Comments on Kang-Park's Security Scheme for Fast Handover in Hierarchical Mobile IPv6

Ilsun YOU
School of Information Science
Korean Bible University
Seoul, Republic of Korea
Email: isyou@bible.ac.kr

Kouichi SAKURAI and Yoshiaki HORI
Department of Computer Science and Communication Engineering
Kyushu University
Fukuoka, Japan
Email: {sakurai,hori}@csce.kyushu-u.ac.jp

***Abstract*—While gracefully combining FMIPv6 and HMIPv6 together, F-HMIPv6 enables the best performance in terms of handover latency and signaling overhead. Recently, to protect F-HMIPv6, Kang and Park proposed a security scheme. This scheme successfully achieves seamless integration with F-HMIPv6 while providing the session key exchange as well as the mobile node authentication. In this paper, Kang-Park's scheme is formally verified based on BAN-logic, and then its weaknesses and related attacks are discussed.**

***Keywords*-MIPv6, F-HMIPv6, Security, BAN-logic**

I. Introduction

Mobile IPv6 Fast Handovers (FMIPv6) [1] and Hierarchical Mobile IPv6 (HMIPv6)[2] were proposed to improve Mobile IPv6 (MIPv6) [3]. Then, to take all their advantages, Fast Handover for Hierarchical MIPv6 (F-HMIPv6) was developed [4], [5]. While gracefully combining FMIPv6 and HMIPv6 together, the protocol succeeded in providing the best performance in terms of handover latency and signaling overhead [6]. In 2007, Kang and Park proposed a securiy scheme to protect F-HMIPv6 [7]. In this scheme, a Mobility Anchor Point (MAP) leverages the Authentication, Authorization, and Accounting (AAA) infrastructure [8] to authenticate a Mobile Node (MN) while exchanging a session key with it. Also, the MAP uses the group key and the ticket to distribute the session key to its Access Routers (ARs). More importantly, the scheme achieves seamless harmony with F-HMIPv6. However, we find that this scheme suffers from the Denial of Service (DoS), malicious mobile node flooding and replay attacks while largely depending on the group key. In this paper, we use BAN-logic [9] to formally and precisely analyze Kang-Park's scheme. Then, the found weaknesses and the related attacks are discussed.

II. Review of Kang-Park's Security Scheme

A. Notations and Preliminary

Fig. 1 shows the notations used in this paper.

In this scheme, a MAP and its ARs share a group key GK. Also, there is a secure channel between each AR and its MAP. Every MN belongs to an Authentication Server AS and can be authenticated by the server through the AAA infrastructure. In addition, it is assumed that all involved nodes are time-synchronized.

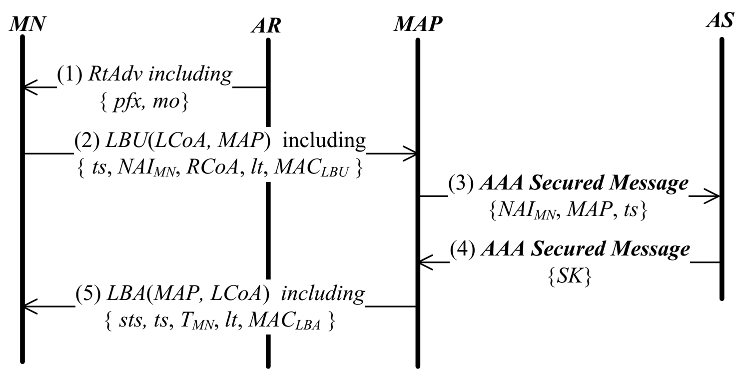
Msg(*A*, *B*)	the message *Msg* sent from *A* to *B*, where *A* and *B* are an IPv6 address
E(*K*, *M*)	a function that encrypts the message *M* with the given key *K*, where *K* can be a secret key or a public key
MN and *AS*	a Mobile Node and an Authentication Server respectively
AR	an Access Router and its IPv6 address (*pAR*: previous *AR*, *nAR*: new *AR*)
MAP	a Mobility Anchor Point and its IPv6 address
CoA	Care-of Address (*LCoA*: Local *CoA*, *RCoA*: Regional *CoA*)
NAI_X	the *X*'s Network Access Identifier
GK	the group key of the *MAP* and its *AR*s
HMAC(*K*, *M*)	an HMAC Value computed using the secret *K* over the message *M*
|	concatenation operation

Figure 1. Notations

B. Operation

This protocol can be divided into two phases: MAP registration phase and handover phase. The MAP registration phase, shown in Fig. 2, is executed whenever an MN enters a new MAP domain.

Once the MN moves to a new MAP domain, it receives the *RtAdv message* from the current AR. Based on the pfx and mo options included in the message, the MN configures both the *Local Care-of Address (LCoA)* and the *Regional Care-of Address (RCoA)* while computing a session key SK. This session key will be used to protect protocol messages in both the MAP registration and handover phases. Then, the MN performs the local binding update by exchanging the local binding update (*LBU*) and local binding acknowledgement (*LBA*) messages with the MAP. The two messages are protected by MAC_{LBU} and MAC_{LBA} respectively. Note that the MAP securely receives SK from the MN's authentication server AS depending on the AAA infrastructure. Additionally, it issues the MN a ticket T_{MN} encrypted with GK to securely distribute SK to its ARs in the handover phase. As a result of this phase, the MAP believes the binding between the MN's the *RCoA* and the *LCoA* while sharing SK with the MN.



- *pfx*: the prefix information of *AR*
- *mo*: the MAP option
- *ts*: the current time stamp
- *sts*: the result of the local binding update
- *lt*: the lifetime of the local binding
- *Kma*: the key shared by *MN* and *AS*
- $SK = H(Kma|NAI_{MN}|MAP|ts)$
- $T_{MN} = E(GK, SK|RCoA|exp)$
- *exp*: the expiration time of T_{MN}
- $MAC_{LBU} = HMAC(SK, LBU)$
- $MAC_{LBA} = HMAC(SK, LBA)$

Figure 2. MAP Registration phase

Fig. 3 depicts the handover phase, which is performed when the MN moves within its current MAP domain. In this phase, all messages are protected with the HMAC values computed using SK or GK.

If the MN knows its movement by using link layer (L2) triggers, it sends the pAR the *Router Solicitation for Proxy Advertisement (RtSolPr)* message protected by the authenticator $M1$. On receiving the message, the pAR decrypts and verifies the included T_{MN} with the group key GK. At this point, the pAR becomes aware of the session key SK. By using this key, the pAR verifies the message's authenticator $M1$, and then returns the *Proxy Routter Advertisement (PrRtAdv)* message. If the message is valid, the MN configures its new local care-of address *nLCoA* using the nAR's information contained in the message. After the *nLCoA* configuration, it transmits the *Fast Binding Update (FBU)* message to the MAP. In case that the included $M3$ is correct, the MAP trusts the MN's new binding information indicated by the *FBU* message, thus updating its local care-of address to $nLCoA$. Based on such a trust, the MAP exchanges the *Handover Initiate(HI)* and *Handover Acknowledge(HACK)* messages with the new access router nAR. After then, it responds to the *FBU* message with the *Fast Binding Acknowledge(FBA)* one while starting to tunnel the traffic sent to the MN's $RCoA$ to the nAR. As soon as the MN arrives at the new network, it informs the nAR of its attachment by sending the *Fast Neigbhor Advertisement (FNA)* message. At this point, the nAR uses GK to recover SK from T_{MN}, then verifying this message. The valid *FNA* message makes the nAR start to deliver the buffered packets to the MN's $nLCoA$.

III. Formal Analysis

In this section, Kang-Park's scheme is formally analyzed. For this goal, we use BAN-logic, which is one of the most popular formal methods to analyze security protocols [9]. In BAN-logic, the following steps are typically taken to verify a protocol: (i) transforming the original protocol into an idealized one, (ii) making assumptions on the initial state and (iii) iteratively applying BAN-logic rules until finding the meaningful results.

Note that BAN-logic privides no notation and rule for the HMAC operation. Thus, we use $< M >_K$ to express $HMAC(K, M)$. Also, for more precise verification, we define an extended rule E1 as follows:

$$\text{E1:}\quad \frac{MAP \models MN \models A,\ MAP \models AR \models A}{MAP \models MN@A}$$

* *A* is an IPv6 address
MN@A means *MN* exists at *A*

This rule helps to verify if the MN truely exists at its new *LCoA*. In addition, the message-meaning, nonce-verification and jurisdiction rules are denoted as R1, R2 and R3 respecively. For details on BAN-logic, refer to [9].

A. MAP registration phase

In order to verify the MAP registration phase, we first transform it into the following idealized version:

(1-1) $MN \rightarrow MAP : <LBU>_{SK}$
(1-2) $MAP \rightarrow MN : <LBA>_{SK}$

* *LBU* includes *ts*, *LCoA* and *RCoA*
LBA includes *ts* and T_{MN}
$T_{MN}=\{SK, \#(SK), RCoA, exp\}_{GK}$

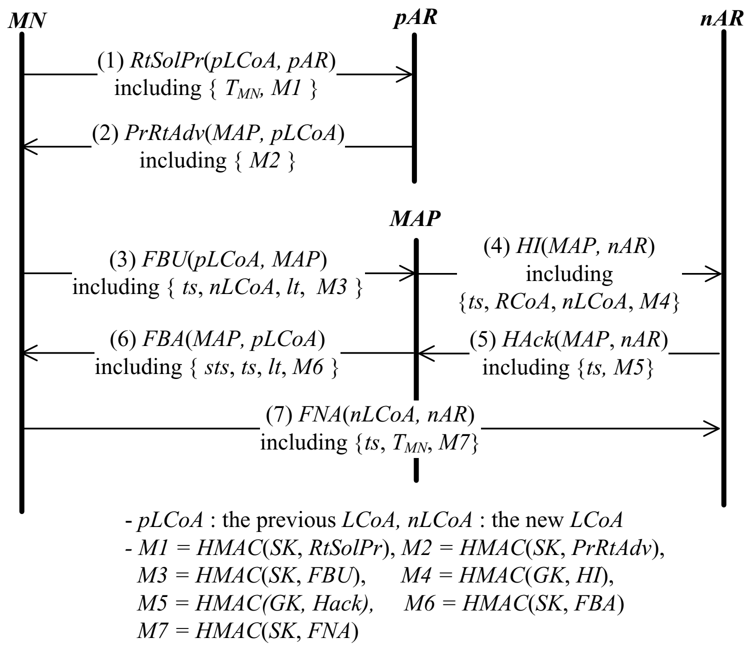


Figure 3. Handover phase

Also, the assumptions are defined as follows:

A11: $MAP \models MAP \overset{SK}{\rightleftharpoons} MN$
A12: $MAP \models \#(ts)$
A13: $MN \models MAP \overset{SK}{\rightleftharpoons} MN$
A14: $MN \models \#(ts)$
A15: $MN \models MAP \Rightarrow T_{MN}$
H0: $MN \models RtAdv$
H1: $MAP \models AR \models LCoA$

Because of being secured based on the AAA infrastructure, the communication between the MAP and the AS is omitted in the ideadlized version. Instead, A11 is added to the assumptions to keep the same logic. Now, we can proceed to analyze this phase as follows:

From (1-1), we derive:
(1) $MAP \models MN \models LBU$ [by A11, R1, A12, R2]
(2) $MAP \models MN \models LCoA$ [by (1)]
(3) $MAP \models MN @ LCoA$ [by (2), H1, E1]
From (1-2), we derive:
(4) $MN \models MAP \models LBA$ [by A13, R1, A14, R2]
(5) $MN \models T_{MN}$ [by (4), A15, R3]

Before (1-1), the MN has no belief to advance this analysis as it just sees the *RtAdv* message. Thus, at this point, we can decide that Kang-Park's scheme is not correct. But, to discover other security weaknesses, we assume that the MN believes the *RtAdv* message (i.e., H0 is added). Similarly, we add H1 to allow the MAP to have enough belief that the MN is present at *LCoA* (i.e., (3)). As a result, we can see that without H0 and H1, this phase is incorrect. That is, H0 and H1 indicate the security flaws of this phase.

B. Handover phase

As the idealized version of this handover phase, we present:

(2-1) $MN \rightarrow pAR$: <RtSolPr>$_{SK}$
(2-2) $pAR \rightarrow MN$: <PrRtAdv>$_{SK}$
(2-3) $MN \rightarrow MAP$: <FBU>$_{SK}$
(2-4) $MAP \rightarrow nAR$: <HI>$_{GK}$
(2-5) $nAR \rightarrow MAP$: <HAck>$_{GK}$
(2-6) $MAP \rightarrow MN$: <FBA>$_{SK}$
(2-7) $MN \rightarrow nAR$: <FNA>$_{SK}$
* *ts* is included in *FBU, HI, Hack, FBA* and *FNA*.
T_{MN} is included in *RtSolPr* and *FNA*.
nLCoA is included in *FBU* and *FNA*.
HI includes ($MN \models nLCoA$) <u>instead of *nLCoA*</u>.

To start this analysis, we make the following assumptions:

A21: $AR \models \#(exp)$ only in T_{MN}
A22: $MAP \models \#(ts)$
A23: $nAR \models \#(ts)$
A24: $MN \models \#(ts)$
H2: $AR \models MAP \overset{GK}{\longleftrightarrow} AR$
H3: $AR \models MAP \Rightarrow MN \overset{SK}{\rightleftharpoons} AR$
H4: $pAR \models \#(RtSolPr)$
H5: $MN \models MN \overset{SK}{\rightleftharpoons} AR$
H6: $MN \models \#(PrRtAdv)$
H7: $MAP \models MAP \overset{SK}{\rightleftharpoons} MN$
H8: $MAP \models MAP \overset{GK}{\longleftrightarrow} AR$
H9: $MN \models MAP \overset{SK}{\rightleftharpoons} MN$

Note that the AR believes that exp is fresh just in the MN's ticket T_{MN}. Also, we assume that based on H2 and H8, GK can be used as a shared secret in addition to as an encryption key.

With the above idealized version and assumptions, we can proceed to analyze this phase as follows:

From (2-1), we derive:
(1) $pAR \models MAP \models TBody$ [by H2, R1, A21, R2]
(2) $pAR \models MN \overset{SK}{\rightleftharpoons} pAR$ [by (1), H3, R3]
(3) $pAR \models MN \models RtSolPr$ [by (2), R1, H4, R2]
From (2-2), we derive:
(4) $MN \models pAR \models PrRtAdv$ [by H5, R1, H6, R2]
From (2-3), we derive:
(5) $MAP \models MN \models FBU$ [by H7, R1, A22, R2]
(6) $MAP \models MN \models nLCoA$ [by (5)]
From (2-4), we derive:
(7) $nAR \models MAP \models HI$ [by H2, R1, A23, R2]
(8) $nAR \models MAP \models MN \models nLCoA$ [by (7)]
From (2-5), we derive:
(9) $MAP \models nAR \models HAck$ [by H8, R1, A22, R2]
From (2-6), we derive:
(10) $MN \models MAP \models FBA$ [by H9, R1, A24, R2]
From (2-7), we derive:
(11) $nAR \models MN \overset{SK}{\rightleftharpoons} nAR$ [by H2, R1, A21, R2, H3, R3]
(12) $nAR \models MN \models FNA$ [by (11), R1, A23, R2]
(13) $nAR \models MN \models nLCoA$ [by (12)]
* $Tbody = MN \overset{SK}{\rightleftharpoons} pAR, \#(MN \overset{SK}{\rightleftharpoons} pAR), RCoA, exp$
AR is pAR or nAR

The additional suppositions H2-H9 are given due to the same reason as the previous subsection. That is, they mean the security flaws of this phase. Especially, while GK is shared among the MAP and its ARs, SK is shared among the MN, the MAP and its ARs (i.e., more than two entities share a key). That makes this phase not be able to provide true authentication and confidentiality. Also, because the *RtSolPr* and *PrRtAdv* messages lack freshness, we give (H4) and (H6) to derive the beliefs (3) and (4). It is worth noting that based on (8) and (13), the nAR can detect the MN's attachment to its network. Unlike the nAR, the MAP just trusts that the MN believes its *nLCoA* (i.e., (6)). With this belief, it cannot ensure that the MN arrives at *nLCoA*. As a result, we can conclude that this phase is incorrect.

IV. Discussion

A. Dependency on the Group Key

Kang-Park's scheme depends on the group key method to securely distribute SK in addition to protecting the *HI* and *HAck* messages. However, such an approach causes this scheme to rely upon H2 and H8. Without them, every AR, which shares GK, can see and even forge all messages exchanged between its MAP and other router. Moreover, if the group key GK is revealed, this scheme is susceptible to various security threats. Unfortunately, it is difficult to safely manage the group key, and in the worst case, the cost for recovering the key is expensive. On the other hand, SK is used to protect most messages in spite of being shared among the MN, the MAP and its ARs. That makes Kang-Park's scheme dependent on the assumptions H3, H5, H7 and H9 to be robust.

B. Denial of Service attack

Because the *RtAdv* message is not protected, the MAP registration phase needs the additional assumption H0. This vulnerability enables an adversary to fabricate the message to deceive MNs into believing that they have just entered a victim MAP's domain. Consequently, the victim and the associated ASs are interrupted while postponing their meaningful jobs.

C. Malicious mobile node flooding attak

Without the supposition H1, the MAP just trusts that the MN beleives $LCoA$ in the MAP registration phase. Similarly, after the handover phase, it just trusts that the MN believes $nLCoA$. Thus, in Kang-Park's scheme, the MAP cannot ensure that the MN is really present at the asserted $LCoA$ or $nLCoA$. That makes this scheme vulnerable to the malicious mobile node flooding attack. Let us assume there is a malicious but legitimate MN. While exploitng this security flaw, it can launch the malicious mobile node flooding attack as follows:

(1) A victim network is selected and analyzed.
(2) The MN makes sessions with corresponding nodes, which can result in excessive traffic.
(3) The adversary counterfeits an *FBU* message indicating that it is moving to the victim network.
(4) The MN sends the forged message to the MAP whithout moving to the victim network. If the MAP believes the forged message, it starts to redirect the MN's traffic to the victim network.

As a result of this attack, the victim network will be flooded with excessive traffic.

D. Replay attak

The *RtSolPr* and *PrRtAdv* messages have no freshness. Thus, the messages can be replayed. Especially, an adversary can launch DoS attacks by replying the *PrRtAdv* message. For this goal, it collects proper messages in advance.

V. Conclusion

Based on BAN-logic, we formally analyzed Kang-Park's security scheme, and then discussed its the weaknesses and related attacks. According to our analysis, the scheme suffers from the dependency on the group key while being vulnerable to the denial of service, malicious mobile node flooding and replay attacks. We believe that our analysis and discussions are meaningful to enhance the security for F-HMIPv6.

Acknowledgment

This work was supported by the National High Technology Research and Development Program (863 Program) of China (Nos. 2006AA01Z172 and 2008AA01Z106), National Natural Science Foundation of China (Nos. 60773089 and 60533040), National Science Fund for Distinguished Young Scholars (NSFC, No.60725208), and Shanghai Pujiang Program (No. 07pj14049).

References

[1] R. Koodli, "Mobile IPv6 Fast Handovers," IETF RFC 5268, June 2008.

[2] H. Soliman, C. Castelluccia, K. ElMalki, L. Bellier. "Hierarchical Mobile IPv6 (HMIPv6) Mobility Management," IETF RFC 5380, October 2008.

[3] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6," IETF RFC 3775, June 2004.

[4] H. Jung, H. Soliman, S. Koh and J. Lee, "Fast Handover for Hierarchical MIPv6 (F-HMIPv6)," IETF Internet Draft, draft-jung-mobopts-fhmipv6-00.txt, April 2005.

[5] H. Jung, E. Kim, J. Yi and H. Lee, "A scheme for supporting fast handover in hierarchical mobile IPv6 networks," ETRI Journal, vol. 27, no. 6, pp. 798-801, December 2005.

[6] S. Fu and M. Atiquzzaman, "Handover latency comparison of SIGMA, FMIPv6, HMIPv6, and FHMIPv6," IEEE GLOBECOM 2005, vol. 6, pp. 3809-3813, December 2005.

[7] H. Kang and C. Park, "Authenticated Fast Handover Scheme in the Hierarchical Mobile IPv6," Lecture Notes in Computer Science 4298, pp. 211-224, 2007.

[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. Computer Systems, vol. 8, no. 1, pp. 18-36, 1990.