STARVATION DELAYED DHCP SERVICE FOR ENABLING POOL RECOVERY

Mayoon Yaibuates[1], Roungsan Chaisricharoen[2,3*]

[1]School of Computer and Information Technology, Chiang Rai Rajabhat University
80 Moo 9, Mueng, Chiang Rai 57100, Thailand

[2]Brain Science and Engineering Innovation Research Group,
School of Information Technology, Mae Fah Luang University
333 Moo1, Thasud, Muang, Chiang Rai 57100, Thailand

[3]School of Information Technology, Mae Fah Luang University
333 Moo1, Thasud, Muang, Chiang Rai 57100, Thailand

E-mail: mayoon.yai@crru.ac.th[1]; roungsan.cha@mfu.ac.th[2]* (corresponding author)

DOI: https://doi.org/10.22452/mjcs.sp2019no2.2

ABSTRACT

Dynamic Host Configuration Protocol (DHCP) Internet Protocol (IP) address starvation is a method, used by attackers, to breakdown communication over IP network. In order to solve this problem, a method to detect and recover malicious IP address request by using Internet Control Message Protocol (ICMP) protocol has been proposed. However, the ICMP based was not be able to work faster in detecting and recovering the malicious request than the attack rate. This study proposed an ease and effective authentication method to emphasize on limiting the rate of IP addresses request by malicious client during the DHCP discovering process and prevent the DHCP server from being IP address starved. Experimental results revealed that the proposed method was not only limited to the IP addresses requested time by attackers but also able to prevent the DHCP server from facing the IP address starvation attack.

Keywords: DHCP, DHCP starvation attack, DHCP discovering, Network security.

1.0 INTRODUCTION

DHCP is a communication protocol for providing IP address and network configuration parameters dynamically to IP network devices. Incorrect configuration leads to a deny in network and access of services to the device. Attackers use DHCP IP address starvation attack to destroy new client's IP network communication by exhausting all available IP addresses in the DHCP server [1]. After launching the attack, attackers may attach their own DHCP server– Rouge DHCP which acts as a DHCP server to provide network configuration parameters to the other legitimate user devices, and assign an IP address of their own computer as a default gateway parameter. As a consequence, there is a possibility for attackers to deny, capture, modify, and analyze every packet such as privacy information, instant messaging, or secret password that had been sent from the attacked device [2].

Attackers send large quantity of DHCP Discover messages to the target network in order to establish a DHCP IP address starvation attack. A spoofed unique physical network identity, media access control (MAC) address, was used in the attacking process. When DHCP server received DHCP Discover messages, it must reply to the sender with the DHCP Offer message. So, attackers can starve the DHCP IP address allocation service by consuming all available IP addresses and cannot give any IP addresses to new requested clients.

ICMP protocol has been introduced as a method to successfully detect and recover the IP addresses that was hold by the attackers in a scenario study [3-4]. The speed of detecting and recovering still has been challenged for practical implementation. The method based on ICMP protocol spent much time in detecting and recovering, this was higher than the attack rate. Therefore, the method to delay the attack rate should be considered.

This study proposed a simple challenge-response authentication method during the DHCP discovering process. This method can limit the rate of IP address request sending by malicious–not faster than legitimate clients. The DHCP server required at least two out of four DHCP Discover messages from challengers, who request an IP address, to initiate the IP address allocation task. The proposed method was evaluated by four main measurements: (1) Amount of time used by an attacker for obtaining IP address comparing with detected and recovered time, (2) Amount of IP address hold by malicious and legitimate clients, (3) Amount of memory usage by comparing to the conventional DHCP sever, it was measured only at the server side since there were no changes at the client side, and (4) Probability difference of clients in obtaining IP address when compared with the conventional DHCP server.

The results showed that the proposed authentication method can delay the attack rate and prevent the server from starvation attacks with a slightly consuming memory. The probability of the general DHCP server to receive DHCP Discover message was higher than the modified DHCP server. However, there was no effect on the legitimate clients.

2.0 LITERATURE REVIEWS

The related literature works on DHCP are on the history of DHCP and its operation, the security issues in DHCP, and existing DHCP starvation mitigation techniques.

2.1 The History of DHCP and Operation

DHCP, a client-server based network protocol, has been used for automating that assigns the network configuration parameters of TCP/IP implementation system [5]. DHCP was developed by the Internet Engineering Task Force (IETF) Dynamic Host Configuration (DHC), a well-recognized working group as part of the Daft Standard in 1997. The protocol consists of two parts - DHCP server and DHCP client. DHCP server is responsible for allocating network address and other protocol stack configuration parameters to DHCP client. The protocol relies on User Datagram Protocol (UDP) [6].

Normally DHCP protocol provides a hand check by using four DHCP messages which are DHCP Discover, DHCP Offer, DHCP Request, and DHCP Ack that is exchanged between client and server to assign a network configuration parameters automatically. Figure 1 demonstrates the process of DHCP operation. When DHCP client is connected to the network, it will broadcasts DHCP Discover message to the network in order to find the DHCP server which is located in a connected network. A DHCP server that receives the broadcast message will check its available IP addresses; an unused address will be selected and responded to the DHCP Offer message for the requesting client. After the client receives the DHCP Offer message, the client will uses these configuration parameters to setting an IP address before sending the DHCP Request message which is to be confirmed by accepting these setting parameters. The DHCP server that receives the DHCP Request message will return the DHCP Ack message as an acknowledgement to the client.

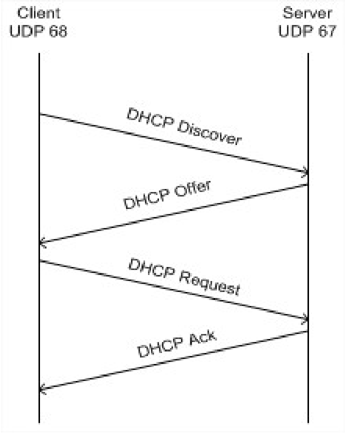


Fig. 1: DHCP protocol operation

A study done by [7], they investigated on how the DHCP client and server exchange their messages. They claimed that if the DHCP client did not receive any DHCP Offers from the server, it will send DHCP Discover message four times with a gap of 2 seconds in every 5 minutes. [8] also agreed and added their findings that DHCP Discover messages would be sent by the DHCP client until it received a DHCP Offer message from the server. Moreover, there was nothing specified in RFCs on demonstrating how the client should handle the case when there were no DHCP Offer messages responding from the server. They also found that client's behavior in different operating systems including Windows XP, Windows 7, IOS 5.0.1, Symbian S60 5th, and Android (2.3.7) will attempt to resend DHCP Discover messages to the server.

2.2 Security Issues in DHCP

At the beginning of DHCP development, security was not that critical as in the present time. The following protocol did not provide any authentication mechanisms between client and server. That was a reason why the protocol became the target of various attacks, namely DHCP starvation and Rouge DHCP.

DHCP starvation attack is considered as Denial of Service (DoS) attack. It is an easy way for an attacker to prevent the attacked device from accessing to network and services. *Scapy*, *Gobbler*, and *Yersinia* are well-known tools for attackers to launch DHCP starvation attack. Attackers will send many DHCP Discover messages with spoofing MAC address for consuming all of the useable IP addresses on the DHCP Server. For this reason, the new legitimate client will be denied from obtaining an IP address and network configuration parameters from the DHCP server.

After the DHCP starvation attack had run successfully, an attacker may setup their own DHCP server, and Rouge DHCP, by turning the DHCP Server function on and provide the malicious network parameters such as default gateway, DNS server to the victim [9]. Thus, an attacker can capture, modify, and analyze any information that had been sent from attacked devices. The rouge DHCP can be effectively prevented by implementing DHCP snooping in a network switch [10]. The function of DHCP snooping can also be implemented in Wireless network by using Wireless Controller [11].

2.3 Existing DHCP Starvation Mitigation Techniques

The survey was conducted for reviewing on the existing techniques for mitigating DHCP starvation. In this research, the mitigation techniques were divided into two categories namely cryptology based and non-cryptology based.

2.3.1 Cryptology based

At the early stage, a secret shared key was used in an authentication between the DHCP client and server, which was done in a token based format [12]. However, the token was a plaintext which could be easily sniffed by any attackers. To prevent attackers from sniffing the secret shared key, the digital certificate based has been proposed for authenticating the DHCP message between DHCP client and server [13-18]. Even though the authentication was based on the digital certificate it could be an efficient way for preventing DHCP starvation attack, by verifying the legitimate client and server. The certificate requires a more complex environment to fulfill this objective. In fact, the key that is used between the DHCP client and server must be shared before initialing normal DHCP operation. Due to this reason, the DHCP starvation attack mitigation techniques which is based on cryptology are rarely implemented in the real world networks [19].

2.3.2 Non-cryptology based

A number of research works agreed that configuring the port security in network switch can mitigate DHCP starvation attack [10, 20-21]. Even though port security could work well in wired network, this method could not be applied with the shared medium network like Wi-Fi. The research [22] introduced the enhancement of port security which could work with the shared medium network. The estimate numbers of contending users at each port had been used for a fairly IP addresses allocation. However, attackers still have consumed all allocated IP addresses to each port and move to another port by switching to other Wireless Access Point [23]. A method for detecting and recovering malicious IP address request by using ICMP protocol has been proposed [3-4]. These methods can use to detect and recover IP address from the malicious request accurately in spite of the fact that the ICMP based could not detect the malicious request and recover the IP address hold by attackers faster than the attack rate. Therefore, the reduction of time spent for IP address request by attackers need to be focused on for more practical implementation.

3.0 METHODOLOGY

Before proposing the DHCP starvation mitigation method, the behavior of legitimate and malicious DHCP client was studied and summarized. After that, the researchers proposed the method based on the results found on this study. The results were analyzed and compared for a proposed method with a general DHCP server in terms of probability.

3.1 Investigation on Behavior of Legitimate and Malicious DHCP Client

There were two network scenarios, used to investigate the behavior of a legitimate and malicious DHCP client, 100 legitimate and 100 malicious IP address requests, (1) with and (2) without a DHCP server. In this investigation, the number of 100 DHCP Discover messages that were sent from a malicious client could be enough to reveal the characteristic of a malicious request. The characteristics of malicious request results are shown in Table 1. Since the reference from Khan et al. [7] claimed that if the DHCP client did not receive any DHCP Offers from the server, it will send a DHCP Discover message four times with a gap of two seconds. The results from none of the DHCP servers studied supported this, it was found that the malicious client sent only one DHCP Discover message per spoofed MAC address whether it received a DHCP Offer from the server or not. To clarify the reason of using the client without DHCP server investigation could be stated that the case of none DHCP server was used to study the characteristics of the client in depth, practically with the characteristics of a malicious client. In this investigation, legitimate IP address requests were sent from a DHCP client using Windows 7 Service Pack1. In addition, the malicious IP address requests were sent from a packet injection tool (*Scapy*) which operates on Kali Linux version 1.1.0. The justification of using different OS for the client was due to the legitimate client DHCP Discover requests that were being sent directly from the protocol stack of Windows 7 Service Pack 1, whereas *Scapy* generated malicious requests and was required to be run on a Kali Linux version 1.1.0 operating system.

Table 1**:** The distinction behaviors of a legitimate and malicious client

Scenario	Legitimate		Malicious	
	without DHCP Server	with DHCP Server	without DHCP Server	with DHCP Server
Number of DHCP Discover messages	400	100	100	100
Number of DHCP Discover messages per IP address request	4	1	1	1
Number of DHCP Discover massages with the same MAC address	400	100	0	0
Duration time between each DHCP Discover messages	>2s	>2s	<0.1ms	<0.1ms
Number of DHCP Offer messages	0	100	0	100
Number of DHCP Request messages	0	100	-	0
Deliver time for DHCP Request message to the DHCP Server	-	<4ms	-	-

Number of DHCP Ack messages	0	100	0	0

Without a DHCP server scenario, the legitimate client sent four DHCP Discover messages per IP address request since it did not received any DHCP Offer message from the server, while malicious clients sent only one DHCP Discover message per IP address request in order to subscribe to the DHCP service. The duration time between each message of the legitimate (more than 2 seconds) was higher than the malicious request (less than 0.1 milliseconds).

In contrast with the DHCP server scenario, both clients sent one DHCP Discover message per IP address request. The legitimate client sent only one DHCP Discover message because it received a DHCP Offer message. DHCP Request messages were sent by the legitimate client whereas no DHCP Request message was sent from a malicious client. The time spent by the legitimate client to deliver DHCP Request message after it received the DHCP Offer message was less than 4 milliseconds. In the case without a DHCP server the legitimate client sent four DHCP messages because there was no DHCP Offer message to replying to the legitimate client. Thus, in the case without a DHCP server, the duration times between each DHCP Discover message were counted by using the four DHCP Discover messages. On the other hand, in the case with a DHCP server, the duration times between each DHCP Discovers message were counted with only one message as same as the malicious client. The DHCP Offer message was replied to as being legitimate.

The different behaviors of legitimate and malicious requests were identified as three key behaviors. First, malicious clients spoofed its MAC address then sent one DHCP Discover message per spoofed MAC address while legitimate clients sent four DHCP Discover messages with its own MAC address. Second, the duration time between each DHCP Discover message sent by a malicious client was a lot faster than a legitimate client. Finally, there were no other types of DHCP messages except for the DHCP Discover messages being sent by the malicious client. To launch a DHCP starvation attack, sending only a large number of DHCP Discover messages to the target DHCP server is enough to starve the IP address allocation services. Since the DHCP server responds to a DHCP Discover message with a DHCP Offer message. So, there would be no other type of DHCP messages being sent from the malicious client.

3.2 DHCP Starvation Delay and Prevention

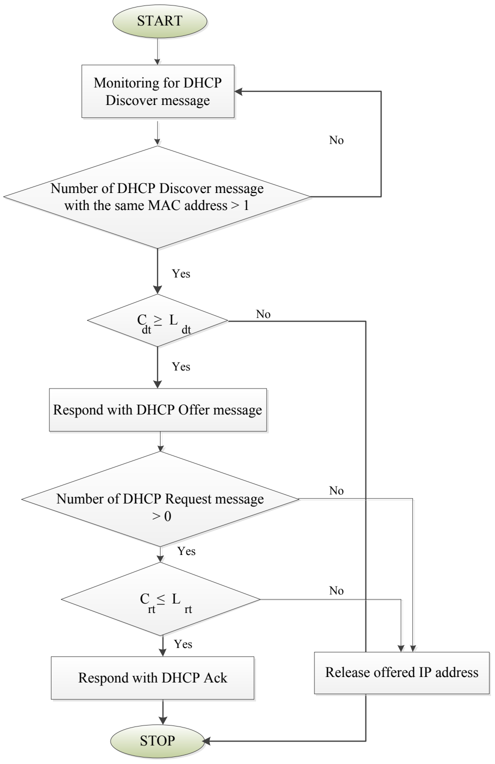

START
Monitoring for DHCP Discover message
No
Number of DHCP Discover message with the same MAC address > 1
Yes
C_dt ≥ L_dt
No
Yes
Respond with DHCP Offer message
Number of DHCP Request message > 0
No
Yes
C_rt ≤ L_rt
No
Yes
Respond with DHCP Ack
Release offered IP address
STOP

Fig. 2: The flowchart showing the procedure of the proposed method.

In the DHCP discovering process, there are three differences in behaviors between the legitimate and malicious client. The proposed method used them to make decisions for completing the rest of IP address allocation task. Figure 2 illustrated the proposed authentication method for delaying the attackers IP address time and prevented the DHCP server from a starvation attack.

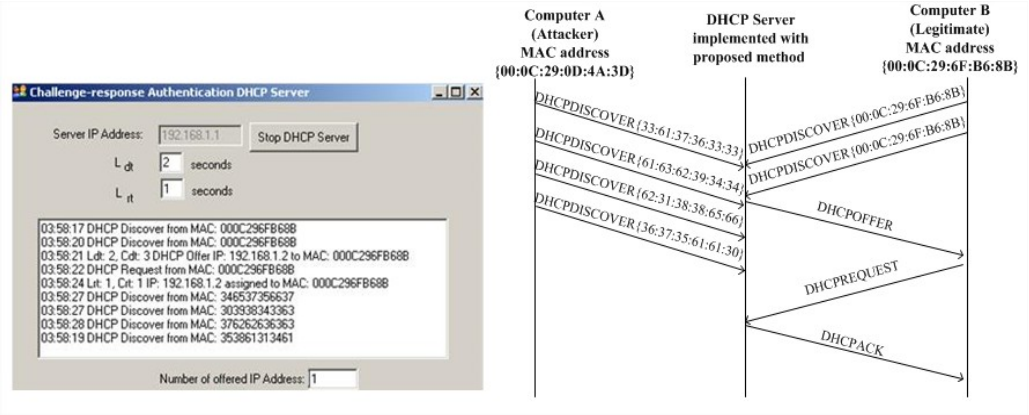
In the proposed method, the DHCP server required at least two DHCP Discover messages with identical MAC address from the challenger to initiate an IP address allocating task. The first reached message is used as a purpose challenge. If the challenger transmits another message with the same MAC address to the server in proper time, the server will send the DHCP Offer message to that challenger. The condition of the proposed authentication method for sending the DHCP Offer to the challenger can be defined as the logic below:

$$(N_d > 1) \wedge (C_{dt} \geq L_{dt}) \tag{1}$$

The abbreviation could be represented as follows; N_d denotes the number of DHCP Discover message with the same MAC address. Challenger deliver time (C_{dt}) is the time in second used by the challenger to deliver two DHCP Discover messages with the same MAC address to the server. C_{dt} can be computed from the time different between the first and the second DHCP Discover messages timestamp. Legitimate deliver time (L_{dt}) is the minimum based time in second used by the legitimate DHCP client to deliver two DHCP Discover messages with the same MAC address to the server. L_{dt} aims to limit the IP address request rate under the conditional of having same MAC address. In case that $C_{dt} \geq L_{dt}$, the DHCP Request message must be sent to the server by the challenger within L_{rt} time window for completing the IP address allocation task. The condition can be expressed in logical as,

$$(N_r > 0) \wedge (C_{rt} \leq L_{rt}) \tag{2}$$

N_r is the number of DHCP Request message. Challengers request time (C_{rt}) is the time in second that the challenger delivers the DHCP Request messages to the server. Legitimate request time (L_{rt}) is the maximum based time in second used by the legitimate DHCP client for sending DHCP Request message to the DHCP server after it received the DHCP Offer.


Challenge-response Authentication DHCP Server
Stop DHCP Server
Computer A
(Attacker)
MAC address
{00:0C:29:0D:4A:3D}
DHCP Server
implemented with
proposed method
Computer B
(Legitimate)
MAC address
{00:0C:29:6F:B6:8B}
DHCPDISCOVER{33:61:37:36:33:33}
DHCPDISCOVER{61:63:62:39:34:34}
DHCPDISCOVER{62:31:38:38:65:66}
DHCPDISCOVER{36:37:35:61:61:30}
DHCPDISCOVER{00:0C:29:6F:B6:8B}
DHCPDISCOVER{00:0C:29:6F:B6:8B}
DHCPOFFER
DHCPREQUEST
DHCPACK

Server IP Address: 192.168.1.1

L_{dt} 2 seconds

L_{rt} 1 seconds

```
03:58:17 DHCP Discover from MAC: 000C296FB68B
03:58:20 DHCP Discover from MAC: 000C296FB68B
03:58:21 Ldt: 2, Cdt: 3 DHCP Offer IP: 192.168.1.2 to MAC: 000C296FB68B
03:58:22 DHCP Request from MAC: 000C296FB68B
03:58:24 Lrt: 1, Crt: 1 IP: 192.168.1.2 assigned to MAC: 000C296FB68B
03:58:27 DHCP Discover from MAC: 346537356637
03:58:27 DHCP Discover from MAC: 303938343363
03:58:28 DHCP Discover from MAC: 376262636363
03:58:19 DHCP Discover from MAC: 353861313461
```

Number of offered IP Address: 1

Fig**.** 3**:** The set-up scenario with malicious and legitimate DHCP client

The set-up scenario of two DHCP clients: malicious (computer A) and legitimate (computer B) shown in Figure 3 is used to explain the authenticating method. The stable value of L_{dt} is set as 2 seconds whereas L_{rt} is 1 second. Normally, after the legitimate client receives the DHCP Offer message from the DHCP server the legitimate client responds to the DHCP server with a DHCP Request message within 4 milliseconds. In contrast with a malicious client, the malicious never responded to any DHCP Offer messages sent from the DHCP server. The deliver time for a DHCP Request message was designed for use in an assumption case. The malicious user modifies their tools to act like a legitimate client by sending two DHCP Discover messages to overcome our proposed authentication. In this case, the malicious client has to spend the same amount of time as the legitimate client. Even though there are four DHCP Discover messages sent from computer A to the DHCP server, none have the same MAC address. According to the logical condition defined in Eq. (1), there is no IP address assigned to computer A. In contrast, computer B sent two DHCP Discover messages with the same MAC address to the DHCP server. The value of C_{dt} is 3 seconds (calculated from 03:58:20 - 03:58:17) which is greater than L_{dt}. As a consequence, the DHCP Offer is sent to computer B. Based on the logical condition in Eq. (2), the value of C_{rt} is 1 second (calculated from 03:58:22 – 03:58:21) which is equal to L_{rt}. Therefore, the IP address is assigned to computer B.

3.3 Probability Analysis

In DHCP Discovering, since the IP address is necessary for communicating with other network devices and services the client will send another DHCP Discover message if there is no DHCP Offer message response from the server.

In general, with a DHCP operation, the DHCP server requires receiving at least one DHCP Discover message from the client device to initiate the address allocation process. Thus, the probability for the DHCP server receiving any DHCP Discover messages out of four sent messages can be expressed using a tree diagram; each probability should be multiplied along the branches and added to vertically. The sum of the probabilities for any set of branches is always 1. The following below is an example:

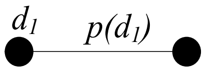


Fig**.** 4**:** The tree diagram of the DHCP server receiving any DHCP Discover messages from sending one DHCP Discover message (d_1)

First, in Figure 4, when the client is connected to the network, the first DHCP Discover message *(d_1)* is sent in order to locate the DHCP server and attach to the DHCP service that is provided in the network. So, the probability of the DHCP server receiving any DHCP Discover messages from sending one DHCP Discover message is expressed as:

$$P(D)=P(d_1) \tag{3}$$

Where:

P(D) is the probability for the DHCP server receiving any DHCP Discover messages.

$p(d_i)$ is the probability of each DHCP Discover messages to be received by the DHCP server.

$1- p(d_i)$ is the probability of each DHCP Discover messages unable to reach the DHCP server.

d_i is the DHCP Discover message.

However, in Figure 5, in the case of the first DHCP Discover message being unable to reach the server, the probability of the DHCP server receiving any DHCP Discover messages from sending two DHCP Discover messages (d_1 and d_2) can be written as:

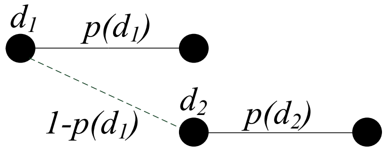


Fig. 5: The tree diagram of the DHCP server receiving any DHCP Discover message from sending two DHCP Discover messages (d_1 and d_2)

$$P(D) = p(d_1)+(1-p(d_1))\, p(d_2) \tag{4}$$

According to Figure 6, in the situation that the first two DHCP Discover messages (d_1 and d_2) are unable to reach the server, the probability of the DHCP server receiving any DHCP Discover messages from sending three DHCP Discover messages (d_1, d_2, and d_3) can be given as:

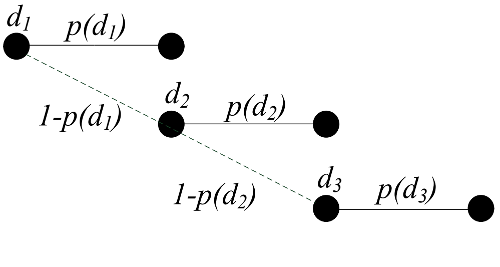


Fig. 6: The tree diagram of the DHCP server receiving any DHCP Discover message from sending three DHCP Discover messages (d_1, d_2, and d_3)

$$P(D) = p(d_1)+(1- p(d_1))p(d_2)+(1- p(d_1)) (1- (pd_2)) p(d_3) \quad (5)$$

Finally, Figure 7, if none of the three messages reach the server, the probability of the DHCP server receiving any DHCP Discover messages can then be calculated by using the Eq. (6):

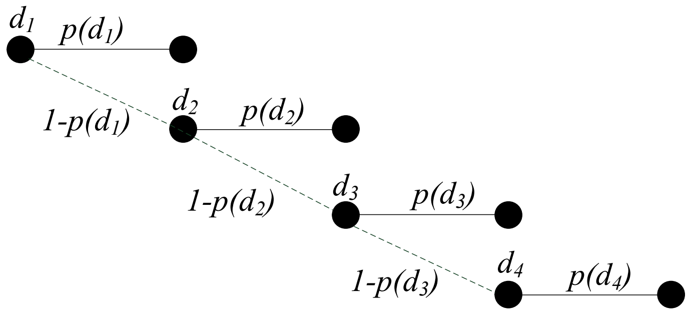


Fig. 7: The tree diagram of the DHCP server receiving any DHCP Discover message from sending four DHCP Discover messages (d_1, d_2, d_3, and d_4)

$$P(D)=p(d_1)+(1-p(d_1))p(d_2)+(1-p(d_1))(1-p(d_2))p(d_3)+(1-p(d_1))(1-p(d_2))(1-p(d_3))p(d_4) \quad (6)$$

From Eq. (6) Let: $p(d_1) = p(d_2) = p(d_3) = p(d_4) = p(d_i)$; the probability for the DHCP server receiving any DHCP Discover messages from sending four DHCP Discover messages (d_1, d_2, d_3, and d_4) can be written as:

$$P(D) = p(d_i)+(1-p(d_i)) p(d_i)+(1-p(d_i))^2p(d_i)+(1-p(d_i))^3p(d_i) \quad (7)$$

The probabilistic model for the DHCP server receiving any DHCP Discover messages from sending four DHCP Discover messages can be computed as:

$$P(D) = -p(d_i)(-4+6p(d_i)-4p(d_i)^2+ p(d_i)^3) \quad (8)$$

In our proposed method, there are six possible cases that two out of four DHCP Discover messages would be able to reach the DHCP server. These possible cases are represented by tree diagrams as the following:

First, Figure 8, when the client is connected to the network, the first DHCP Discover message is sent not only for locating the DHCP server and attending to the DHCP service that is provided in the network, but also initiating the challenge process with the server. After that, the second DHCP Discover message is sent to the server for confirming that it is a legitimate client. So, the probability for the modified DHCP server receiving two DHCP Discover messages, as in this case, can be expressed as:

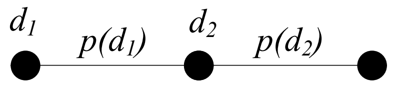


Fig. 8: The tree diagram of the modified DHCP server receiving two DHCP Discover messages (d_1 and d_2) from sending two DHCP Discover messages

$$P(MD) = p(d_1)p(d_2) \tag{9}$$

Where:

P(MD) is the probability for the modified DHCP server receiving two DHCP Discover messages.

$p(d_i)$ is the probability of each DHCP Discover messages to be received by the DHCP sever.

$1- p(d_i)$ is the probability of each DHCP Discover messages unable to reach the DHCP server.

d_i is the DHCP Discover message.

Second, Figure 9, in the situation where the second DHCP Discover message (d_2) is unable to reach the server, but the first and third DHCP Discover messages(d_1 and d_3) were able to reach the server, the probability for the modified DHCP server receiving two DHCP Discover messages can be given as:

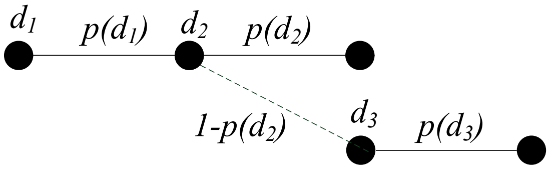


Fig. 9: The tree diagram of the modified DHCP server receiving two DHCP Discover messages (d_1 and d_3) from sending three DHCP Discover messages

$$P(MD) = p(d_1)\ (1\text{-}p(d_2))\ p(d_3) \tag{10}$$

Third, for Figure 10, in the situation that second and third DHCP Discover messages (d_2 and d_3) are unable to reach the server, but the first and fourth DHCP Discover messages were able to reach the server, the probability for the modified DHCP server receiving two DHCP Discover messages (d_1 and d_4) can be given as:

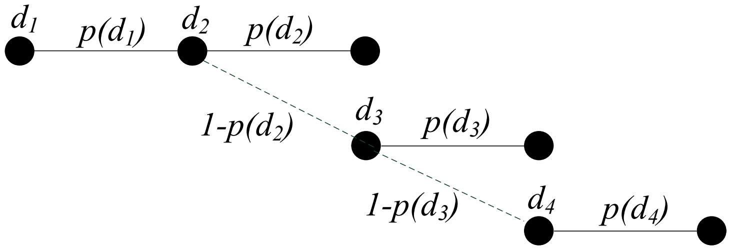


Fig. 10: The tree diagram of the modified DHCP server receiving two DHCP Discover messages (d_1 and d_4) from sending four DHCP Discover messages

$$P(MD) = p(d_1)\ (1\text{-}p(d_2))\ (1\text{-}p(d_3))\ p(d_4) \tag{11}$$

Fourth, for Figure 11, in the situation that the first DHCP Discover message (d_1) is unable to reach the server, but the second and third DHCP Discover messages (d_2 and d_3) were able to reach the server, the probability for the modified DHCP server receiving two DHCP Discover messages can be given as:

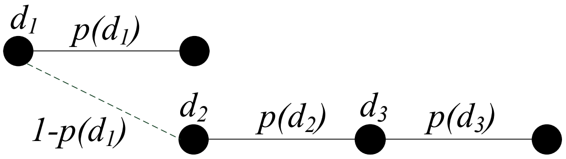


Fig. 11: The tree diagram of the modified DHCP server receiving two DHCP Discover messages (d_2 and d_3) from sending three DHCP Discover messages

$$P(MD) = (1\text{-}p(d_1))\ p(d_2)\ p(d_3) \tag{12}$$

Fifth, for Figure 12, in the situation that the first and third DHCP Discover messages (d_1 and d_3) are unable to reach the server, but the second and fourth DHCP Discover messages were able to reach the server, the probability for the modified DHCP server receiving the two DHCP Discover messages (d_2 and d_4) can be given as:

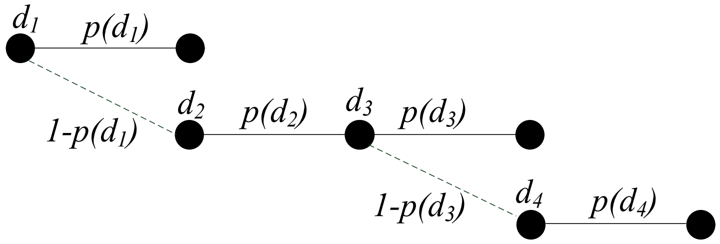


Fig. 12: The tree diagram of the modified DHCP server receiving two DHCP Discover messages (d_2 and d_4) from sending four DHCP Discover messages

$$P(MD) = (1\text{-}p(d_1))\, p(d_2)\, (1\text{-}p(d_3))\, p(d_4) \tag{13}$$

Sixth, for Figure 13, in the situation that the first and second DHCP Discover messages are unable to reach the server, but the third and fourth DHCP Discover messages were able to reach the server, the probability for the modified DHCP server receiving two DHCP Discover messages can be given as:

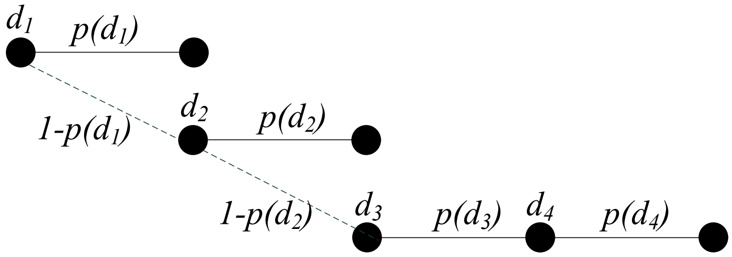


Fig. 13: The tree diagram of the modified DHCP server receiving two DHCP Discover messages (d_3 and d_4) from sending four DHCP Discover messages

$$P(MD) = (1\text{-}p(d_1))\, (1\text{-}p(d_2))\, p(d_3)\, p(d_4) \tag{14}$$

Hence, the overall probability for the modified DHCP server receiving two DHCP Discover messages from sending four DHCP Discover messages can be given as:

$$\begin{gathered} P(MD) = p(d_1)p(d_2) + p(d_1)\, (1\text{-}p(d_2))\, p(d_3) + p(d_1)\, (1\text{-}p(d_2))\, (1\text{-}p(d_3))\, p(d_4) + (1\text{-}p(d_1))\, p(d_2)\, p(d_3) + \\ (1\text{-}p(d_1))p(d_2)\, (1\text{-}p(d_3))\, p(d_4) + 1\text{-}p(d_1))\, p(d_2)\, (1\text{-}p(d_3))\, p(d_4) \end{gathered} \tag{15}$$

From Eq. (15) Let: $p(d_1) = p(d_2) = p(d_3) = p(d_4) = p(d_i)$; the probability for the modified DHCP server receiving two DHCP Discover messages can be written as:

$$P(MD) = p(d_i)^2 + p(d_i)^2 (1\text{-}p(d_i) + p(d_i)^2 (1\text{-}p(d_i))^2 + p(d_i)^2 (1\text{-}p(d_i)) + p(d_i)^2 (1\text{-}p(d_i))^2 + p(d_i)^2 (1\text{-}p(d_i))^2) \quad (16)$$

Finally, the probabilistic model for the modified DHCP server receiving two DHCP Discover messages can be computed as:

$$P(MD) = p(d_i)^2 (6\text{-}8p(d_i) + 3p(d_i)^2) \quad (17)$$

The percentage loose in probability of the modified DHCP server by requiring two DHCP Discover messages to be reached by the server at any value of $p(d_i)$ comparing to the DHCP discovering in general method can be computed by Eq. (8) minus Eq. (17) expressed as:

$$P(D \text{ and } MD_{Dif}) = (-4(-1+p(d_i))^3 p(d_i)) \quad (18)$$

$P(D \text{ and } MD_{Dif})$ represents the differentiation values between the value of $P(D)$ and $P(MD)$.

4.0 RESULT AND DISCUSSION

4.1 DHCP Starvation Delayed

In this experiment, the network consisted of a DHCP server implemented with the proposed method and 30 malicious clients. In this case, the malicious client pretended to be a legitimate client by sending more than one DHCP Discover messages and delivering DHCP Request after it received the DHCP Offer. In the DHCP server implemented with the proposed method, the constant value of L_{dt} was set to 2 seconds and L_{rt} was set to 1 second.

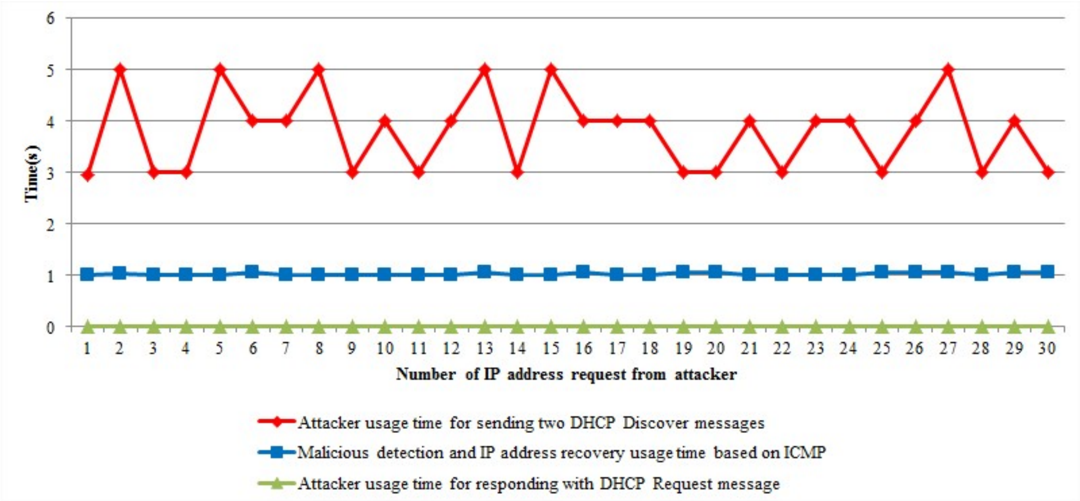
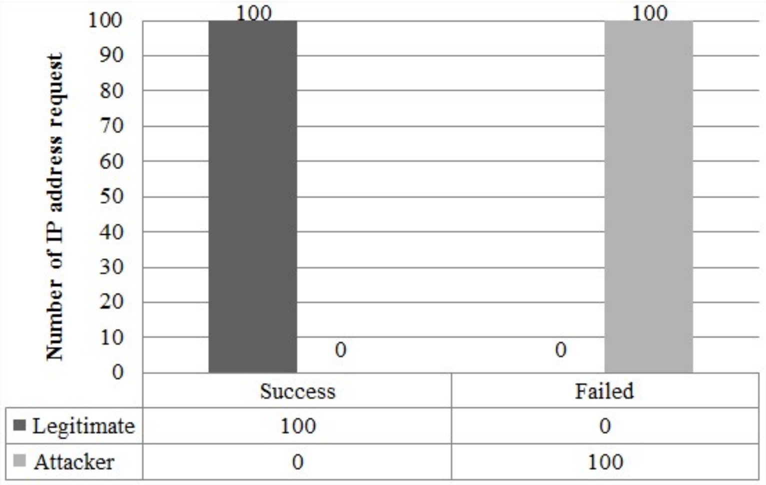


Fig. 14: The time used for detect and recovery IP addresses comparing with the time used by attacker to ruin each IP address

Figure 14 is the results from delaying the attackers' attack rate. Advance attackers may able to modify their tools by sending more than one DHCP Discover message with the same MAC address per round. However, our proposed method can limit the attack rate by using L_{dt} and L_{rt} since the interval time of DHCP Discover messages in each round should be greater or equal to L_{dt} and the DHCP Request must be delivered to the DHCP server within time L_{rt}. Although the attacker could be able to ruin the IP address, the attacker had to spend at least the same amount of time as legitimate clients (at least 2 seconds). Moreover, the ruin time (3-5 seconds) was greater than usage time for detection and recovery (less than 1.5 seconds) by the server. Thus, the detection and recovery method based on ICMP can be applied effectively.

4.2 DHCP Starvation Prevention

In this experiment, the network consisted of a DHCP server implemented with the proposed method, a legitimate client running on Windows 7 Service Pack1, and malicious client ran *Scapy* on Kali Linux version 1.1.0. Both clients sent 100 IP address requests. A malicious client sent an IP address request using the DHCP Discover message with an interval of 0.1 second. In the DHCP server implemented with the proposed method, the constant value of L_{dt} was set to 2 seconds and L_{rt} was set to 1 second. The time used in the experiment for L_{dt} is 2 seconds which corresponded with Khan et al. [7]. Their work claimed that if the DHCP client did not receive any DHCP Offer messages from the server, it will send a DHCP Discover message four times with a gap of 2 seconds. Moreover, the information was gathered from section 3.1 as shown in Table 1 (Duration time between each DHCP Discover message >2 seconds). The time used in the experiment for L_{rt} is 1 second which is based on the information gathered from section 3.2 as shown in Table 1 (Deliver time for DHCP Request message to the DHCP Server <4 milliseconds). The value of L_{rt} is set to 1, which had included the possibilities of the delay in network transmission. The delay may lead the value of delivery time for the DHCP Request message to the DHCP Server greater than 4 milliseconds but the value of L_{rt} should not be less than 1 second.



	Success	Failed
■ Legitimate	100	0
■ Attacker	0	100

Fig. 15: The prevention accuracy result of DHCP server implemented with proposed method

The experimental results from Figure 15 indicate that the DHCP server implemented with the proposed method could prevent the attacker from obtaining the IP address. Meanwhile, the legitimate client was still able to obtain the IP address. This reflected on the effectively tolerance towards the DHCP IP address starvation attack of the proposed method.

4.3 Resource Consuming

The comparison of resource consuming between conventional DHCP service and DHCP service implemented with the proposed method was measured by using the memory usage value. The Performance monitor tool was used to collect maximum memory usage of the DHCP service. The maximum memory used by the conventional DHCP service and the DHCP service implemented with the proposed method was measured in two situations; normal and under attacked. In both situations, a legitimate client performed 100 IP address requests. A malicious client sent 100 fake DHCP Discover messages with an interval of 0.1 second only in an attack situation.

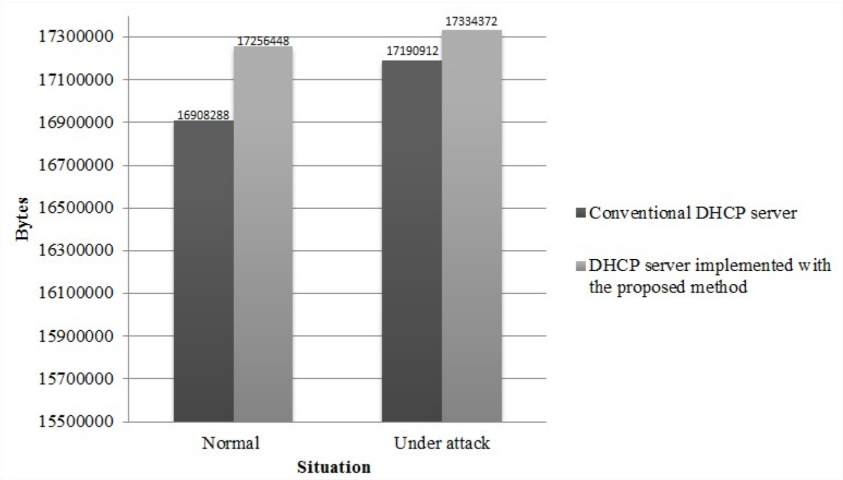


Fig. 16: The result of maximum memory usage comparison

The comparison of maximum memory used by conventional DHCP server and DHCP server implemented with the proposed method is shown in Figure 16. The result found that the DHCP service implemented with the proposed method consumes more memory than the conventional DHCP service. The reason was that the proposed method added more incoming request checking steps when it was compared to the conventional DHCP service. However, the legitimate client was still able to obtain the IP address.

4.4 Probability Difference

The probability analysis result of general DHCP discovering process by comparing the value of *P(D)* from calculation (*$P(D)_{Cal}$*) with *P(D)* from experiment (*$P(D)_{Exp}$*) was made in order to prove the proposed probabilistic model in Eq. (8).

The researchers tested the probability for the general DHCP server receiving any DHCP Discover messages (*$P(D)_{Exp}$*) three times (round 1, round2, and round 3). The compared average values of *$P(D)_{Exp}$* with *$P(D)_{Cal}$*, *$P(D)_{Exp}$* was computed by collecting the number of DHCP Offer messages after sending 100 IP address requests to the conventional DHCP server. Each round of the IP address request contained four DHCP Discover messages. The probability of each DHCP Discover messages to be received by the DHCP server was set from 0.1 to 1. Therefore, the *$P(D)_{Exp}$* is the ratio of the numbers of DHCP Offer messages per the number of IP address request. The values of *$P(D)_{Cal}$* and *$P(D)_{Exp}$* with difference *$p(d_i)$* are shown in Table 2.

Table 2: The values of *$P(D)_{Cal}$* and *$P(D)_{Exp}$* with different values of *$p(d_i)$*

$p(d_i)$	**$P(D)_{Exp}$**			**Average of $P(D)_{Exp}$**	**$P(D)_{Cal}$**
	round 1	**round 2**	**round 3**		
0.1	0.323	0.33	0.36	0.3377	0.3439

0.2	0.61	0.57	0.55	0.5767	0.5904
0.3	0.76	0.77	0.76	0.7633	0.7599
0.4	0.85	0.91	0.87	0.8767	0.8704
0.5	0.93	0.92	0.91	0.9200	0.9375
0.6	1	0.97	0.99	0.9867	0.9744
0.7	1	1	0.99	0.9967	0.9919
0.8	1	1	1	1	0.9984
0.9	1	1	1	1	0.9999
1	1	1	1	1	1

The graph in Figure 17 shows the similarity between the values of $P(D)_{Cal}$ and $P(D)_{Exp}$. The average values of the $P(D)_{Exp}$ agree well with the calculated values. Moreover, the value of $P(D)_{Cal}$ and $P(D)_{Exp}$ both depend on the value of $p(d_i)$ in the same way. If the value of $p(d_i)$ increases, the value of $P(D)_{Cal}$ and $P(D)_{Exp}$ also increase. If the value of $p(d_i)$ decreases then the value of $P(D)_{Cal}$ and $P(D)_{Exp}$ also decrease.

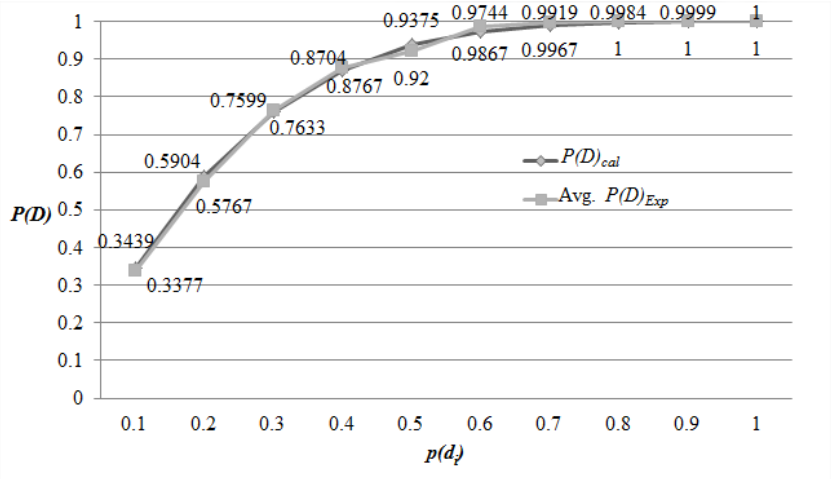


Fig. 17: The value of $P(D)_{Cal}$ versus the average of $P(D)_{Exp}$

The probability analysis result of modified DHCP discovering process was made by comparing the value of $P(MD)$ from calculation ($P(MD)_{Cal}$) with $P(MD)$ from experiment ($P(MD)_{Exp}$) for proving our proposed probabilistic model in Eq. (17).

The researchers tested the probability for the modified DHCP server receiving two out of four DHCP Discover messages ($P(MD)_{Exp}$) three times (round 1, round2, and round 3). To compared average values of $P(MD)_{Exp}$ with $P(MD)_{Cal}$, $P(MD)_{Exp}$ was computed by collecting the number of DHCP Offer messages from sending 100 IP address request to the conventional DHCP server. Each round of the IP address request contained four DHCP Discover messages. The probability of each DHCP Discover messages to be received by the DHCP server was set from 0.1 to 1 in each round of the IP address request. Therefore, the $P(MD)_{Exp}$ is the ratio of the numbers of DHCP Offer messages per the number of IP address request. The values of $P(MD)_{Cal}$ and $P(MD)_{Exp}$ with difference $p(d_i)$ are shown in Table 3.

Table 3: The values of $P(MD)_{Cal}$ and $P(MD)_{Exp}$ with different values of $p(d_i)$

$p(d_i)$	$P(MD)_{Exp}$			Average of $P(MD)_{Exp}$	$P(MD)_{Cal}$
	round 1	round 2	round 3		
0.1	0.05	0.04	0.04	0.0433	0.0523
0.2	0.17	0.16	0.17	0.1667	0.1808
0.3	0.34	0.35	0.34	0.3433	0.3483
0.4	0.59	0.48	0.5	0.5233	0.5248
0.5	0.66	0.74	0.63	0.6767	0.6875
0.6	0.84	0.77	0.84	0.8167	0.8208
0.7	0.93	0.94	0.93	0.9333	0.9162
0.8	0.93	0.99	0.99	0.9700	0.9728
0.9	1	0.99	1	0.9967	0.9963
1	1	1	1	1	1

The graph in Figure 18 shows the similarity between the value of $P(MD)_{Cal}$ and $P(MD)_{Exp}$. The value of $P(MD)_{Cal}$ and $P(MD)_{Exp}$ were both affected by the value of $p(d_i)$ in the same direction. On one hand, if the value of $p(d_i)$ increases then the both value of $P(MD)_{Cal}$ and $P(MD)_{Exp}$ increase. One another hand, if the value of $p(d_i)$ decreases then the value of $P(MD)_{Cal}$ and $P(MD)_{Exp}$ decrease.

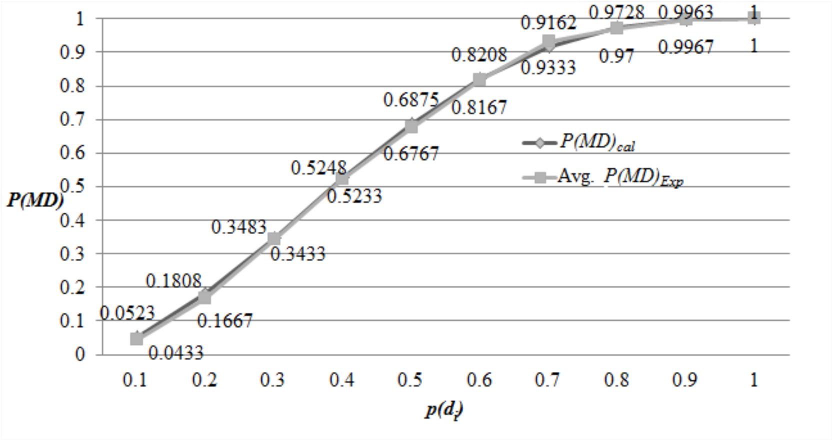


Fig. 18: The values of $P(MD)_{Cal}$ versus the average of $P(MD)_{Exp}$

In Figure 19, the value of $P(D)_{Cal}$ and $P(MD)_{Cal}$ were both affected by the value of $p(d_i)$ in the same direction. The probability of the general DHCP server to receive DHCP Discover message was higher than the modified DHCP server. Since general DHCP server requires only one DHCP Discover message whereas the modified DHCP server requires two DHCP Discover messages to reach the server. However, the value of in $P(D\ and\ MD)_{dif}$ tended to decrease when the values $p(d_i)$ was increased from 0.3 to 1. There was't any difference between $P(D)_{Cal}$ and $P(MD)_{Cal}$ at the value of $p(d_i)$ equal to 1.

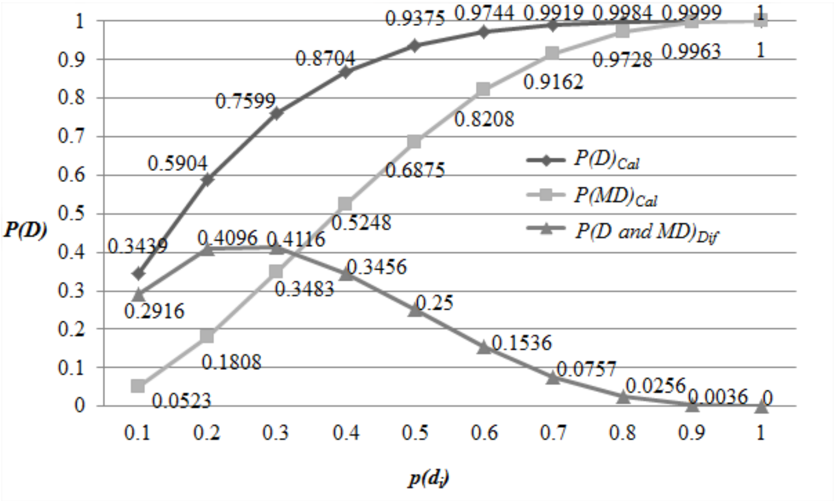


Fig. 19: The difference values of $P(D)_{Cal}$ and $P(MD)_{Cal}$ are in $P(D\ and\ MD)_{dif}$

In the real local area network (LAN), the value of $p(d_i)$ may be affected by any network failures. The cause of a network failure can be divided into physical failure and logical failure. They are commonly known as a hardware failure and a software failure [24]. In case of the hardware failure, the client could not be able to communicate with the other people; this can easily be addressed by checking the network interface and the transmission medium. In the software failure, the client may sometimes able to communicate with each other. This may be caused by the transmission delay and link congestion. By increasing the bandwidth of transmission medium this could reduce the link congestion. Thus, this solution could be considered as an option to minimize the impact of $p(d_i)$.

5.0 CONCLUSION

In this current study, the researchers have proposed the authentication method for DHCP discovering process based on a challenge-response authentication. The results showed that the proposed method can limit the IP addresses requested time by attackers and prevent the DHCP server from the IP address starvation attack by tradeoff with memory consumption and probability of the server to receive DHCP Discover message compared with conventional DHCP server without required any changes in DHCP clients. To avoid the key problem that detectors could not be able to detect the malicious request faster than the attack rate occurs in ICMP based technique, the proposed method can delay the attacker's IP addresses requested time. Consequently, the ICMP based can apply to the server, detect and recover hold IP addresses by the attacker efficiently, since the detection and recovery time was less than the time spent by attacker on obtaining IP addresses. Moreover when comparing with other non-cryptology based techniques, our proposed could be able to work with all existing DHCP-enabled client without the requirement of any modification or additional equipment.

REFERENCES

[1] U. Salasabi, M. T. Ali, M. M. Islam, "A Practical Approach to Asses Fatal Attacks in Enterprise Network to Identify Effective Mitigation Techniques". *International Journal of Computer Networks and Communications Security*, 2(9), 2014, pp. 298-307.

[2] S. Naaz, F. A. Badroo, "Investigating DHCP and DNS Protocols Using Wireshark". *IOSR Journal of Computer Engineering (IOSR-JCE)*, 18(3), 2016, pp.1-8.

[3] M. Yaibuates , R. Chaisricharoen, "ICMP Based Malicious Attack Identification Method for DHCP", In *proceedings of the 4th Joint International Conference on Information and Communication Technology, Electronic and Electrical Engineering (JICTEE)*, 2014, pp.1-5.

[4] M. Yaibuates, R.Upra, R. Chaisricharoen. "ICMP Based IP address Recovery Method for DHCP". In *proceedings of the 6th Global Wireless Summit (GWS)*, 2016, pp.267-271.

[5] R. Droms, "Automated configuration of TCP/IP with DHCP". *IEEE Internet Computing*, 3(4), 1999, pp. 45-53.

[6] R. Droms, "Dynamic Host Configuration Protocol", https://www.ietf.org/rfc/rfc2131.txt , 1997.

[7] M. Khan, S. Alshomrani, S. Qamar, "Investigation of DHCP Packets using Wireshark", *International Journal of Computer Applications*, 63(4),2013, pp. 1-9.

[8] T. Yang, L. Li, Q. Ma, (2012). "Mitigating Aggregated Traffic of DHCP Discover Messages draft-yang-dhc-ipv4-dis-01", https://www.ietf.org/proceedings/84/slides/slides-84-sunset4-11.pdf, 2012.

[9] P. Wilson, "Rogue Servers", *Network Security*, 2003(8), pp. 16-18.

[10] G. Narasimha, M. J. Reddy, "Increasing network efficiency by preventing attacks at access layer", *International Journal of Research in Engineering and Technology*, 3(5), 2014, pp. 37-41.

[11] Cisco Systems, Inc., "Enterprise Mobility 7.3 Design Guide", https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/emob73dg/emob73.html, 2015.

[12] R. Droms, W. Arbaugh, "Authentication for DHCP messages", https://www.ietf.org/rfc/rfc3118.txt, 2001.

[13] J. Demerjian, A. Serhrouchni, "DHCP Authentication Using Certificates", *Security and Protection in Information Processing Systems*. Springer, 2004, pp. 457-472.

[14] Y. I. Jerschow, C. Lochert, B. Scheuermann, M. Mauve, "CLL: A Cryptographic Link Layer for Local Area Networks", in *proceedings of the 6th International Conference on Security and Cryptography for Networks*, 2008, pp.21-38.

[15] C. A. Shue, A. J. Kalafut, M. Gupta, "A Unified approach to intra-domain security", In *proceedings of the12th International Conference on Computational Science and Engineering(CSE)*, 2009, pp.219-224.

[16] S. Duangphasuk, S. Kungpisdan, S. Hankla, "Design and implementation of improved security protocols for DHCP using digital certificates", in *proceedings of the 17th IEEE international conference on Networks*, 2011. pp. 287-292.

[17] D. D. Dinu, M.Togan, (2014). "DHCP server authentication using digital certificates", in *proceedings of the 10th International Conference on Communications (COMM),* 2014, pp.1-6.

[18] O.S. Younes, "A Secure DHCP Protocol to Mitigate LAN Attacks", *Journal of Computer and Communications*, 2016(4). pp. 39-50.

[19] N. Tripathi, N. Hubballi, “Detecting stealth DHCP starvation attack using machine learning approach”, *Journal of Computer Virology and Hacking Techniques*, 2017, pp. 1-12.

[20] Juniper Networks, Inc., “Complete Software Guide for Junos® OS for EX Series Ethernet Switches, Release 12.3” https://www.juniper.net/documentation/en_US/junos12.3/information-products/topic-collections/ex-series/software-all/book-software-ex-series-123-all.pdf, 2013.

[21] Cisco System, Inc., “Using Port Security to Mitigate a DHCP Starvation Attack”, https://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob30dg/SecInteg.pdf, 2007.

[22] H. Mukhtar, K. Salah, & Y. Iraqi, “Mitigation of DHCP starvation attack”, *Computers and Electrical Engineering*, 38(5), 2012, pp. 1115-1128.

[23] N. Hubballi, N. Tripathi, “A closer look into DHCP starvation attack in wireless networks”, *Computers & Security*, 2017(65), pp. 387-404.

[24] Y. Han, X. Zhao, J. Li, “Computer Network Failure and Solution”, *Journal of Computer Hardware Engineering*, 1(1), 2018, pp. 16-26.