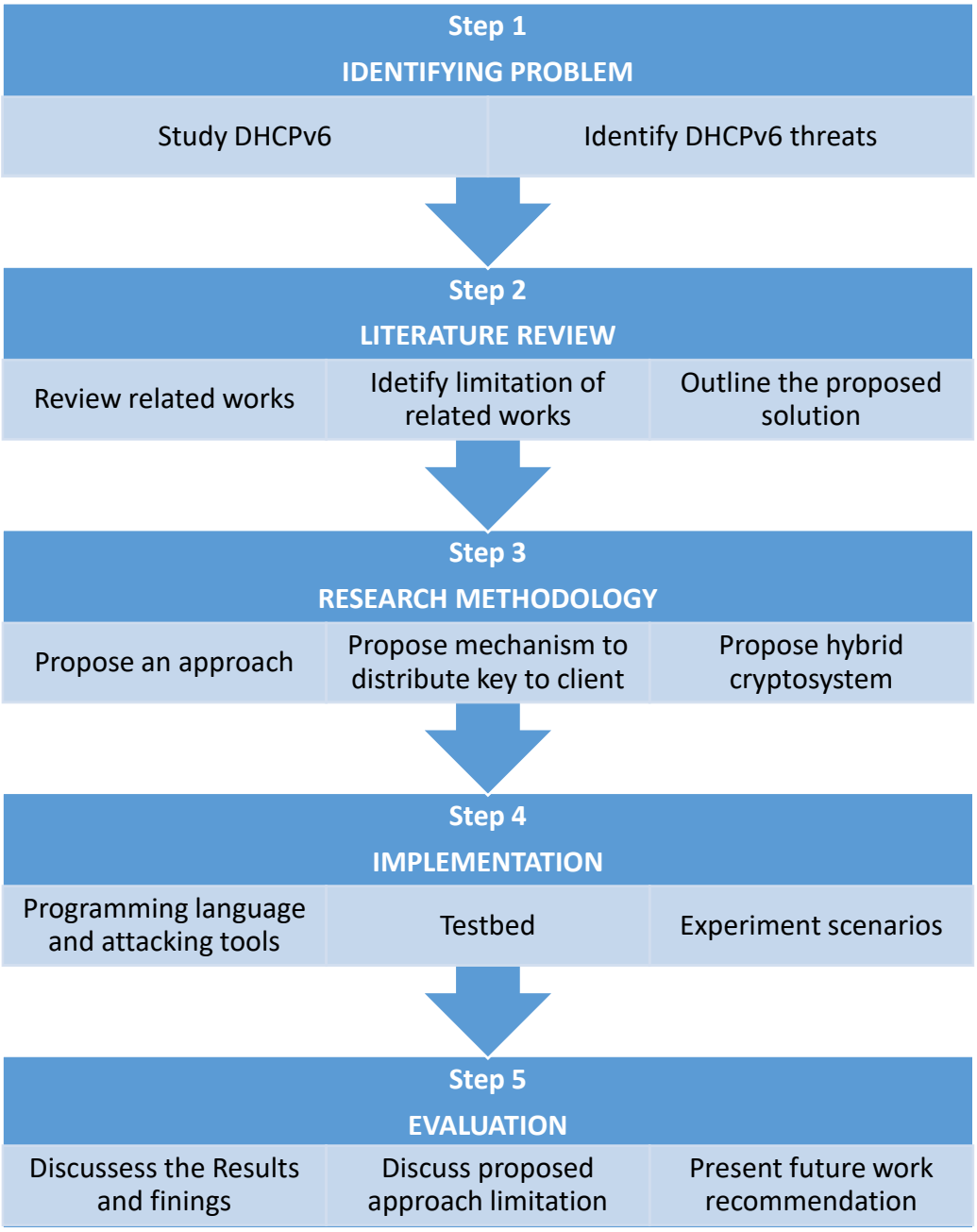

Figure 1.2: Research Steps

1.8 Thesis Organization

This research is divided into six chapters. The research topic is introduced in Chapter 1. The other chapters are arranged as follows:

Chapter 2 critically reviews the background of the DHCPv6 process in an IPv6 link-local network. This chapter also reviews the basic concepts related to this research, the relevant studies, and the limitations of each extant mechanisms.

Chapter 3 discusses the research methodology of the proposed DHCPv6Sec mechanism and elaborates its requirements.

Chapter 4 analyses the proposed mechanism as well as describes its structural design and implementation.

Chapter 5 presents and compares the performance of the proposed DHCPv6Sec mechanism with the Standard-DHCPv6 and Secure-DHCPv6 mechanism.

Chapter 6 summarises the findings of this research and outlines its scope. This chapter also proposes some useful suggestions and recommendations for future work.

CHAPTER 2

LITERATURE REVIEW

This chapter presents a detailed and comprehensive background of the DHCPv6 and foundational concepts related to this research. It discusses the related works on securing service node and DHCPv6. Besides, it highlights the limitations of each solution, which provide the motivation for this research.

The organization of the chapter is as follows: Section 2.1 provides a background of DHCPv6 protocol. Section 2.2 presents the DHCPv6 Architecture. DHCPv6 and IPv6 Network in Section 2.3. DHCPv6 Threat Model is provided in Section 2.4. Section 2.5 discusses the existing mechanisms to secure the RA message. Section 2.6 reviews the related studies, and finally, Section 2.7 summarizes the chapter.

2.1 Background

DHCPv6 server is typically deployed to assign IPv6 addresses and distribute network configuration parameters, such as DNS and NTP server addresses (Brzozowski & de Velde, 2017; Horley & Horley, 2014) to DHCPv6 clients. DHCPv6 is similar to DHCPv4 in the IPv4 network in term of functionalities. However, the message formats are different, and both are vulnerable and susceptible to different types of attacks. For example, DHCPv4 is susceptible to starvation attack, but not DHCPv6 since it has a huge amount of IPv6 address pool at its disposal (Huitema et al., 2016). Therefore, most of the existing DHCPv4 security mechanisms are not applicable to DHCPv6.

In an IPv6 network, a client can use SLAAC, as described by Request for Comments (RFC) [4862], to obtain its IPv6 addresses independent of any server-based

address assignment mechanism (Lindqvist, 2007). However, if SLAAC is used, no network device keeps the record of all IPv6 addresses used by clients in the network; thus resulted in poor manageability. Besides, clients configured with SLAAC cannot obtain other configuration parameters such as the DNS server address and domain (Skjesol et al., 2013). DHCPv6 solves this problem by providing a distribution service of other network configuration to the clients. DHCPv6 has the following advantages over SLAAC mechanism:

1) It allows central management, providing administrators with information such as which addresses were in use at what time. This may be important for auditing, billing, and other purposes (Jeong et al., 2010).
2) It allows administrators to change nodes' addresses frequently. This may be useful to prevent tracking to protect client's privacy (Groat et al., 2011).
3) It could be used to distribute many service parameters, such as DNS and SIP, on behalf of the clients (Frankel et al., 2010).
4) More effective and reasonable in large networks where SLAAC could cause flooding. (Wang et al., 2017).

2.2 DHCPv6 Architecture

DHCPv6 protocol consists of three main components: DHCPv6 Client, DHCPv6 Server, and DHCPv6 Relay as shown in Figure 2.1 (Simon et al., 2011).

DHCPv6 client: A DHCPv6 client requests IPv6 addresses, prefixes, and network configuration parameters from a DHCPv6 server to complete its address configuration.

DHCPv6 server: A DHCPv6 server processes the address allocation, address lease extension, and address release requests from DHCPv6 clients or DHCPv6 relay

agents; and assigns IPv6 addresses and other network configuration parameters to DHCPv6 clients.

DHCPv6 relay: A DHCPv6 relay agent serves as an intermediary between DHCPv6 client and DHCPv6 server that is not connected to the same IPv6 link-local network of the client. The DHCPv6 relay is optional; some network does not require DHCPv6 relay if the client and the server are on the same IPv6 link-local network.

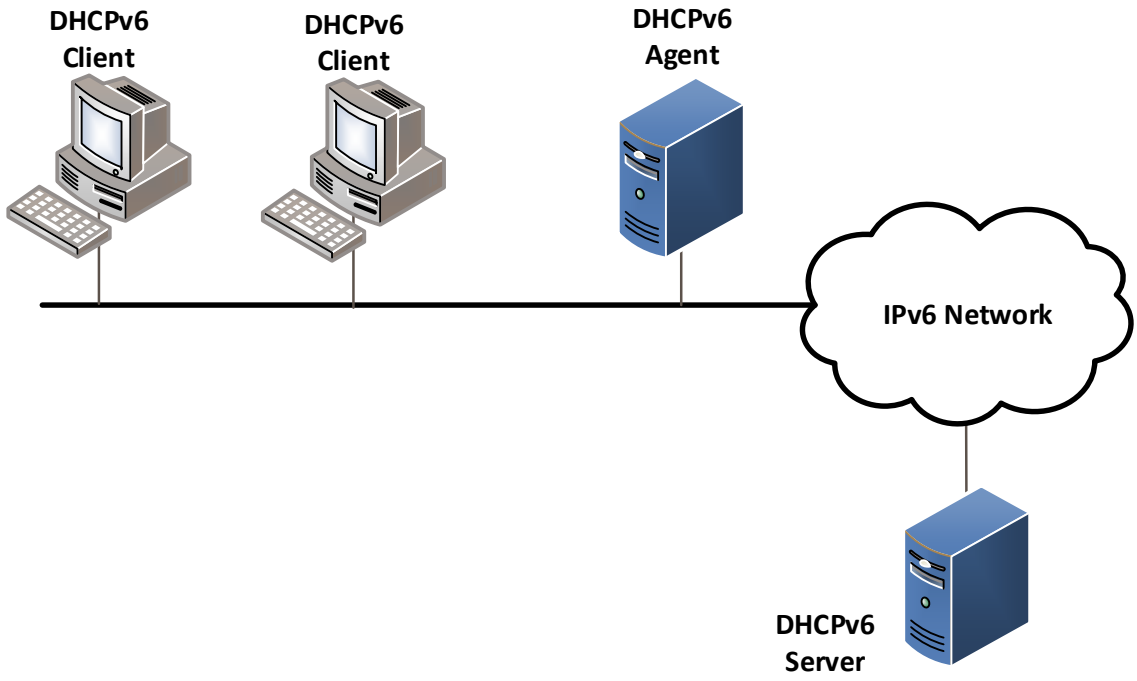

Figure 2.1: DHCPv6 Architecture.

RFC 8213 document stated that the connection between the DHCPv6 relay agent and DHCPv6 server could be secured using IP security (IPSec) (Volz & Pal, 2017). Therefore, this study focus on the security issues related to the DHCPv6 message exchange between DHCPv6 client and its first hop, which could either be a DHCPv6 server or a DHCPv6 relay agent.

2.3 DHCPv6 and IPv6 Network

IPv6 network either uses SLAAC or DHCPv6 to assigned IP address to clients (Savolainen et al., 2013). A router in the network is configured by the administrator to select the type of client configuration method to be used, either SLAAC, Stateless, or Stateful. The type of configuration method to be used in the network is conveyed to the clients via Router Advertisement (RA) message. The RA message has two flags: Managed Flag (M) and Other Config Flag (O). These flags specify what type of DHCPv6 operation mode the client is required to use: stateless or stateful. When M flag is set, the client will configure its address by using DHCPv6 stateful mode; otherwise, the client will use SLAAC. When O flag is set, the client will use DHCPv6 stateless mode to obtain other network configuration parameters; otherwise, the client will not use DHCPv6 stateless mode. If both flags are reset, the end-user nodes know that no DHCPv6 service is available in the network (Arjuman et al., 2017; Kim et al., 2018) .

In standard IPv6 link-local network, whenever a new client joins the network, it either waits for the arrival of an RA message that the router transmits every 200 seconds; or immediately sends out an Router Solicit (RS) message asking for a response from the router in the form of RA message as shown in Figure 2.2. The RA message contains the main configuration parameters of the network, which specifies the DHCPv6 operation mode (i.e., stateful or stateful). The client configures itself based on the RA message. If the client requires the use of DHCPv6 to configure itself, the client and the DHCPv6 server start the message exchange (Barbhuiya et al., 2011; Cerveny et al., 2017). The following sections explain the DHCPv6 operation modes.

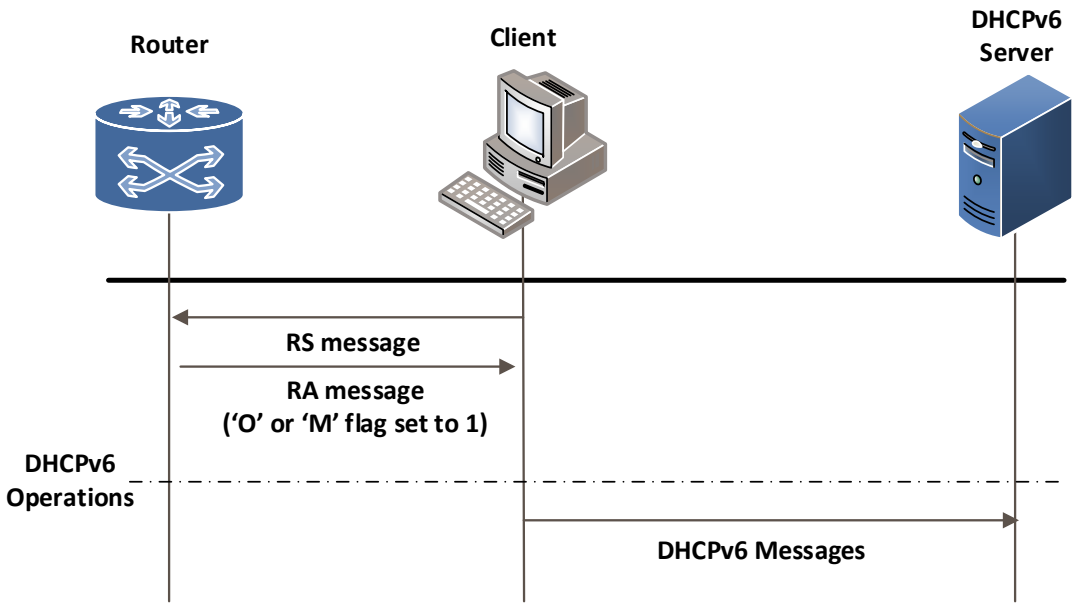

Figure 2.2: DHCPv6 Client Exchange Message with Router

2.3.1 DHCPv6 Stateless Mode

As mentioned in the previous section, the client configures itself according to the flags in the RA messages. In stateless mode, a DHCPv6 server provides other network configuration parameters such as the IP addresses of the DNS and NIS servers (R Droms, 2004). As illustrated in Figure 2.3, the client and the server exchange the following messages to configure the client with an IPv6 address in DHCPv6 stateless mode:

1) The client sends an information request message to the DHCPv6 server on the same link.
2) Upon receiving the client's message, the server responds by sending a Reply message containing the configuration parameters.

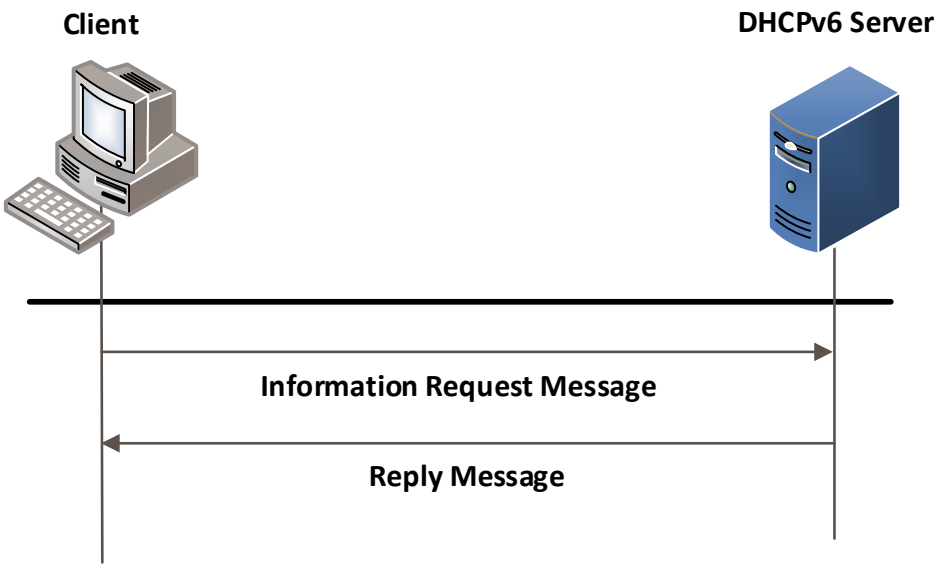

Figure 2.3: DHCPv6 Message Exchange of Stateless Mode.

2.3.2 DHCPv6 Stateful Mode

A DHCPv6 server can also be used to configure clients with IPv6 addresses and network configuration parameters. The client and server are required to exchange the following messages to configure the client's network interface while operating in DHCPv6 stateful mode, as shown in Figure 2.4 (R Droms & Troan, 2003; Su et al., 2011):

1. A client multicasts a DHCPv6 Solicit message to the DHCPv6 Server.
2. All servers on the link that received the Solicit message respond by taking an address from its own address pool and unicasts an Advertise message with options including the address and configuration parameters to the client.
3. The client may receive many Advertise messages but should only choose one. If the DHCPv6 server message has been appended with a preference option, the client chooses the Advertise message with the highest server preference value.

4. The client places the DHCPv6 server identifier of the destination server in a Server Identifier option. Client multicasts a Request message to the DHCPv6 Relay Agents and Servers.
5. Servers receive the Request and determine whether it has been chosen by Server Identifier option in the DHCPv6 Advertise message. Only the chosen DHCPv6 server responds by unicasting the Reply message to the client. Other DHCPv6 servers recycle the address to its address pool. After the client receives Reply, it can use the address to access network, as shown in Figure 2.4.

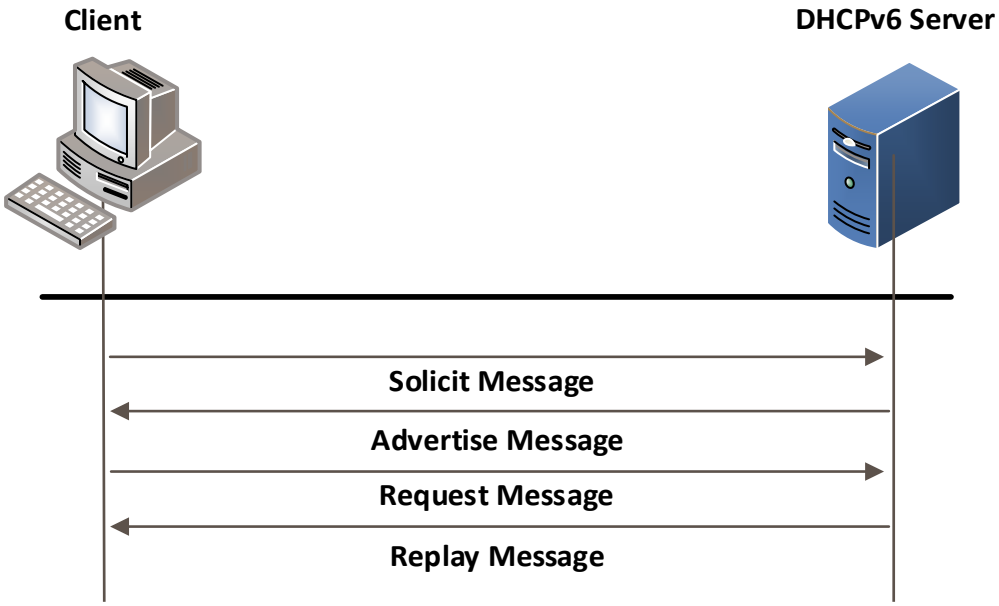

Figure 2.4: DHCPv6 Message Exchange of Stateful mode.

2.3.3 Reconfigure Message

Reconfigure message is a DHCPv6 server message that is used by the server to prompt the client to reconfigure itself with a new network configuration parameters. However, not all client is willing to accept Reconfigure message, since the client continuously listens to the DHCPv6 server message which may be exploited by the

attacker to reconfigure the client message anytime. The following message exchange should take place between the client and the server to reconfigure the client while operating in DHCPv6 stateful mode (Mrugalski et al., 2018), as shown in Figure 2.5.

1. If the DHCPv6 client is willing to accept Reconfigure Message, it should include a Reconfigure Accept option to the first message sent to the server such as a Solicit message.
2. Whenever the DHCPv6 server wants the client to reconfigure itself with a new IPv6 address or network configuration parameters, the server sends a Reconfigure message to the client to prompt the client to send a Renew message, a Rebind message, or an Information-request message.

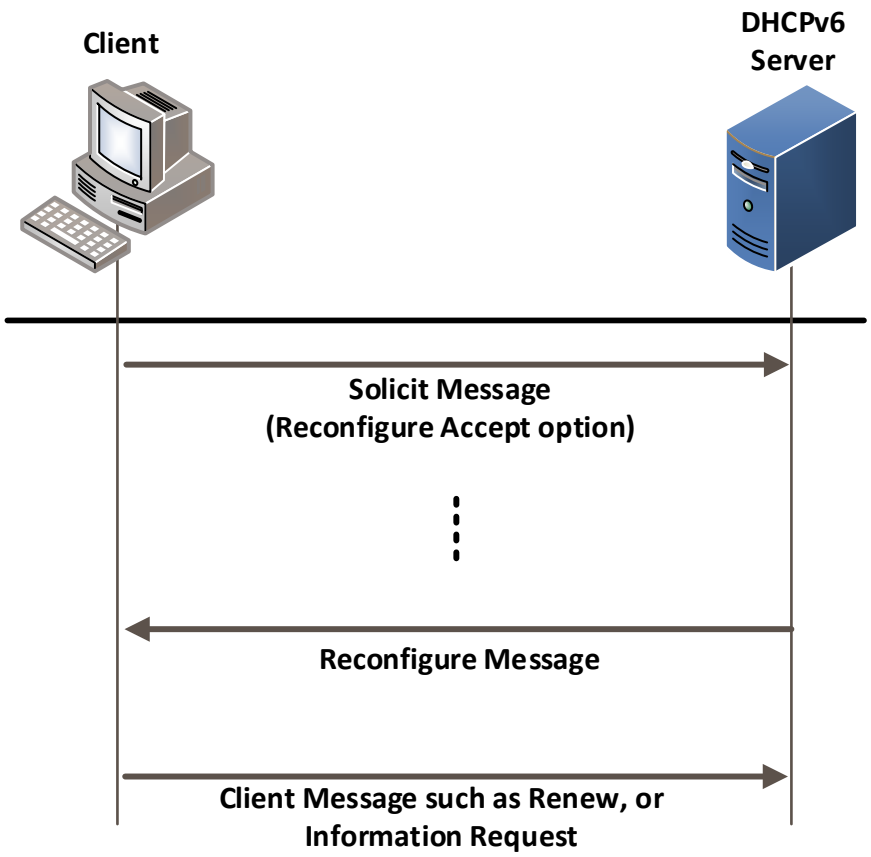

Figure 2.5: DHCPv6 Message Exchange of Reconfigure Messages.

2.3.4 Client and Server Message Formats

All DHCPv6 messages exchanged between servers and clients have an identical fixed format header and a variable format area for options. All values in the message header and in options are in network byte order. Options are stored serially in the "options" field, with no padding between the options. Options are byte-aligned but are not aligned in any other way (such as on 2-byte or 4-byte boundaries). Figure 2.6 illustrates the format of DHCPv6 messages (Mrugalski et al., 2018):

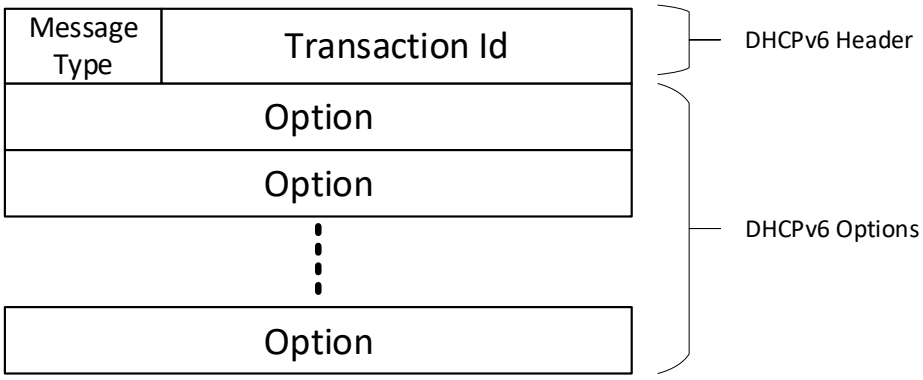

Figure 2.6: DHCPv6 Message Format.

- **Message Type (1 byte):** This field is used to identifies the DHCP message type such as Solicit, Advertise, Reply, and Request.
- **Transaction Id (3 byte):** This field is used by the client to know the server message that received is the reply for its message that was sent earlier.
- **Options (variable length)**: Options carried in this message, such as Client Identifier Option and Server Identifier Option. They used to exhcnage DHCPv6 information.

2.4 DHCPv6 Threat Model

DHCPv6 is considered one of the main elements in the IPv6 link-local network. Therefore, knowing of DHCPv6 threats is essential. Kasanda and Phiri identify that "A threat is anything that can exploit a vulnerability and cause damage to an asset" (Kasanda & Phiri, 2018). The most well-known security issues facing DHCPv6 are rogue DHCPv6 server attack and threats to the DHCPv6 client's privacy. The following sections discuss these issues in detail.

2.4.1 Rogue DHCPv6 Server Attack Issue

A rogue DHCPv6 server is a DHCPv6 server that is owned or exploited by an attacker to feed forged network configuration parameters to DHCPv6 clients in IPv6 link-local network. The clients could be misled to believe that the DHCPv6 server messages are from legitimate DHCPv6 servers. There are more than 30 different network configuration parameters that could be distributed by the DHCPv6 server, such as NTP server address, SIP server address, and DNS server address (Brzozowski & de Velde, 2017; Horley & Horley, 2014) for DHCPv6 clients. The attackers could easily forge these network configuration parameters. The main intention behind this attack is to cause a DoS or to lead the user to a phishing website. Malicious servers may also provide clients with partially modified information that allows the attacker to route traffic through certain client where information could be monitored and collected (L. Li et al., 2018; Su et al., 2011).

The attack occurs when the client sends a Solicit message to seek a response from the server. An attacker on the network will respond back with a fake Advertise message containing a wrong network configuration parameters. Since the client does not have at its disposal a mechanism to verify the source of this message, it will readily accept the message and configure its IP address, as well as other network configuration parameters with incorrect information. Hence, the client falls victim to an attack such as DoS or meet-in-the-middle (MITM) attack that redirects the user's traffic to rogue servers as shown in Figure 2.7 (Alangar & Swaminathan, 2013; Gont & Liu, 2016; L. Li et al., 2018). Taking into account the scenario that was described above, it is clear that authentication of the DHCPv6 server message should be considered essential in IPv6 networks.