TAF
Journal of Applied and Physical Sciences
2016, 2(2): 37-41
JAPS

PRIMARY RESEARCH

A method for detecting man-in-the-middle attacks using time synchronization one time password in interlock protocol based internet of things

Tae-Ho Cho [1,*], Garam-Moe Jeon [2]

[1, 2] Department of Information and Communication Engineering, Sungkyunkwan University, Seoul, South Korea

Index Terms
Internet of Things
One-time Password
Interlock Protocol
WiMAX Femtocell

Received: 7 May 2016
Accepted: 8 June 2016
Published: 24 June 2016

Abstract— Internet of Things (IoT) is used for devices to interact with each other, and Femtocells are used to provide reliable communication by eliminating shaded areas where wireless signals have become weak. IoT security is crucial since the untethered nature of wireless networks primarily allows for eavesdropping threats to confidential information. Therefore, the interlock protocol is proposed to protect confidential information that is prone to eavesdropping due to the use of an unsecure public key. This paper addresses this limitation through a countermeasure that combines the time synchronization one-time password (OTP) and the interlock protocol. In the proposed method, we use OTP for authentication before transmitting the public key and data. In order to counter eavesdropping attacks, the OTP should be first used to detect the attacker. Simulations show that both methods have up to 46% of detection rate. However, our method has a prevention rate that is 54% higher than that of the interlock protocol.

I. INTRODUCTION

The internet protocol (IP) has enabled for Internet of Things (IoT) devices to be interconnected and to interact. The internet protocol (IP) has enabled for Internet of Things (IoT) devices to be interconnected and to interact [1]. IoT devices are used in wide area networks (WANs), such as in WiMAX, and shadowed areas should be illuminated to ensure uninterrupted communication. The shadow area problem is where there is an interruption in wireless signals due to a shadow or to signal fading with distance. A femtocell is a prevalent type of IoT device that eliminates this problem [2]. However, the femtocell is susceptible to Man-in-the-middle (MITM) attack [3] because wireless signals can be tapped from outside the premises. The interlock protocol was thus proposed to detect such an attack [4]. In the interlock protocol, data are encrypted using a public key and are then transmitted in two equal segments. This protocol has been proposed in order to detect eavesdropping by an MITM attack since without a countermeasure, security can easily be compromised if the public key has been exposed [5].

We have applied a time synchronization-based One-

*Corresponding author: Tae-Ho Cho
E-mail: thcho@skku.edu

Time Password (OTP) to improve the performance of the interlock protocol [6]. The time synchronization OTP generates an OTP value by using the key and the time [7] parameters at the client end. At the server, another OTP value is generated for comparison with the OTP value of the client in order to validate the data. The time synchronization OTP changes the OTP value using the time parameter, and thus, an attacker cannot be re-certified in the case of eavesdropping. The method proposed in this paper combines the time synchronization OTP and the interlock protocol to further safeguard the interlock protocol. The proposed method authenticates the client using the OTP prior to the exchange of public keys. This method improves security by detecting an attack through authentication. It may be difficult for the adversary to launch the MITM attack due to the OTP authentication. The MITM attack in the proposed method can be detected before the exchange of public keys, and thus the proposed method uses the OTP with additional authentication to obtain a high rate of prevention against eavesdropping.

The rest of the paper is structured as follows. Section 2 introduces the OTP and the interlock protocol. The proposed method overview is presented in Section 3, and Section 4 provides the experimental results. The conclusion and future work are provided at the end of this paper.

II. BACKGROUND

This section provides background information. In Section 2.1, it describes the generation method and advantages and disadvantages of OTP, and in Section 2.2 also explains the process and the introduction of the interlock protocol.

A. OTP

An OTP is used in a one-time password authentication system [8] as additional authentication security after the username and password have been input. It is used in games and in internet banking, and the methods with which to generate the OTP consist of time synchronization [7] and event synchronization [9]. The time synchronization method is shown in Figure 1.

(a) OTP Generator generates an OTP by time and private key

(b) The user enters the OTP value into the login server and waits for the login authentication

(c) The login server transmits the user's secret key to the OTP server

(d) The OTP server generates an OTP value using the user's secret key and the time value.

(e) The login server compares the OTP value generated by the OTP server and the OTP generator for authentication.

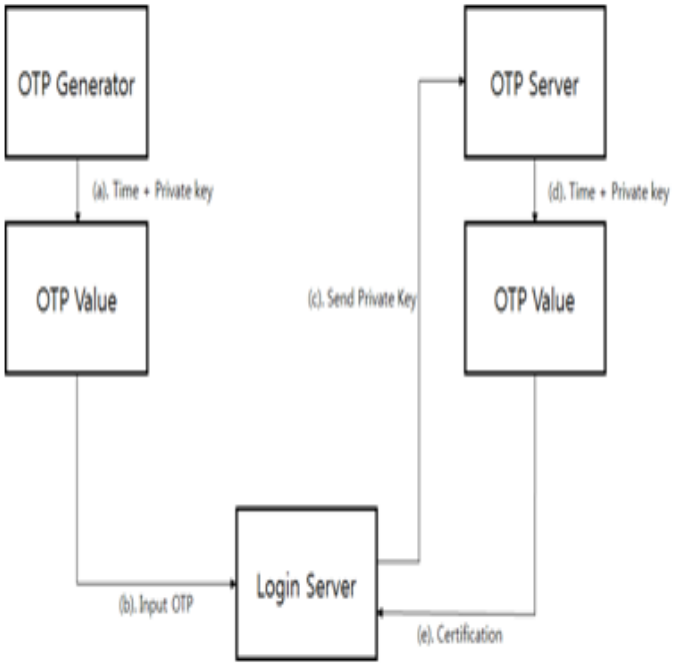

Fig. 1. Time synchronization OTP

If the time synchronization value of the OTP is not equal to the time of the OTP Generator and OTP Server, authentication fails. A 30-second OTP generation interval is recommended to compensate for a failure to authenticate.

Secondly, the event synchronization OTP is one where there is an equal increase in the count of the OTP server and the OTP generator, after generating the OTP as the count value. If the OTP Generator generates an OTP and is not authorized by the OTP Server, then the count value is different. To address this problem, a method to receive a sequence of OTP is used in order to determine the efficacy when the count is observed to be different.

B. Interlock Protocol

The interlock protocol is proposed in order to prevent eavesdropping [4]. It designed to ensure security by both parties in order to use a key exchange protocol. The interlock protocol process is shown in Figure 2 [10].

ISSN: 2414-3103
DOI: 10.20474/japs-2.2.2

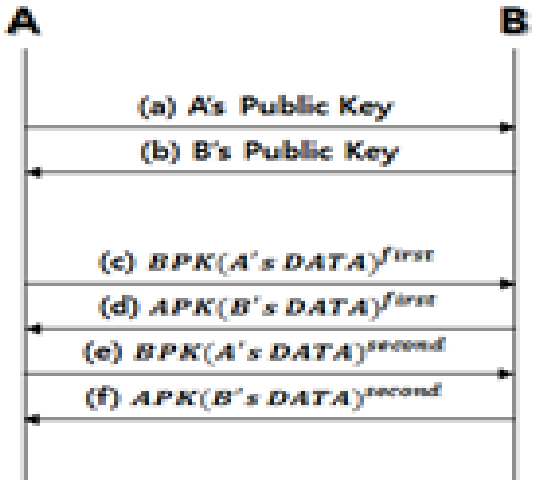

Fig. 2. Interlock protocol

A and B have their own secret key as follows:
(a) A sends his public key to B.
(b) B sends his public key to A.
(c) A is encrypted with B's public key and sends half of the encrypted data to B.
(d) B is encrypted with A's public key and sends half of the encrypted data to A.
(e) A sends the other half to B. B gathers the two parts of the data received from A and decrypts them using its private key.
(f) A gathers the two parts of the data received from B and decrypts them using its private key.

III. PROPOSED METHOD

A. Assumption

The first assumption is that in the man in the middle attack, an attacker has a 50% probability of data tampering and 50% probability of eavesdropping. The second assumption is to continue from the beginning to the end of the protocol when the attacker is eavesdropping or data tampering.

B. Operation

The interlock protocol is susceptible to a security breach when the public key has been exposed. This problem arises in the case where communication is intercepted by a MITM attack before exchanging public keys. The MITM attack sends its own public key to intervene in the communication between A and B, and receives the public key of A and B after receiving normal data from each of A and B. In this paper, we proposed a method to detect the attack by combining interlock protocol and time synchronization OTP. Our method results in a decrease in data tampering. The proposed method is shown in Figure A and B each have one public key and common key.

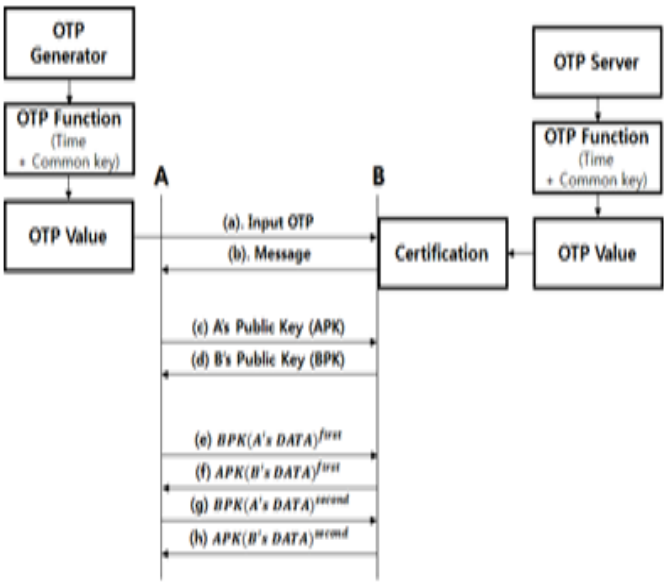

Fig. 3. Proposed method

(a) A sends a certificate to B with the OTP value generated by the OTP generator. (b) B is demonstrated by comparing the values received from OTP value generated by the OTP server and A, after B transmits an authentication message to A. (c) The rest of the procedure is the same as that for the interlock protocol. For further details of the interlock protocol, see Section 2.2.

In the proposed method, OTP authenticdation can protect the public key even if the OTP has been intercepted, and thus an attacker cannot distinguish normal messages. Therefore, A will not transmit data to B to detect the attacker.

IV. EXPERIMENTAL RESULTS

This chapter provides experimental results of the chance to detect an eavesdropper of the OTP with the proposed method. The initial parameters are discussed in Section 4.1, and experimental results are presented in Section 4.2.

ISSN: 2414-3103
DOI: 10.20474/japs-2.2.2

A. Experiment Environment

TABLE 1
The Initial Parameters

Parameter	Value
Attack count	100
Attack ratio	100%
data tampering ratio	50%
data eavesdropping ratio	50%

The attack count is 100 times if an MITM attack. The attack rate was 100% of the attacker eavesdropping or enacting data changes. Then, the data tampering ratio is set to 50% and data eavesdropping to 50%.

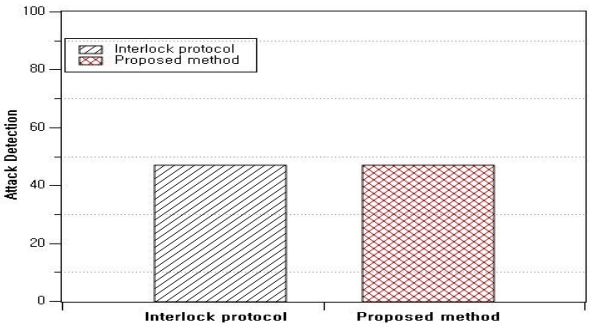

Fig. 4. Attack detection rate

Figure 4 shows the attack detection rate of the interlock protocol and the proposed method. These show the same detection rates.

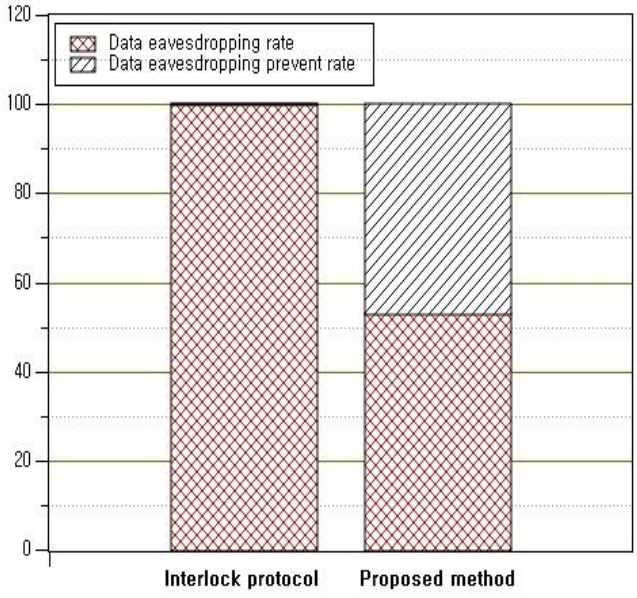

Fig. 5. Data eavesdropping rate

Figure 5 shows the data eavesdropping rate and the data eavesdropping prevention rate. The interlock protocol can be detected after an attacker has been eavesdropping on the data. Therefore, the data rate of the MITM attack is 100%. However the proposed method can detect an attack through the use of the OTP, before data communication. As a result of the experiment, the attacker eavesdropping rate is 54%, and the rate of eavesdropping prevention is 46%.

V. EXPERIMENTAL RESULTS

A WiMAX femtocell is susceptible to an MITM attack due to the ease of access through external communication. Thus, the interlock protocol has been used to detect an MITM attack, and this protocol has a structure whereby data is encrypted and transmitted by splitting it in half. The security of the interlock protocol is weakened when public keys are eavesdropped before data transmission, and thus the proposed method incorporates an OTP with the interlock protocol to significantly lower the eavesdropping with a public key. The attacker is required to authenticate before data transfer, which results in failure and indicates an MITM attack. The results of this paper show that the interlock protocol and the proposed methods have the same attack detection rates but the proposed method significantly increases eavesdropping prevention. In order to further improve our method in the future, we will increase the detection rate by increasing the length of the time parameter in the OTP.

ACKNOWLEDGMENT

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)

REFERENCES

[1] J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Comput Syst,* vol. 29, pp. 1645-1660, 2013. **DOI:** 10.1016/j.future.2013.01.010

[2] V. Chandrasekhar, J. G. Andrews and A. Gatherer, "Femtocell networks: a survey," *Communications Magazine, IEEE,* vol. 46, pp. 59-67, 2008. **DOI:** 10.1109/MCOM.2008.4623708

[3] N. Saquib, E. Hossain, L. B. Le and D. I. Kim, "Interference management in OFDMA femtocell

networks: issues and approaches," *Wireless Communications, IEEE,* vol. 19, pp. 86-95, 2012. **DOI:** 10.1109/MWC.2012.6231163

[4] R. L. Rivest and A. Shamir, "How to expose an eavesdropper," *Communications of the ACM,* vol. 27, pp. 393-394, 1984. **DOI:** 10.1145/358027.358053

[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. **DOI:** 10.1109/18.272497

[6] T. Tsuji and A. Shimizu, "A one-time password authentication method for low spec machines and on internet protocols," *IEICE Transactions on Communications,* vol. 87, pp. 1594-1600, 2004.

[7] D. M'Raihi, S. Machani, M. Pei, J. Rydell, "TOTP: Time-based one-time password algorithm," Request for Comments (RFC), 6238, 2011.

[8] Haller, Neil, Craig Metz, Phil Nesser, and Mike Straw. "A one-time password system." Request for Comments (RFC), 1998.

[9] D. M'Raihi, M. Bellare, F. Hoornaert, D. Naccache and O. Ranen, Hotp. *An hmac-based one-time password algorithm*, 2005.

[10] T. H. Cho and G. M Jeon, "Dynamic delay time decision method for enhancing security of the forced latency interlock protocol in internet of things," *International Journal of Research-Granthaalayah (IJRG),* vol. 4, pp. 1-8, 2016.

— This article does not have any appendix. —

ISSN: 2414-3103
DOI: 10.20474/japs-2.2.2