Bi-AM : Bilateral Authentication on MIPv6 in IoT

Yunjung Lee

Abstract Background/Objectives: ***This paper proposes a method to provide security to Mobile IPv6 (MIPv6), a protocol for supporting the mobility of IoT devices.***

Methods/Statistical analysis: ***This paper presents a security protocol for binding update bi-directional authentication, which can be used in limited IoT and MIPv6 environments without using IPSec.***

Findings: ***It reduces the load on the network and the computational cost of each node since the key-based key pair is used. The size of the exchanged protocol message is also less than existing protocols.***

Improvements/Applications: ***It can exchange a minimum number of messages in an IoT environment with limited computing power.***

Keywords: IoT Security, MIPv6, Authentication, IPSec, IKE

I. INTRODUCTION

The future Internet will provide a ubiquitous mobile Internet environment that is even larger than today's. The support of mobility is increasing the applicability of future Internet to new areas. Mobile platforms such as smartphones and tablets enable a tremendous range of applications based on ubiquitous location, context awareness, social networking and interactions with the environment.

The potential of the future Internet is not limited to smartphones. Internet of Things (IoT) is a new area of the future Internet that brings evolutionary artificial intelligence and integration to the real world one step further. The main goal of IoT is to collect data from real objects and events [1].

There is a myriad of scenarios (e.g. IoT biosensors attached to the human body) that are used in real environments by attaching IoT devices to objects that need to be guaranteed mobility. Therefore, dealing with mobility and dynamic systems is a core requirement of IoT solution and therefore appropriate support should be provided. These IoT devices are often placed in limited resources and environments in power consumption, computing, communications, memory, and so on. In this paper, we propose a method to provide security to Mobile IPv6 (MIPv6) [2], a protocol for supporting the mobility of IoT devices [3].

MIPv6 is a system that adds a standard for mobility above the next generation IPv6 protocol. Figure 1 shows a scenario in which IoT is a mobile node (MN) in MIPv6. The basic components of MIPv6 are the MN, the correspondent node (CN), a home network, a home agent (HA), a home address (HoA), and a care-of address (CoA). The area of interest of this paper is to provide an efficient lightweight authentication method for Binding Update (BU) to inform HA of CoA and HoA of MN. During the binding update process, an attacker can apply CoA forgery attacks, replay attacks, man-in-the-middle attacks, and DoS attacks. In order to effectively defend these, IPSec can be used. When IoT devices with limited availability, such as low power and low memory, are mobile nodes (MN) or correspondent nodes (CN), Authentication and security for IPSec [4, 5] using many resources are practically difficult to apply.

This paper describes a security protocol for bidirectional authentication of binding update messages in Mobile IPv6 (MIPv6) environment. Here, the MN and the CN can authenticate the HoA ownership of the MN by hashing the public key and the HoA with the private key, thereby preventing man-in-the-middle attack. Time-Stamps also helps prevent replay attacks. This paper proposes a protocol that satisfies both the authentication and the public key exchange optimized for both sides of the communication subject with minimum modification based on the message exchange of MIPv6.

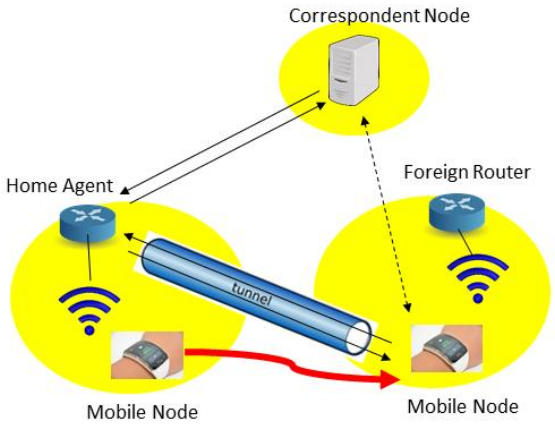

Figure 1. IoT-MN Mobility Scenario on MIPv6

The composition of this paper is as follows. Chapter 2 discusses mobility management technologies and security requirements to consider for mobility updates, and discusses related research. In Chapter 3, the protocol proposed in this paper is described in detail. In Chapter 4, security and performance Analysis of the proposed protocol are verified by comparing the

Revised Manuscript Received on May 22, 2019.

Yunjung Lee*, Computer Science and Statistics Department, Jeju National University, Jeju, South Korea, rheeyj@jejunu.ac.kr

results with the previous studies. Finally, conclusions are made in Chapter 5.

II. SECURITY ISSUES AND RELATED STUDIES

This section discusses mobility management technologies and security requirements to consider for mobility updates, and discusses related research.

2.1. *Binding Update Security Issues*

In the binding update in MIPv6, there are two cases of registering the CoA received from the network to which the mobile node MN has moved to the home agent HA and informing the correspondent node CN of its CoA to optimize the route [6].

The security problems that can occur in binding update are as follows. First, a man-in-the-middle attack due to CoA or HoA modulation. (1) Modification CoA: When an MN sends a BU message to the HA, the attacker intercepts the BU message and modifies the CoA to give information that the MN is located at a different place from the current location. If this information is received, the MN will not receive the packet, while the other node receives the unwanted packet. (2) HoA Modulation: When sending a BU message to the CN, if the malicious MN sets its HoA to the victim's HoA and informs the false information, if the CN accepts this information, the attacker's MN is subject to both the availability and the confidentiality of the packet. Second, DoS attack: If the attacker MN informs its CoA to false, the CN can send DoS attacks by transmitting all packets to the mobile terminal with a false CoA. If the CN sends a lot of meaningless binding update messages at once, the CN may deplete the resource before attempting to perform a DoS attack on the CN before noticing that the message is not valid. Third, retransmission attack: the attacker can replay the old binding update message and forward the packets to the old location of the MN so that the MN cannot receive the packet.

In order to prevent such attacks, HA uses IPsec Encapsulation Security Payload (ESP) to protect the packet when the MN delivers the binding update message. When transmitting the binding update message to the CN, the RR (Return Routerbility) is used as the basic mechanism for security. And HoA and CoA can be reached, and then the message is transmitted [7].

However, when IoT devices with limited availability such as low power and low memory are MN or CN, authentication and security using IPSEC using many system resources and network resources are practically difficult to apply. The key exchange mechanism used in IPsec is the IKE protocol, which has the drawback of requiring too many messages to be exchanged and requiring storage of state information for the ongoing key exchange parties. Storing state information can easily be exploited for denial-of-service attacks through memory consumption, and many of the exponential calculations involved in IKE have vulnerabilities to distributed denial-of-service attacks. The ideal goal of security for binding update is to ensure that only the mobile node whose home address is HoA and whose care-of address is CoA can send a binding update message containing <HoA, CoA> [6].

2.2. Related Studies

[8] proposed a technique to improve authentication of PMIPv6 and handover procedures. Since PMIPv6 is a network-based mobility management technology, the signaling overhead imposed on the MN is reduced because the mobile node MN does not participate in mobility management. However, it has complex authentication procedures, packet loss, and security threats. In addition, although the authentication delay is eliminated by only using the symmetric key and hash, the overhead still occurs due to the use of IPsec.

[9] proposed secure authentication between MN and distributed anchor through dynamic tunneling in DMM. As a mutual authentication method for authenticating an MN, a cost is incurred by using a general server client model.

[10] proposed a technique for providing unidirectional authentication between the MN and the HA, and between MN and CN for binding updates. However, although a single authentication message including a hash and a public key is intended to solve the problem of authentication, integrity, and retransmission prevention, in consideration of a confirmation message from the other party, authentication is impossible. Also, DoS attacks are not considered.

This paper proposes a security protocol for binding update bi-directional authentication, which can be used in limited IoT and MIPv6 environments without using IPSec. Here, the MN and the CN can authenticate the HoA ownership of the MN by hashing the public key and the HoA with the private key, thereby preventing the replay attack. In addition, retransmission attacks can be prevented through time-stamp.

III. PROPOSED MIPV6 AUTHENTICATION PROTOCOL (BI-AM)

In this paper, we consider an Elliptic curve cryptography (ECC) public key scheme considering IoT environment with limited resources. The key length of the RSA scheme is about 1024 bits, while the key length of the ECC is as short as 160 bits, and the computation amount is significantly less than that of the RSA, while providing a similar level of safety, which is essential for IoT devices. The proposed protocol proceeds as follows. When the mobile node is first initialized, ECC public key pair (public key and private key) are created and immediately stored in secure local storage.

The overall process of MIPv6 with Bi-AM protocol is shown in Figure 2.

Step 1: When MN moves to another network, it performs Bi-AM protocol for authentication between MN and HA before sending Binding Update to HA.

Step 2: The MN sends an HA-authenticated binding update message to the HA.

Step 3: The HA sends a binding acknowledgment message

authenticated by the Bi-AM method to the MN.

Step 4: When a packet transmission request is received from the CN to the MN, the MN, HA, and CN perform a Return Routability (RR) procedure for Route Optimization.

Step 5: Perform the Bi-AM protocol for authentication of the binding update process between MN and CN.

Step 6: The MN sends a CN-authenticated binding update message to the CN.

Step 7: The CN sends an MN-authenticated binding confirmation message to the MN.

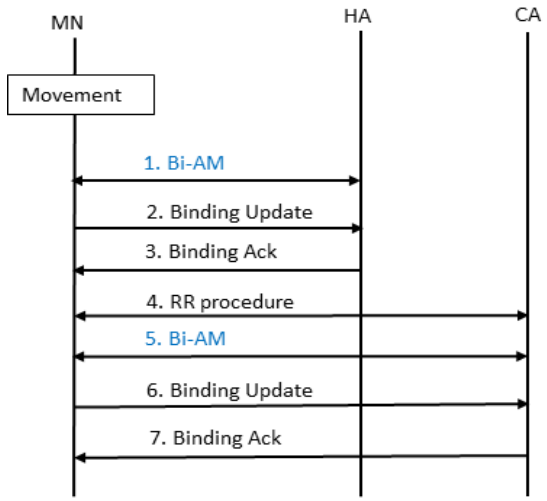

Figure 2. Message Sequence with Bi-AM on MIPv6

The Bi-AM protocol is applied to authentication for binding updates between <MN, HA>, <MN, CN>. It is assumed that the RR procedure is responsible for the authentication and security of the Route Optimization process.

The following notation is used to describe the Bi-AM protocol :***M*** is the mobile node MN, ***C*** is the HA or CN**,** ***A'm*** is the CoA of ***M***, Am is the HoA of ***M,*** and ***Ac*** is the address of ***C, (PKm, SKm)*** is a pair of ECC (public key, private key) of ***M***, ***H(m)*** is a hash of ***M***, ***Tm*** is a time stamp of ***M***, and ***{m} SKm*** is a signature of ***M*** using key ***SKm***.

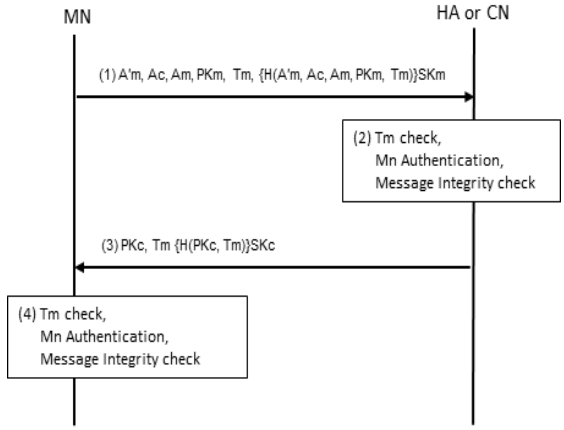

Figure 3. Bi-AM Protocol in MIPv6 Binding Update Procedure

Bi-AM protocol [Figure 3] is as follows.

Step 1: ***M*** sends a Bi-AM Hello message including ***Cm (A'm, Ac, Am, PKm, Tm, {H (A'm, Ac, Am, PKm, Tm)} SKm)***.

Step 2: ***C*** checks Time-Stamp ***Tm*** to prevent Replay-Attacks, and verifies ***{H (A'm, Ac, Am, PKm, Tm)} SKm*** with the public key ***PKm*** of ***M*** and then generates the hash value of ***H (A'm, Ac, Am, PKm, Tm)***, and compares it and the transmitted hash value ***H (A'm, Ac, Am, PKm, Tm)*** to confirm authentication and message integrity for ***M***. If they do not match, ***C*** ignore the entire message.

Step 3: ***C*** sends a ***Bi-AM ACK*** message including ***(PKc, Tm {H (PKc, Tm)} SKc)*** if there is no problem in the authentication process in Step 2.

Step 4: ***M*** checks Time-Stamp ***Tm*** to prevent Replay-Attacks, and verifies ***{H(PKc, Tm)}SKc*** with the public key ***PKc*** of ***C*** , then generates the hash value ***H(PKc, Tm)*** , and compares it and the transmitted hash value ***H(A'm, Ac, Am, PKm, Tm)*** to confirm authentication and message integrity for ***C***. If they do not match, ***C*** ignore the entire message and do not proceed with further binding updates.

The following MIPv6 binding update and authentication for binding response messages are as follows.

Step 1: ***M*** sends ***C*** the whole binding update of ***M*** and Time-Stamp ***Tm*** to ***M***'s private key ***SKm*** and sends it to ***C***.

Step 2: ***C*** verifies the received value with ***M***'s public key ***PKm***.

Step 3: After Step 2, ***C*** sends the entire binding response of ***C*** signed by ***C***'s private key ***SKc*** and sent to ***M.***

Step 4: ***M*** verifies the received value with ***C***'s public key ***PKc***.

IV. SECURITY ANALYSIS AND PERFORMANCE ANALYSIS

In this section, security and performance Analysis of the proposed protocol are verified by comparing the results with the previous studies

4.1. Binding Update Security Issues

(1) CoA forgery attack

The attacker can forge a CoA of the MN in the binding update (BU), and ultimately, intercept the packet headed to the MN. Therefore, the HA verifies the BU message with the MN's public key ***PKm*** obtained in the Bi-AM protocol process. If the HA message does not match, the

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

HA can ignore the BU message and prevent the CoA attack from being stored in the binding cache.

(2) Replay attack

The attacker can retransmit the old binding update (BU) message and apply a retransmission attack that directs the packet to the MN other than the current MN. The Bi-AM protocol includes a timestamp ***Tm*** in the binding update (BU) and the receiver verifies the validity of the timestamp and discards the packet if it does not match.

(3) Man-in-the-middle attack

The attacker can intercept packets transmitted between the MN and the HA or between the MN and the CN and attack the intermediary to modulate the BU. In the Bi-AM protocol, the HA or the CN has the public keys ***PKm*** and Tm of the MN, thereby confirming the integrity of the message. If the HA or the CN cannot validate the message integrity, it can defend the message by discarding the message.

(4) DoS attack

An attacker can execute DoS attack that sends a large number of corrupted BUs to the HA or CN at once, making the system inaccessible. This protocol does not consider protection against this. IPSec needs to be used to defend against it entirely, but it is difficult to consider the use of IPSec right now in the case of IoT devices with limited computing power.

4.2. Performance Analysis

The Bi-AM protocol is based on the use of the ECC scheme as a public key scheme. The RSA scheme has a key length of 1024 bits or more, whereas the ECC scheme has a key length of about 160 bits. This can greatly reduce the overall length of the Bi-AM message including the public key, thereby reducing the load on the network. Also, once the Bi-AM is executed, it is possible to continue using the exchanged public key. Therefore, even if the MN moves to another network, there is no need to exchange additional Bi-AM messages. It does not overload.

From the aspect of calculation amount, the amount of computation for processing ECC algorithm can be drastically reduced compared to that of RSA. Therefore, if MN is IoT device having limited resources and computing power, the computation amount for processing Bi-AM protocol is not a major problem.

In terms of the number of protocol messages for authentication processing, if IPSec uses IKEv2 as a protocol for negotiation of key and protocol parameters, at least 8 message exchanges must occur during this process. On the other hand, Bi-AM can solve both authentication with only two message exchange. Also, IoT devices with limited computing power may not be able to use IPSec.

V. CONCLUSION

This paper proposes a method to provide security to Mobile IPv6 (MIPv6), a protocol for supporting the mobility of IoT devices. This presents a security protocol for binding update bi-directional authentication, which can be used in limited IoT and MIPv6 environments without using IPSec. It reduces load on the network, reduce the computational cost of each node, since the key-based key pair is used, the size of the exchanged protocol message is also less than the existing protocol. It can exchange a minimum number of messages in an IoT environment with limited computing power.

ACKNOWLEDGMENT

This work was supported by the research grant of Jeju National University in 2017.

REFERENCES

1. Ericsson Mobility Report. 2015 Jun. Available from : https://www.ericsson.com/assets/local/news/2015/6/ericsson-mobility-report-june-2015.pdf
2. Perkins C, Johnson D, and Arkko J. Mobility support in IPv6. (IETF RFC 6275). 2011 Jul. Available from : https://tools.ietf.org/html/rfc6275
3. Mehr K, Niya J. Securing Mobile Ad Hoc Networks Using Enhanced Identity-Based Cryptography. ETRI Journal. 2015 Jun; 37(3): 512-522. Available from : https://onlinelibrary.wiley.com/doi/abs/10.4218/etrij.15.0114.0195
4. Security Architecture for the Internet Protocol (IPSec). (IETF RFC 4301). 2005 Dec. Available from : https://tools.ietf.org/html/rfc4301
5. Internet Key Exchange (IKEv2) Protocol. (IETF RFC 4306). 2005 Dec. Available from : https://tools.ietf.org/html/rfc4306
6. Lee G. Available from : http://www.tta.or.kr/data/reportDown.jsp?news_num=549
7. Lee KJ, Lee SY, Park JS, Kim YJ. Available from : http://kidbs.itfind.or.kr/WZIN/jugidong/1050/105001.htm
8. Chuang M, Lee J, Chen M. SPAM: A secure password authentication mechanism for seamless handover in proxy mobile IPv6 networks. IEEE Systems Journal. 2013: 7(1):102-113. Available from : https://ieeexplore.ieee.org/document/6317128
9. Lee J. Secure authentication with dynamic tunneling in distributed IP mobility management. IEEE Wireless Communications. 2016 Oct; 23(5):38-43. Available from : https://ieeexplore.ieee.org/document/7721740
10. O' shea G, Roe M. Child-proof Authentication for MIPv6 (CAM). ACM Computer Communications Review. 2001 Apr; 31(2). Available from: https://www.microsoft.com/en-us/research/wp-content/uploads/2001/04/ccr2001.pdf

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication