Trusted Mobility Support Protocol in the Mobile IPv6 Networks

Jungjoo Kim[1] and Sugwon Hong[2]
[1]National Internet Development Agency of Korea
[2]Department of Computer Software, Myongji University
San 38-2, Yongin, Gyonggi-do, Korea, swhong@mju.ac.kr

Abstract - ***One of the main features of Mobile IPv6 is the automatic address configuration. A mobile node uses the Neighbor Discovery (ND) protocol to discover its default access router and other nodes, and configures its IPv6 addresses. The ND protocol is vulnerable to various attacks. The Secure Neighbor Discovery (SEND) protocol is proposed currently as a security mechanism for the ND protocol. However, it is not sufficient to address all security issues related to the address autoconfiguration. We propose a protocol which can prove the integrity of the ND messages and verify the authenticity of a mobile node as well as a default access router with less cryptographic computation time than the SEND protocol. We compare the computation times by experiment.***

1. Introduction

With the proliferation of mobile wireless devices, the support for network mobility will be indispensable for providing new network services. The Mobile IPv6(MIPv6) protocol will be a promising technology along with IPv6 to support network mobility in the next generation network[1].

The main purpose of MIPv6 is to provide seamless connection with a correspond node (CN) which communicates with a mobile node while it is away from a home network. The procedure concerning address configuration is carried out based on the stateless or stateful mechanism [2]. The main feature of MIPv6 is to provide the automatic address configuration [3]. The Neighbor Discovery (ND) protocol is designed for the router discovery and address autoconfiguration in MIPv6 [3][4]. If the ND messages are fabricated by attackers during this process, it can bring about detrimental effects on communication [5].

The Secure Neighbor Discovery (SEND) protocol is proposed to secure the ND protocol [6]. However the SEND protocol involves a mobile node in a quite amount of cryptographic computation. Moreover the SEND protocol is not sufficient to address all security issues for address autoconfiguration in MIPv6, especially such as certifying mobile nodes to routers.

In this paper we look into security issues in MIPv6 and the SEND protocol. Then we propose the Trusted Mobility Support Protocol (TMSP) which secures the ND messages and also enables mobile nodes and routers to verify each other, reducing cryptographic computation load on mobile nodes compared to the SEND protocol.

This paper is organized as follows. Section 2 summaries briefly the security issues in MIPv6, and presents main features of the proposed security protocols. Section 3 delves into the protocol and finds out some problems it have. We explain TMSP in section 4 and show the results to evaluate the protocol in section 5. Section 6 follows the conclusion

2. Background

A mobile node (MN) is originally located in a home network with its home address. When a mobile node moves from a home network to a foreign network, it forms its new address in the foreign network, called a care-of address, based on the prefix of the foreign network. MN should receive the network prefix of the network which it is currently attached to for address autoconfiguration.

The Neighbor Discovery (ND) protocol enables MN to discover an access router (AR) and obtain information for address autoconfiguration [3, 4].

When MN moves to other network, it should register its care-of address to a home agent (HA) located in the home network in order to redirect packets to MN's home address to its care-of address. For the care-of address registration and route optimization, the Binding Update (BU) protocol is used [2].

The security issues related in this configuration can be addressed in the following ways. First for the relation between MN and routers (HA or AR), when they receive the ND messages, they should be able to authenticate a sender of the message. It is a matter of whether the sender of the ND message can be trusted or not. Second, they have a way of maintaining the integrity of the messages [5]. For the relation between MN and CN, the BU messages should be protected from intruders [7].

The ND protocol requires the use of IP sec to protect the ND messages [4, 6]. However, the either manual or automatic configuration of security association causes serious problems due to key distribution and performance degradation This approach can be also an impractical approach, considering that the ND mechanism and address configuration are bootstapping procedures [4].

The Secure Network Discovery (SEND) protocol is proposed to counter the security problem of the ND protocol without any configuring security association as required in IPsec [6]. The SEND protocol has new ND protocol options: Cryptographically Address (CGA) signature option, RSA signature option, and Timestamp and Nonce options. The SEND protocol also has the Authorization Delegation Discovery which provides a way of verifying routers to a mobile node using a Trust Anchor.

- CGA signature option

The CGA signature option contains cryptographically generated addresses which are used to make sure that the sender of the ND message is the "owner" of the claimed address. A public-private key pair is generated by all nodes before they can claim their addresses. The option is also used to carry a public key in the ND message.

- RSA signature option

This option uses public key signatures which authenticate the identity of their sender and protect the integrity of the ND messages. The public key is distributed by an authorized node, which is called a Trusted Anchor, or by CGA signature option. When the Trusted Anchor is used, all nodes should have certification paths to the anchor node.

- Timestamp option and Nonce option

The Timestamp option protects the neighbor and router Discovery messages from replay attacks without any previously established states or sequence numbers. The Nonce option is used to protect the solicitation and advertisement messages.

- Authorization Delegation Discovery (ADD)

MN connected to a new link should receive address information from a trusted router. In the Authorization Delegation Discovery, MN must be configured with a Trust Anchor to which a router has a certification path before MN can acknowledge the router as its default AR. Certification Path Solicitation (CPS) and Advertisement (CPA) messages are used to discover a certification path to the Trusted Anchor.

The Trust Anchor can be deployed either globally or locally. The global model assumes a centralized root capable of authorizing routers. In the locally decentralized model, public keys can be issued from various places.

- Return Routability (RR) protocol

For MN to keep communication with CN, MN should notify its care-of address to its HA and CN. This is carried out by the Binding Update(BU) protocol. MN and HA are recommended to have security association for protecting the BU messages. However to establish the security association between MN and CN is impractical. For this reason the Return Routability Procedure is proposed for the protection of the BU messages between two nodes. The security issue for protecting the BU messages is not the subject of this paper.

3. Limitations of the SEND protocol

Since the CGA signature option is based on the public key algorithm, they require cryptographic computation for generating an address using the public key algorithm. In the CGA signature option, MN should carry out cryptographic computation to decrypt the option parameter in the router advertisement (RA) message when it receives the first message from the default router. After MN configures its new address, it continues an exchange of two ND messages with a neighboring node for the Duplicate Address Detection (DAD) which prevents other nodes from using the same address. To process theses messages needs public key-based computation like the RSA algorithm. This procedure is shown in figure 1.

The RSA signature option is based on public key-based signature. The public key can be authorized either through the address ownership configuration by CGA or by using certificates issued by a Trust Anchor. The SEND document does not specify how RSA option is applied to specific cases in detail. Let us consider the complete procedure for the router discovery and address autoconfiguration when the RSA option is involved in the process. At the first stage MN and a default AR exchange Router Solicitation (RS) and Router Advertisement (RA) messages. For the integrity of the messages, the public key signature is applied. At the next step they exchange the CPS and CPA messages for MN to verify that the router is a trusted one which has a certification path to a Trusted Anchor. After this verification, MN exchanges the ND messages with a neighboring node for DAD. The procedure is shown in figure 2.

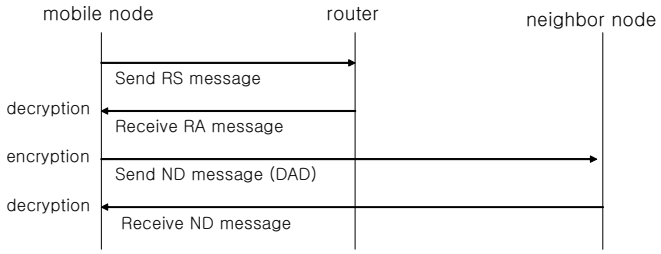

Figure 1: The CGA option procedure for router discovery and address configuration.

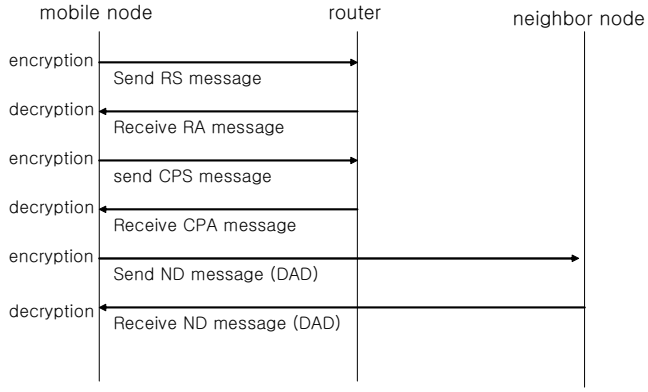

Figure 2: The RSA option procedure for router discovery and address configuration

The CGA signature option can prevent any rogue router from sending false RA messages by verifying the ownership of the address in the message. However the CGA option still lack the way of deciding that a router can be trusted, and proving the integrity of the messages.

The RSA signature option provides the integrity of the ND messages. Moreover, if it is used with the Authorization Delegation Discovery (ADD), a mobile node has a way of deciding whether or not a router can be trusted with the help of a Trusted Anchor. But the problem still lies in that a router is not able to know whether MN can be trusted or not. Even

though it uses the ADD procedure, routers can not verify whether MN is a good or bad node. To deploy the trusted anchor, either globally or locally, is still difficult task.

Another problem of using these options is the amount of computation involved in public key-based algorithms. As shown in figure 1 and 2, these options require a lot of public key-based computation. Considering that most wireless mobile nodes have small power and memory, computation load could be detrimental effect on the node performance and also be some loophole that can be abused by attackers.

4. Trusted Mobility Support Protocol

In this section, we present a protocol for guaranteeing security during the process of the router discovery and address autoconfiguration, which we name Trusted Mobility Support Protocol (TMSP). TMSP enables MN to reduce a load of cryptographic computation. Because MN is configured to have only its own private key, it can avoid the overuse of memory. Unlike the SEND protocol, HA plays a key role in verifying the authenticity of AR and MN, and the integrity of the ND messages.

In order to apply TMSP, HA, AR, and MN should be configured as follows.

1. MN may have more than one home address. The home addresses are connected to a domain-based account (ex, Email address) that is stored in HA's security association database..
2. MN has its own private key.
3. HA has MN's certificate that includes a MN's public key.
4. HA has a public key of the Master Router(MR) that has authority to certify all trusted routers.
5. Each router has a certificate signed by MR.

Figure 3 shows that the complete procedure of TMSP for the router discovery and address autoconfiguration.

At the 1st step MN and AR exchange RS and RA messages as usual. Until verifying AR, MN consider AR as a temporary AR(TR).

At the 2nd step MN sends a message to TR to find out whether or not TR can be trusted. The message has options that include a HA's address, a MN's domain-based identification that can be recognized by HA, and a nonce that is encrypted by MN's private key.

At the 3rd step TR requests a MN's certificate to MN's HA in order to obtain MN's public key. The message includes a certificate option that has a TR's certificate issued by MR.

Since HA is also included in the group which has certification path with MR and has a MR's public key, HA can verify that TR is a trusted one using the TR's certificate. At the 4th step HA sends a MN's public key if TR can be trusted.

At the 5th step TR decrypts the nonce that MN sent at the 2nd step by using MN's public key, and sends it back to MN. If necessary, TR also sends a symmetric key which will be shared with all nodes in the same network and thus can be used for encryption and decryption of other messages. Any information that requires protection should be encrypted by using a MN's public key.

Finally MN compares the nonce in the message with the original value. If two values are same, MN can trust TR, and TR becomes a default AR for MN. MN can use the symmetric key for sending the ND messages or other messages that require the protection from now on.

The messages exchanged in TMSP are shown in figures 4 to 7.

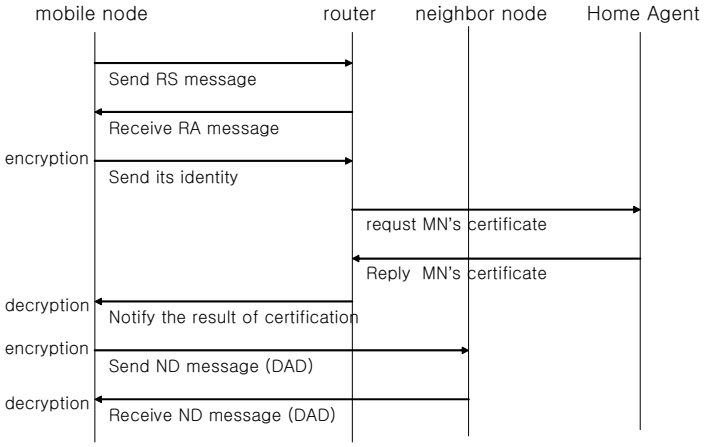

Figure 3: The TMSP procedure for router discovery and address configuration

IP v6 header
  Source=Mobile Node's care-of address (link local address)
  Destination = Temporary Router address
Home agent information option
  Home Agent's address
  Identification of Mobile Node in Home Agent
Nonce option
  Encrypted Nonce with MN's private key

Figure 4: TMSP message format at step 2

IP v6 header
  Source = Temporary router's address
  Destination = Home Agent's address
Certificate address request option
  Identification of Mobile Node in Home Agent
Certificate option
  Temporary Router's certificate signed by Master Router

Figure 5: TMSP message format at step 3

IP v6 header
  Source = Home Agent's address
  Destination = Temporary Router's address
Certificate option
  Mobile node's certificate signed by Home Agent

Figure 6: TMSP message format at step 4

IP v6 header
  Source = Temporary router's address
  Destination = Mobile Node's care-of address
Nonce option
  Decrypted Nonce with Mobile Node's public key
Symmetric key option

Symmetric key

Figure 7: TMSP message format at step 5

In TMSP, MN can verify the authenticity of the sender of the ND messages as in the SEND protocol. At the same time TMSP provides routers with the way of proving that MN is a genuine, not malicious node because HA certifies MN.

As for computation, TMSP carries out only two public key-based computations and two symmetric key-based computations, consequently reducing the amount of cryptographic computation load imposed on MN compared to SEND.

Regarding the deployment of MR, TMSP poses the same problem as a Trusted Anchor in SEND. As a way of deployment model, a hierarchical configuration of multiple MRs can be taken into consideration.

5. Evaluation

We compare cryptographic computation times for the CGA signature option, the RSA signature option, and TMSP. In this experiment, we suppose that the length of a public key and a private key used in the RSA algorithm is 64 bits, and the length of a message is 21.4 Kbytes. We use the Data Encryption Standard(DES) as a symmetric key algorithm which is assumed to have the same key length and the message length as in the RSA algorithm. In this experiment we use a computer with low computing power as wireless mobile devices and have the following results.

Generation time for RSA public key (K_g) : 0.211 sec
Encryption time by RSA algorithm (E_R) : 1.201 sec
Decryption time by RSA algorithm (D_R): 5.09 sec
Encryption time by DES algorithm (E_D) : 0.36 sec
Decryption time by DES algorithm (D_D) : 0.36 sec

Using the CGA signature option, MN can verify the ownership of the address in the ND messages, but not the integrity of the messages. In figure 1 when MN uses the CGA signature option, MN generates a CGA address at sending the RA message and decrypts CGA addresses at receiving two messages from a router and a neighboring node. Thus the computation time T_C (= $K_g + 2D_R$) is 10.391sec.

On the other hand, the RSA signature option enables MN not only to certify the ownership of a claimed address but also to prove the integrity of the messages. With the ADD protocol, the RSA option can authenticate AR. However, naturally this option requires more cryptographic computation than the CGA option. As in figure 2, MN should be involved in the RSA public key-based signature whenever it sends or receives the messages for protecting their integrity. Before MN gets an AR's public key from a Trusted Anchor, MN and AR may use the CGA option to deliver their public keys. Even though we exclude the generation time of CGA addresses, MN is required to do 3 encryptions and 3 decryptions. Thus the computation time T_R (= $3E_R + 3D_R$) is 18.873sec.

The complete procedure for TMSP is shown in figure 3. In this protocol, MN is involved in 1 encryption and 1 decryption using the RSA public key-based computation until it obtains a symmetric key from AR. Since then, MN uses the symmetric key for DAD procedure. Thus the computation time T_T (= $E_R + D_R + E_D + D_D$) is 7.011sec. Even though it requires less computation time, TMSP provides a way of verifying the authenticity of MN as well as AR.

6. Conclusion

In this paper, we explain the security issues for the router discovery and address autoconfiguration which is a main feature of MIPv6, and the SEND protocol which is currently proposed as a security mechanism for this process. Then we propose a protocol which can guarantee secure address configuration. The strength of this protocol is that it can prove the integrity of the ND messages and at the same time verify the authenticity of AR and MN as well. And the whole procedure of the protocol can be done with less cryptographic computation load on MN than the SEND protocol.

Acknowledgments

This work was supported by the ERC program of MOST/KOSEF (Next-generation Power Technology Center) and the development program of Intelligent Distribution Management System of Ministry of Commerce, Industry and Energy.

References

1. H. Soliman, Mobile IPv6: Mobility in a Wireless Internet, Addison-Wesley, 2004.
2. D. Johnson, C. Perkins, and J. Arkko, " Mobility Support in IPv6," RFC 3775, June 2004
3. S. Thomson and T. Narten, " IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998.
4. T. Narten, B. Nordmark, and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998
5. P. Nikander, ED, J Kempf, and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", RFC3756, May 2004.
6. J. Arkko, ED, J. Kempf, B. Zill and P. Nikander "SEcure Neighbor Discovery (SEND)" , RFC3971, March 2005.
7. Y. Qiu, J. Zhou, and R. Deng, "Security Analysis and Improvement of Return Routability Protocol," International Workshop on Secure Mobile Ad-hoc Networks and Sensnors, September 2005]