LETTER *Special Section on New Technologies and their Applications of the Internet*

An Enhanced Security Protocol for Fast Mobile IPv6

Ilsun YOU[†a)], **Kouichi SAKURAI**[††], ***and*** **Yoshiaki HORI**[††], ***Members***

SUMMARY Recently, Kempf and Koodli have proposed a security protocol for Fast Mobile IPv6 (FMIPv6). Through the SEcure Neighbor Discovery (SEND) protocol, it achieves secure distribution of a handover key, and consequently becomes a security standard for FMIPv6. However, it is still vulnerable to redirection attacks. In addition, due to the SEND protocol, it suffers from denial of service attacks and expensive computational cost. In this paper, we present a security protocol, which enhances Kempf-Koodli's one with the help of the AAA infrastructure.

key words: *FMIPv6 security, MIPv6, secure neighbor discovery, cryptographically generated address, BAN-logic*

1. Introduction

Fast Mobile IPv6 (FMIPv6) becomes vulnerable to various attacks if it is not secured [1]. For example, an attacker can redirect a victim mobile node's traffic at will by using a forged $FastBindingUpdate(FBU)$ message. In order to protect FMIPv6, several security protocols have been provided [2]–[5]. Recently, Kempf-Koodli's protocol has been adopted as a security standard for FMIPv6 (RFC 5269) [2]. It provides the public key based strong security by adopting the SEcure Neighbor Discovery (SEND) protocol [6], which is based on the Cryptographically Generated Address (CGA) method [7]. With the help of the CGA method, a mobile node can tightly bind its care-of address to its handover key. Also, because it is FMIPv6-seamless unlike the protocols proposed in [3] and [4], it does not result in the additional messages and round trip times. Despite such advantages, it suffers from expensive computational cost and Denial of Service (DoS) attacks because it depends on the SEND protocol. More importantly, it is still vulnerable to redirection attacks since it does not protect the $UnsolicitedNeighborAdvertisement(UNA)$ message like other protocols. In this paper, we propose an FMIPv6 security protocol, which improves Kempf-Koodli's one while keeping its advantages.

Manuscript received January 26, 2009.

Manuscript revised May 24, 2009.

[†]The author is with School of Information Science, Korean Bible University, South Korea.

[††]The authors are with the Dept. of Computer Science and Communication Engineering, Kyushu University, Fukuoka-shi, 819–0395 Japan.

a) E-mail: isyou@bible.ac.kr

DOI: 10.1587/transinf.E92.D.1979

2. Proposed FMIPV6 Authentication Protocol

2.1 Notations and Preliminary

- $Msg(address1, address2)$ means that the message Msg is sent from $address1$ to $address2$.
- $E(K, M)$ denotes a function that encrypts the message M with the given key K, where K can be a secret key or a public key.
- $SIGN(K, M)$ denotes a function that digitally signs the message M with the private key K.
- MN denotes a mobile node.
- $AR(i)$ denotes the ith access router which the MN visits, and its IPv6 address, where $i > 0$.
- $CoA(i)$ is the ith care-of address of the MN, where $i > 0$.
- PU_X is the X's public key from which the CGA is derived.
- PR_X is the X's private key which corresponds to PU_X.
- $HK(i)$ is the ith handover key, where $i > 0$.
- $K(i)$ is the ith message protection secret, where $i > 0$.
- $CGA - PARAM_X$ is the X's parameters which are used to verify that the X's CGA is derived from PU_X.

It is assumed that the MN has a public/private key pair PU_{MN}/PR_{MN} and its address is a CGA, which derived from PU_{MN}. And it is supposed that during the bootstrapping step, the MN shares the message protection secret $K(1)$ with the first access router $AR(1)$ through the Authentication, Authorization, and Accounting (AAA) infrastructure [3], [8]. This assumption is reasonable because the AAA infrastructure is widely used for the network access authentication in Mobile Internet environment. Moreover, we assume that there is a secure channel between access routers.

2.2 Operation

As illustrated in Fig. 1, this protocol is composed of three phases: handover key negotiation, fast binding update and new network attachment phases.

During the handover key negotiation phase, the MN negotiates a new handover key $HK(i)$ with the current access router $AR(i)$ through its public key PU_{MN}. Especially, in order to protect the $RtSolPr$ and $PrRtAdv$ messages, the MN and the $AR(i)$ adopt the HMAC method instead of the public key based digital signature. That makes it possible

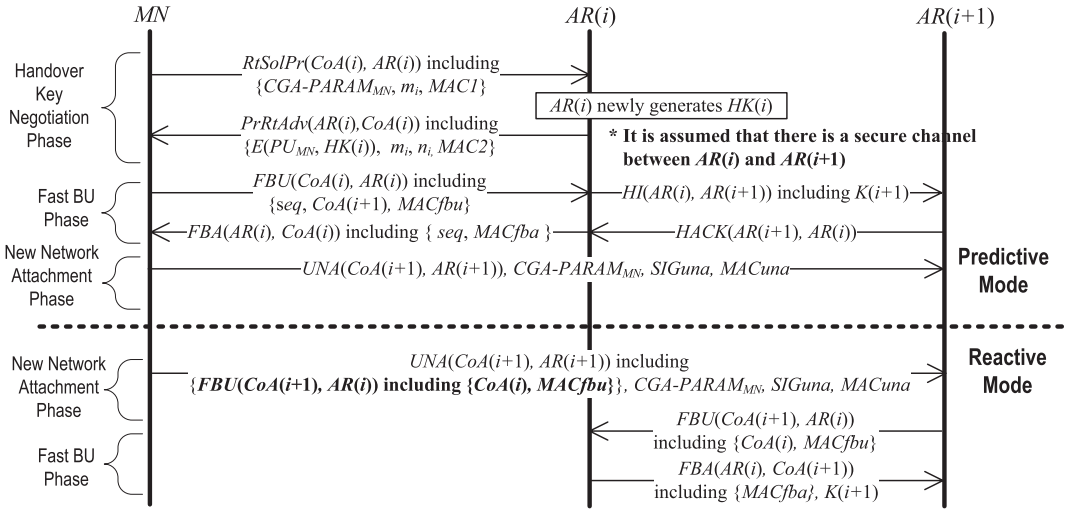

Fig. 1 Proposed protocol.

for them to defend against the DoS attack while reducing the heavy computation overhead caused by the asymmetric cryptographic operations. For the HMAC method, a message protection secret $K(i)$, derived from its related handover key and nonces, is introduced. Note that during the bootstrapping step, the first message protection secret $K(1)$ is shared between the MN and the $AR(1)$ with the help of the AAA infrastructure as mentioned above. Once the shared handover key $HK(i)$ has been constructed, the MN starts the fast binding update phase by sending the FBU message to the $AR(i)$ when a link-specific handover event occurs. If the FBU message is valid, the $AR(i)$ can believe that the MN truly owns both $CoA(i)$ and PU_{MN} because it can get $HK(i)$ in the only case that PR_{MN} belongs to itself. With such belief, the $AR(i)$ starts to act as a temporary home agent for the MN while exchanging the HI and $HACK$ messages with the next access router $AR(i+1)$. Note that the HI message includes the $(i+1)$th message protection secret $K(i+1)$. Thus, the $AR(i)$ allows the $AR(i+1)$ to securely share $K(i+1)$ with the MN. After that, the $AR(i)$ returns the MN the FBA message while stating to tunnels the traffic sent to $CoA(i)$ on its link to $CoA(i+1)$ on the $AR(i+1)$'s link. If the FBA message is valid, the MN assumes that data packets are being forwarded to its new location. As soon as the MN handovers to the $AR(i+1)$'s link, it announces its attachment by sending the UNA message to the $AR(i+1)$. This is the new network attachment phase. In order to secure the UNA message, the proposed protocol uses both the digital signature, $SIGuna$, and the HMAC value, $MACfna$. Especially, the digital signature is adopted to provide the handover key independence. When the MN cannot send the FBU message or receive the FBA message on the $AR(i)$'s link (the reactive mode), the $AR(i+1)$ performs the fast binding update phase on behalf of the MN before verifying the UNA message.

3. Analysis

In this section, the proposed protocol is formally analyzed through BAN-logic [9]. After that, the protocol's security properties and computation overhead are discussed.

3.1 Formal Verification by BAN-Logic

Since introduced by Burrows, Abadi and Needham in 1989, BAN-logic has become the best-known and widely used method for verifying security protocols due to simplicity and robustness. For details on notations and logical postulates of BAN-logic, refer to [9]. As the first step of this verification, we define the goals as follows:

$$\text{Goal1} : AR(i) \models FBU$$

$$\text{Goal2} : AR(i+1) \models UNA$$

$$\text{Goal3} : MN \models MN \overset{K(i+1)}{\rightleftharpoons} AR(i+1)$$

For the next handover, the validity of $K(i+1)$ should be believed by both the MN and the $AR(i+1)$. Because the $AR(i)$, who controls $K(i+1)$, sends the secret to the $AR(i+1)$ through their secure channel, we can assume that the $AR(i+1)$ believes that the secret is valid and fresh. Thus, we provide the assumptions A4 and A6 in addition to Goal3.

Also, we use the following definition besides the basic rules of BAN-logic. It is clear from the meaning of the definition that it is intuitively true.

$$\text{Definition1} : \frac{A \models \overset{PR_A}{\mapsto} A,\ A \models B \models \{M\}_{PU_A}}{A \models B \models M}$$

The idealized form of the proposed protocol is shown in Fig. 2. For the converting, we express the $HMAC(K, M)$ operation as $< M >_K$. In the $PrRtAdv$ message, besides $HK(i)$, $K(i+1)$ is added in the encrypted part because that secret can be derived from the handover key. Also, the assumptions are defined as shown in Fig. 3. Strictly speaking, in the BAN logic, we cannot prove that the public key, PU_{MN} belongs to the MN though it can be verified by the CGA method. Thus, we present A9 and A10 instead.

(1) $MN \rightarrow AR(i)$: $< m_i >_{K(i)}$
(2) $AR(i) \rightarrow MN$: $<\{MN \overset{HK(i)}{\rightleftharpoons} AR(i), MN \overset{K(i+1)}{\rightleftharpoons} AR(i+1)\}_{PU_{MN}}, m_i, n_i >_{K(i)}$
(3) $MN \rightarrow AR(i)$: $< FBU, seq, MN \overset{HK(i)}{\rightleftharpoons} AR(i) >_{HK(i)}$
(4) $AR(i) \rightarrow MN$: $< FBA, seq, MN \overset{HK(i)}{\rightleftharpoons} AR(i) >_{HK(i)}$
(5) $MN \rightarrow AR(i+1)$: $\{H(UNA)\}_{PR_{MN}}, < UNA, MN \overset{K(i+1)}{\rightleftharpoons} AR(i+1) >_{K(i+1)}$

Fig. 2 Idealized protocol.

A1: $MN \equiv AR(i) \Rightarrow MN \overset{HK(i)}{\rightleftharpoons} AR(i)$
A2: $MN \equiv AR(i) \Rightarrow MN \overset{K(i+1)}{\rightleftharpoons} AR(i+1)$
A3: $AR(i) \equiv MN \overset{HK(i)}{\rightleftharpoons} AR(i)$
A4: $AR(i+1) \equiv MN \overset{K(i+1)}{\rightleftharpoons} AR(i+1)$
A5: $AR(i) \equiv \#(MN \overset{HK(i)}{\rightleftharpoons} AR(i))$
A6: $AR(i+1) \equiv \#(MN \overset{K(i+1)}{\rightleftharpoons} AR(i+1))$
A7: $MN \equiv MN \overset{K(i)}{\rightleftharpoons} AR(i)$
A8: $AR(i) \equiv MN \overset{K(i)}{\rightleftharpoons} AR(i)$
A9: $AR(i) \equiv \overset{PU_{MN}}{\mapsto} MN$
A10: $AR(i+1) \equiv \overset{PU_{MN}}{\mapsto} MN$
A11: $MN \equiv \overset{PR_{MN}}{\mapsto} MN$
A12: $MN \equiv \overset{PU_{MN}}{\mapsto} MN$
A13: $MN \equiv \#(m_i)$
A14: $AR(i) \equiv \#(n_i)$
A15: $MN \equiv \#(seq)$
A16: $AR(i) \equiv MN \Rightarrow FBU$
A17: $AR(i+1) \equiv MN \Rightarrow UNA$

Fig. 3 Assumptions.

Once the assumptions are made, we can now proceed with the analysis (where R1 denotes the message-meaning rule, R2 denotes the nonce verification rule and R3 denotes the jurisdiction rule).

From the *RtSolPr* message, we derive by:

(1) $AR(i) \models MN \mid\sim m_i$ [by A8, R1]

From the *PrRtAdv* message, we derive:

(2) $MN \models AR(i) \mid\sim \{MN \overset{HK(i)}{\rightleftharpoons} AR(i),\ MN \overset{K(i+1)}{\rightleftharpoons} AR(i+1)\}_{PU_{MN}}, m_i, n_i$ [by A7, R1]

(3) $MN \models \#(\{MN \overset{HK(i)}{\rightleftharpoons} AR(i),\ MN \overset{K(i+1)}{\rightleftharpoons} AR(i+1)\}_{PU_{MN}}, m_i, n_i)$ [by A5]

(4) $MN \models AR(i) \models \{MN \overset{HK(i)}{\rightleftharpoons} AR(i),\ MN \overset{K(i+1)}{\rightleftharpoons} AR(i+1)\}_{PU_{MN}}$ [by (2), (3), R2]

(5) $MN \models MN \overset{HK(i)}{\rightleftharpoons} AR(i)$ [by A11, (4), Definition1, A1, R3]

(6) $MN \models MN \overset{K(i+1)}{\rightleftharpoons} AR(i+1)$ [by A11, (4), Definition1, A1, R3]

From the *FBU* message, we derive:

(7) $AR(i) \models MN \models FBU$ [by (5), R1, A5, R2]

(8) $AR(i) \models FBU$ [by (7), A16, R3]

From the *FBA* message, we derive:

(9) $MN \models AR(i) \models FBA$ [by (5), R1, A15, R2]

From the *UNA* message, we derive:

(10) $AR(i+1) \models MN \models UNA$ [by A4, R1, A6, R2]

(11) $AR(i+1) \models UNA$ [by (9), A17, R3]

Note that only the right part of the *UNA* message can leads to the formula (11). However, the left part of the message is required to prove the handover key independence. By the formulas (6), (8), (11), we can conclude that the proposed protocol achieve the given goals.

3.2 Security Analysis

(1) Tight binding between $HK(i)$ and $CoA(i)$: In the proposed protocol, the $AR(i)$ encrypts $HK(i)$ with the MN's public key PU_{MN}, which corresponds to $CoA(i)$. If the FBU message, protected by $HK(i)$, is valid, the $AR(i)$ can be sure that the MN truly owns PR_{MN} and $CoA(i)$. Thus, there exists the tight binding between $HK(i)$ and $CoA(i)$.

(2) Handover key independence: In the proposed protocol, each handover key is not used for generating or distributing other handover keys. Therefore, even if one handover key is compromised, the previous or successive handover keys are not compromised.

(3) Preventing Denial of Service attacks: The proposed protocol adopts the HMAC method to protect the $RtSolPr$, $PrRtAdv$, FBU, FBA and UNA messages. Especially, each involved entity validates the related HMAC value such as $MAC1$, $MAC2$ or $MACuna$ before performing its public key operation. In this way, it can defend against the DoS attacks.

(4) Secure UNA messages: In the proposed protocol, each UNA message is protected by both the public key based digital signature and HMAC methods. Because of not knowing $K(i+1)$ and PR_{MN}, an attacker cannot fabricate UNA messages and launch session hijacking attacks by just eavesdropping. Note that though the message can be protected by only the HMAC method, the digital signature method is used to protect the proposed protocol even though handover keys are compromised. Like our approach, Kempf-Koodli's protocol can use the digital signature based on the CGA method to protect the UNA messages. However, in this case, its computational costs can be considerabley increased due to the expensive assymetric operations.

3.3 Computational Cost Comparison

Table 1 compares the computational cost of the proposed protocol with that of Kempf-Koodli's one. As described in it, while the MN reduces (V+H) at the expense of 3 HM, the $AR(i)$ and $AR(i+1)$ reduce S at the expense of 3(H+HM). In addition to such an advantage, the proposed protocol exploits the existing messages of the FMIPv6 protocol to present an FMIPv6-seamless structure. Therefore, it does not introduce new signaling messages and additional round trip times.

4. Conclusion

A new security protocol for FMIPv6 was proposed. The proposed protocol uses the message protection secret to solve the drawbacks of Kempf-Koodli's one. Through the HMAC

Table 1 Computational cost comparison (S: the cost for the one signature generation, V: the cost for verifying the one signature, H: the cost for one hash operation, HM: the cost for one HMAC operation, E: the cost for one public key encryption, D: the cost for one public key decryption, $MN*$ and $AR*$: the nodes of Kempf-Koodli's protocol, MN and AR: the nodes of the proposed protocol).

Message	$MN*$	$AR*$	MN	AR
$RtSolPr$	S	2H+V	HM	HM+2H
$PrRtAdv$	2H+V+D	E+S	HM+D	E+HM
FBU	HM	HM	HM	HM
FBA	HM	HM	HM	HM
UNA	0	0	S+H+HM	3H+HM+V
*Values	86,035 K	46,061 K	84,009 K	4,070 K

* The parameters provided in [10] are applied to compute the values. It is assumed that the size of the message is 100 byte message and the used algorithms are $SHA1$, $HMAC-SHA1$ and RSA. The values are measured in cycles.

values computed with this secret, it can prevent the DoS attacks while minimizing the public key operations. Note that the first message protection secret is negotiated between the MN and its first AR with the help of the AAA infrastructure. By using BAN-logic, the proposed protocol's correctness is formally verified. From security analysis and computational cost comparison, we can conclude that the protocol is more secure and efficient than Kempf-Koodli's one.

Acknowledgments

This paper is supported by JSPS RONPAKU Program (ID No.KOSEF-10910).

References

[1] R. Koodli, "Mobile IPv6 fast handovers," IETF RFC 5268, June 2008.
[2] J. Kempf and R. Koodli, "Distributing a symmetric fast mobile IPv6 (FMIPv6) handover key using secure neighbor discovery (SEND)," IETF RFC 5269, June 2008.
[3] V. Narayanan, N. Venkitaraman, H. Tschofenig, G. Giaretta, and J. Bournelle, "Establishing handover keys using shared keys," IETF draft-vidya-mipshop-handover-keys-aaa-04, March 2007.
[4] W. Haddad and S. Krishnan, "Authenticating FMIPv6 handovers," IETF draft-haddad-mipshop-fmipv6-auth-02, Sept. 2006.
[5] J. Choi and S. Jung, "A secure and efficient handover authentication based on light-weight diffie-hellman on mobile node in FMIPv6," IEICE Trans. Commun., vol.E91-B, no.2, pp.605–608, Feb. 2008.
[6] J. Arkko, J. Kempf, B. Zill, and P. Nikander, "Secure neighbor discovery (SEND)," IETF RFC 3971, March 2005.
[7] T. Aura, "Cryptographically generated addresses (CGA)," IETF RFC 3972, March 2005.
[8] C. Perkins and P. Calhoun, "Authentication, authorization, and accounting (AAA) registration keys for mobile IPv4," IETF RFC 3957, March 2005.
[9] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," ACM Trans. Comput. Syst., vol.8, no.1, pp.18–36, 1990.
[10] B. Preneel, et al., "Performance of optimized implementations of the NESSIE primitives," Technical Report, NES/DOC/TEC/WP6/D21/2, Feb. 2003.