ISSN- 2350-0530(O) ISSN- 2394-3629(P)
Impact Factor: 2.035 (I2OR)
DOI: 10.29121/granthaalayah.v4.i2.2016.2825

INTERNATIONAL JOURNAL OF RESEARCH – GRANTHAALAYAH
A knowledge Repository

Science

DYNAMIC DELAY TIME DECISION METHOD FOR ENHANCING SECURITY OF THE FORCED LATENCY INTERLOCK PROTOCOL IN INTERNET OF THINGS

Tae-Ho Cho [*1], Garam-Moe Jeon [2]
[*1, 2] Department of Information and Communication Engineering, SungKyunKwan University, Republic of Korea

ABSTRACT

Most devices in the Internet of Things (IoT) utilize WiMAX communication, and Femtocells are used to provide reliable communication by eliminating shaded areas where wireless signals become weaker with distance and underground facilities. One downfall of this method is the possibility of eavesdropping through Man-in-the-Middle attacks. Forced latency interlock protocol is used to detect these attacks. This protocol uses a fixed latency value and does not consider packet size and distance. In this paper, we propose a dynamic delay time decision method for reducing the fixed delay time of the forced latency interlock protocol in wireless communications based on the IoT. The evaluation function considers the distance between the device, the packet size, and the bit rate of the broadband internet. The simulation experiments demonstrate the validity of our method, which reduces delay time by an average of 88.19% and increases detection rate by an average of 7.97%.

Keywords:
IoT; Femtocell; Man in the Middle; Interlock Protocol; Forced Latency Interlock Protocol.

Cite This Article: Tae-Ho Cho, and Garam-Moe Jeon, "DYNAMIC DELAY TIME DECISION METHOD FOR ENHANCING SECURITY OF THE FORCED LATENCY INTERLOCK PROTOCOL IN INTERNET OF THINGS" International Journal of Research – Granthaalayah, Vol. 4, No. 2 (2016): 151-158.

1. INTRODUCTION

The Internet of Things (IoT) is the interaction of the state with or without user intervention between people/things and things. Many IoT devices configured on the IoT environment can suffer from the shaded area problem or signal weakness due to distance and underground communications in existing networks (WiMAX). When shaded areas cause door lock, refrigerators, washing machines, lighting, and electronic devices such as IoT devices may deteriorate the internet service [1]. This problem can be solved by installing base station (BS) in the shaded area; however, installing them over many shaded areas may expand the area where service is affected.

ISSN- 2350-0530(O) ISSN- 2394-3629(P)
Impact Factor: 2.035 (I2OR)

Femtocells are a cost-effective method of countering the effect of shaded areas [2] and provide reliable communication in IoT. The femtocell is capable of optimal power settings [3] because it uses existing wide area networks in small-output compact mobile communication BS, which are used indoors in areas such as homes and offices. Femtocells also provide service in areas of smaller coverage.

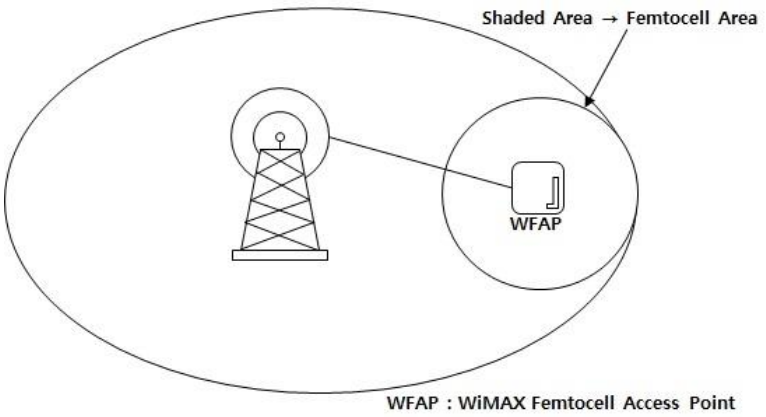

Figure 1: Femtocell

Interlock protocol has been proposed to detect Man-in-the-Middle attacks in wireless communications [4]. However, Bellovin and Merritt prove the vulnerability of the interlock protocol by demonstrating Man-in-the-Middle attacks [5]. Then, forced latency interlock protocol has been proposed. However, Forced latency interlock protocol uses a fixed forced delay [6] and has been proposed to improve the Man-in-the-Middle attack detection.

This paper proposes a method for adjusting the forced delay time depending upon the actual distance of the devices. We use the evaluation function in order to determine this delay. The evaluation function must consider the distance and packet size of the two devices within the range of WiMAX femtocells; the delay time is proportional to the distance and packet size.

The rest of the paper is structured as follows. Section 2 introduces the interlock and forced latency interlock protocols, a proposed method overview is presented in Section 3, and Section 4 provides the experimental results. Conclusions and areas for future work are presented at the end of this paper.

2. BACKGROUND

2.1.INTERLOCK PROTOCOL

Interlock protocol is based on wireless communication and is applicable in WiMAX femtocells [4]. Interlock protocol compensates for the public key cryptosystem and provides secure communication for normal wireless communication; this protocol has been proposed to expose eavesdropping generated from Man-in-the-Middle attacks. The data transmission method of this protocol is shown below.

ISSN- 2350-0530(O) ISSN- 2394-3629(P)
Impact Factor: 2.035 (I2OR)

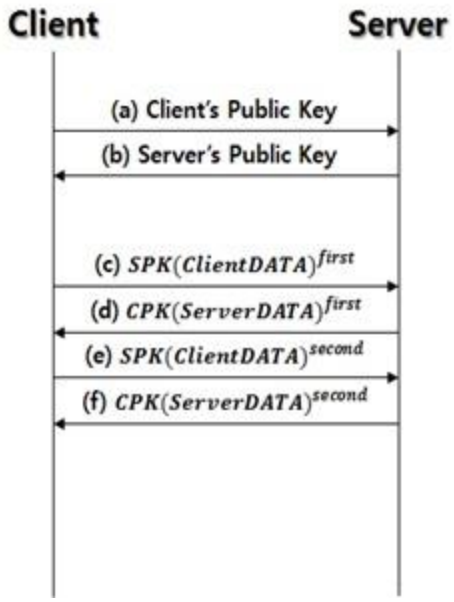

Figure 2: Interlock Protocol

The process of the interlock protocol is shown in Figure 2. The Client and Server each have their own secret key, as follows:

a) The Client sends his public key to the Server.
b) The Server sends his public key to the Client.
c) The Client is encrypted with the Server's public key and sends half of the encrypted data to the Server.
d) The Server is encrypted with the Client's public key and sends half of the encrypted data to the Client.
e) The Client sends the other half to the Server.
f) The Server gathers the two parts of the data received from the Client and decrypts them using its private key. The Server sends the other half to the Client. Finally, the Client gathers the two parts of the data received from the Server, and decrypts it with his private key. In this protocol, each step is performed after receiving the information transmitted in the previous step.

2.2.FORCED LATENCY INTERLOCK PROTOCOL

In their work, Bellovin and Merritt presented a case of successful Man-in-the-Middle attacks on the interlock protocol.

ISSN- 2350-0530(O) ISSN- 2394-3629(P)
Impact Factor: 2.035 (I2OR)

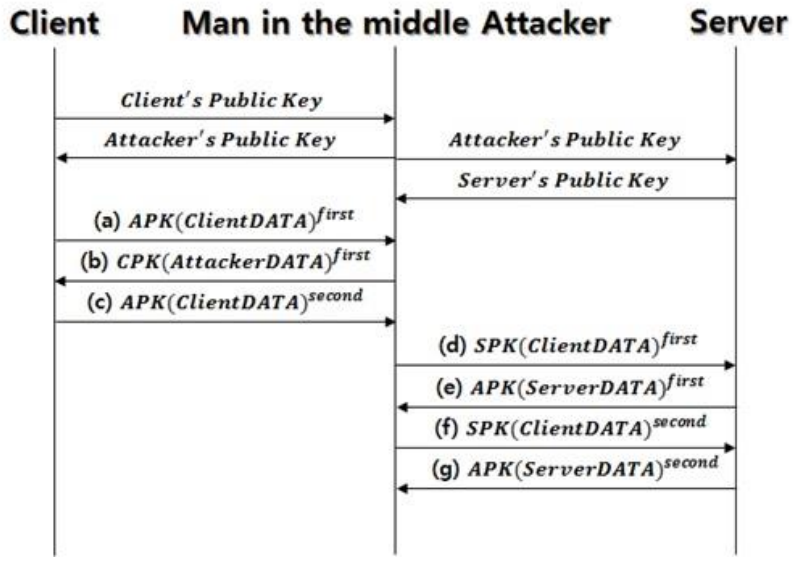

Figure 3: Successful Attack on the Interlock Protocol

The successful Man-in-the-Middle attack scenario is shown in Figure 3. The attacker is involved when the client and the server exchange public keys. After the client and server's public keys are intercepted to hand out the attacker's public key, the subsequent procedure is:

a. The Client sends half of the encrypted data to the Server, but the attacker intercepts it.
b. The attacker encrypts the data with the Client's public key and transmits half of the encrypted data to the Client.
c. The Client cannot properly check the values. The Client sends the other half to the Server, but the attacker intercepts it.

The attacker then combines the two data received from the client with his private key to decrypt and re-encrypt using the Server's public key divided in half.

d. The Attacker sends half of the encrypted data to the Server.
e. The Server sends half of the encrypted data to the Client, but the Attacker intercepts it.
f. The Attacker sends the other half to the Server.
g. The Server sends the other half to the Client, but the Attacker intercepts it.

The attacker is capable of normal communications with the server and alerts the client of network errors or exceptions. In this way, it is possible to mitigate the client's doubts. The attacker then sends the data received from the client to the server and he can authenticate both the server and the client. A forced latency interlock protocol has been proposed to address these problems [7, 8].

ISSN- 2350-0530(O) ISSN- 2394-3629(P)
Impact Factor: 2.035 (I2OR)

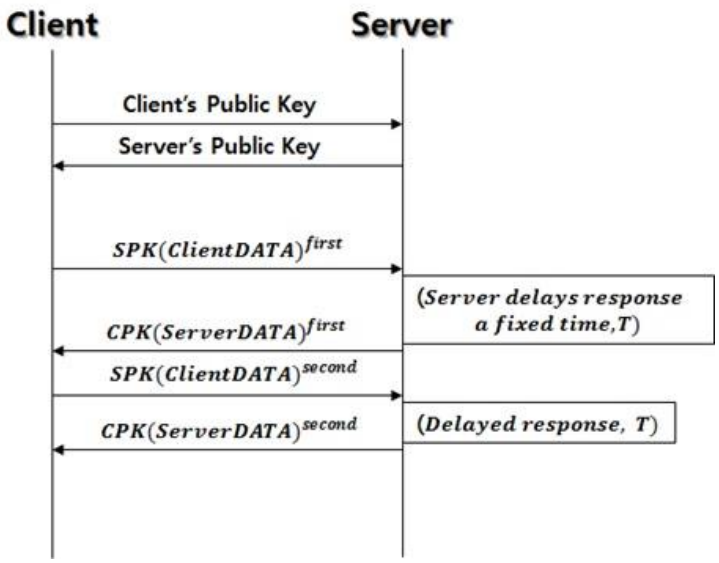

Figure 4: Forced Latency Interlock Protocol

3. PROPOSED METHOD

In the conventional technique using a fixed delay time, the packet transmission time may be less efficient than the interlock protocol that does not use delay time. This paper proposes a method for determining the dynamic delay time using the evaluation function and efficient delivery to shorten the delay time [9, 10]. The proposed evaluation function takes three input values:

Distance: This value is the distance between the devices. The maximum value is within the average range of the femtocell. In the evaluation function, longer distances will increase the delay time.
Packet Size: This value is the size of data to transmit. In the evaluation function, longer distances will increase the delay time.
Bit Rate: This value is the rate of the broadband internet network. The maximum value is within the average bit rate of WiMAX.

The evaluation function of the proposed method is as follows:

$$\mathrm{H}(\mathrm{d},\mathrm{p}) = \frac{Distance}{Propagation\ Speed} \times \frac{Packet\ Size}{Bit\ Rate}, \qquad (1)$$

Where d is the *Distance*, p is the *Packet Size*, and $\mathrm{H}(\mathrm{d},\mathrm{p})$ is an algorithm used in the session. For example, if the *Distance* is 1000 m and the *Packet Size* is 100 kb, then the *Bit rate* is 70 mbit/s and the delay time is 3.72 nanoseconds. The proposed method can be applied flexibly and at a rapid rate.

4. EXPERIMENTAL RESULTS

This section provides the experimental results. The initial parameters are discussed in Section 4.1, and the results are presented in Section 4.2.

ISSN- 2350-0530(O) ISSN- 2394-3629(P)
Impact Factor: 2.035 (I2OR)

4.1.INITIAL PARAMETERS

Table 1: The initial parameters

Parameter	**Value**
Distance	30 (1 - 30 m)
Packet Size	8 MB
Bit Rate	70 mbit/s
Attack Ratio	100%
The Number of Attack	1,000,000

In the first experiment, we used Distance, Packet Size, and Bit Rate. The second and third experiments added Attack Ratio and the Number of Attack.

4.2.RESULTS

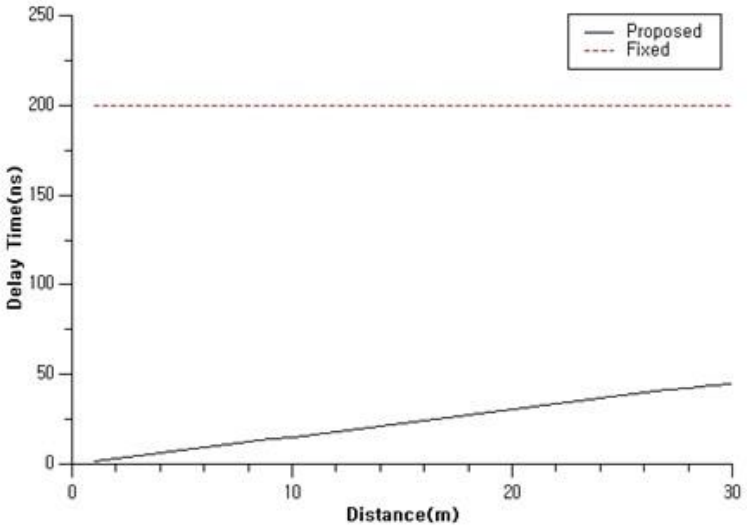

Figure 5: Delay Time versus the Distance

Conventional techniques utilize fixed delay time within a radial range; however, the proposed method increases the delay time versus the distance and is faster than existing techniques, as shown in Figure 5.

ISSN- 2350-0530(O) ISSN- 2394-3629(P)
Impact Factor: 2.035 (I2OR)

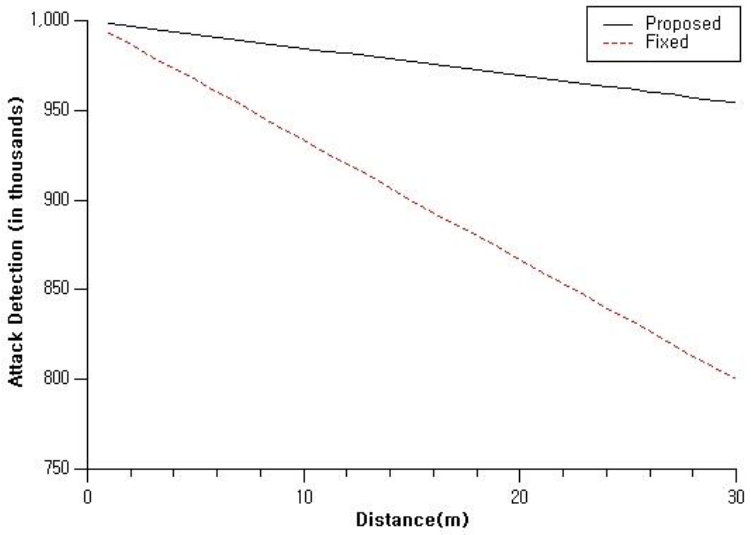

Figure 6: Attack Detection versus Distance

As shown in Figure 6, the attack occurred a million times per meter. The number of detected attacks drops sharply with distance in the conventional technique, and slowly in the proposed technique.

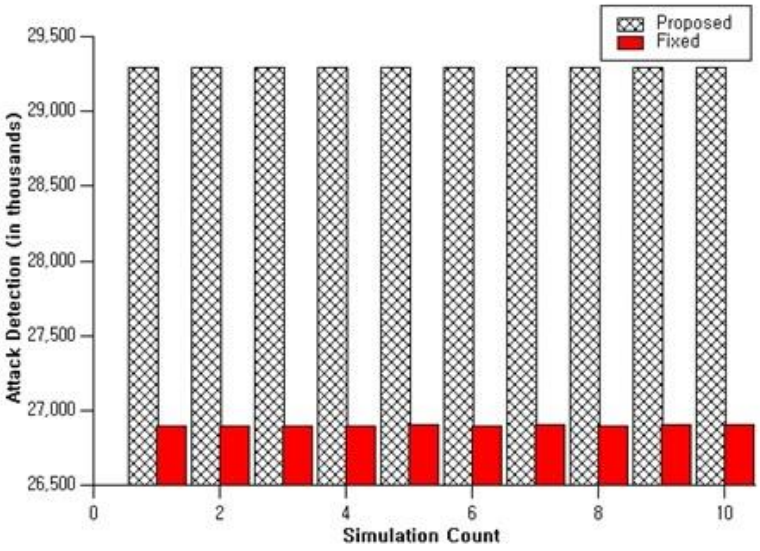

Figure 7: Attack Detection versus the Simulation Count

Figure 7 shows the results of 10 simulations, where the number of detected attacks is higher under the proposed method than in the conventional technique.

5. CONCLUSION

Man-in-the-Middle attacks can be used on WiMAX femtocell to eavesdrop data between two devices. In the past, forced latency interlock protocol was proposed to counter these attacks using a fixed delay time. The proposed method dynamically changes the delay time according to the

ISSN- 2350-0530(O) ISSN- 2394-3629(P)
Impact Factor: 2.035 (I2OR)

packet size and distance, and is shown to more efficiently reduce the delay time compared to conventional techniques. We also observed improved attack detection using our method. In order to further improve our method in the future, we will increase the distance accuracy of wireless communication devices.

6. ACKNOWLEDGEMENTS

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (No. NRF-2015R1D1A1A01059484).

7. *REFERENCES*

[1] *K. Scarfone, C. Tibbs and M. Sexton, "Guide to securing WiMAX wireless communications," NIST Special Publication, vol. 800, pp. 127, 2010.*
[2] *V. Chandrasekhar, J. G. Andrews and A. Gatherer, "Femtocell networks: a survey," Communications Magazine, IEEE, vol. 46, pp. 59-67, 2008.*
[3] *R. Y. Kim, J. S. Kwak and K. Etemad, "WiMAX femtocell: requirements, challenges, and solutions," Communications Magazine, IEEE, vol. 47, pp. 84-91, 2009.*
[4] *R. L. Rivest and A. Shamir, "How to expose an eavesdropper," Commun ACM, vol. 27, pp. 393-394, 1984.*
[5] *S. M. Bellovin and M. Merritt, "An attack on the interlock protocol when used for authentication," Information Theory, IEEE Transactions On, vol. 40, pp. 273-275, 1994.*
[6] *Interlock Protocol. Available: https://en.wikipedia.org/wiki/Interlock_protocol.*
[7] *Forced-Latency Interlock Protocol. Available: http://www.liquisearch.com/interlock_protocol/forced-latency_interlock_protocol.*
[8] *Forced-Latency Interlock Protocol. Available: http://www.cisa.umbc.edu/papers/theses/newton-thesis-2010.pdf.*
[9] *B. Forouzan, C. Coombs and S. C. Fegan, Introduction to Data Communications and Networking. McGraw-Hill, Inc., 1997.*
[10] *J. F. Kurose and K. W. Ross, Computer Networking: A Top-Down Approach. Addison-Wesley, 2007.*