Forwarding Scheme Extension for Fast and Secure Handoff in Hierarchical MIPv6*

Hoseong Jeon[1], Jungmuk Lim[1], Hyunseung Choo[1], and Gyung-Leen Park[2]

[1] School of Information and Communication Engineering, Sungkyunkwan University, 440-746, Suwon, Korea
{liard, izeye, choo}@ece.skku.ac.kr
[2] Computer Science and Statistics Department, College of Natual Science, Cheju National University,
glpark@cheju.ac.kr

Abstract. Quality of service (QoS) and security in Mobile IP networks are becoming significant issues due to an increasing number of wireless devices [1]. For this reason, the Hierarchical Mobile IPv6 (HMIPv6) protocol [2] and the Authentication, Authorization, and Accounting (AAA) protocol [3] are proposed. However this protocol has inefficient authenticating and binding update procedures that limit its QoS. In this paper, we propose a forwarding scheme extension for fast and secure handoff that can reduce a handoff delay while maintaining a security level by a forwarding and session key exchange mechanism. The performance results show that the proposed mechanism reduces the handoff latency up to 10% and the handoff failure rate up to 25% compared to the previous mechanism.

1 Introduction

Based on mobility as the essential characteristic for mobile networks, the Mobile IP standard solution for use with the wireless Internet was developed by the Internet Engineering Task Force (IETF) [4]. However, Mobile IP does not extend well to highly mobile users. When a mobile node (MN) moves from one subnet to another one, it must send a location update to its home agent (HA) even though the MN does not communicate with others. These location updates incur the latency of messages traveling to the possibly distant home network [5]. Moreover, the term mobility implies higher security risks than static operation in fixed networks, since the traffic may at times take unexpected network paths with unknown or unpredictable security characteristics. Hence, there is a need to develop technologies that simultaneously enable IP security and mobility over wireless links.

* This work was supported in parts by Brain Korea 21 and the Ministry of Information and Communication in Republic of Korea. Dr. H. Choo is the corresponding author.

V.S. Sunderam et al. (Eds.): ICCS 2005, LNCS 3515, pp. 468–476, 2005.

For this reason, the IETF suggests that the Hierarchical Mobile IPv6 (HMIPv6) and the Authentication, Authorization, and Accounting (AAA) protocol be employed. HMIPv6 adds hierarchy, built on MIPv6, which separates local from global mobility. In the HMIPv6, inter-handoff (global mobility) is managed by the MIPv6 protocols, while intra-handoff (local mobility) is managed locally.

In the basic AAA protocol, AAA server distributes the session keys to the MN and agents to guarantee security during data transmission. Yet, while an MN roams in foreign networks, a continuous exchange of control messages is required with the AAA server in the home network. Thus, the standard AAA handoff mechanism has inefficient authenticating procedures limiting its QoS. To resolve such problems, the forwarding scheme [6] and the session key exchange mechanism [7] are proposed.

The forwarding scheme is the proposed solution to the complications when the MN is required to send a binding update (BU) message to the HA during inter-handoff. In this scheme, the MN sends BU messages to a previous Mobility Anchor Point (MAP), subsequently the previous MAP forwards packets to a new MAP. The session key exchange mechanism essentially reuses the previously assigned session keys. This mechanism is important as it can drastically reduce the handoff delay. However, this mechanism requires that a trusted third party support the key exchange between the Access Routers (AR). For this reason, it uses only the intra-handoff within the same domain.

In this paper, we propose a modified session key exchange mechanism combined with a forwarding scheme. In Section 2, an overview of the HMIPv6 and AAA protocol is presented and the session key exchange mechanism and the forwarding scheme are given. Our proposed mechanism is discussed in Section 3. Performance evaluation for the proposed and previous methods follows in Section 4. Finally we conclude the paper in Section 5.

2 Preliminaries

In HMIPv6, global (between-site) mobility is managed by the MIPv6 protocol, while local (within-site) handoffs are managed locally. A new node in HMIPv6, termed the MAP serves as a local entity to aid in mobile handoffs. The MAP, which replaces MIPv4's foreign agent, can be located anywhere within a hierarchy of routers. In contrast to the foreign agent (FA), there is no requirement for a MAP to reside on each subnet. The MAP helps to decrease handoff-related latency since a local MAP can be updated faster than a HA of the MN.

Using MIPv6, a mobile node sends location updates to any node it corresponds with each time it changes its location, and at intermittent intervals otherwise. This involves a lot of signaling and processing, and requiring a lot of resources. Furthermore, although it is not necessary for external hosts to be updated when a mobile node moves locally, these updates occur for both inter and intra-handoffs. By separating inter and intra-handoff, HMIPv6 makes it possible to deal with either situation appropriately [2].

In this scheme, the MN moves around in a local domain based primarily on HMIPv6 as follows. The MN entering a MAP domain will receive a router advertisement message containing the information for one of several local ARs. It binds its current location with an address on the subnet of the MAP (RCoA). Acting as a local HA, the MAP will receive all packets on behalf of the MN and will encapsulate and forward them directly to the MN's current address. If the MN changes its current address within the local MAP domain (LCoA), it only needs to register the new address with the MAP. Hence, only in the beginning does the RCoA need to be registered with CNs and the HA. The RCoA remains constant as long as the MN moves around within the MAP domain. This makes the MN's mobility transparent to the CNs it is communicating with. Nevertheless, this protocol is restricted to apply only to the intra-handoff cases.

The Forwarding Scheme: The forwarding scheme improves the global mobility of HMIPv6. This scheme operates as follows. If the MN enters an initial regional network, and then the MAP_0 in its subnet will function as the MAP. When the MN enters a MAP_1 domain, it sends the BU message to the MAP_1, and the MAP_1 sends it back to the MAP_0. When the MAP_0 receives its message, it compares it to the MAP list and finds the MN's field. It then updates the current MAP address of the MN. After that, the MAP_0 relays the packet to the MAP_1 without the binding update through the HA. Fig. 1 shows the mechanism of the forwarding scheme [6].

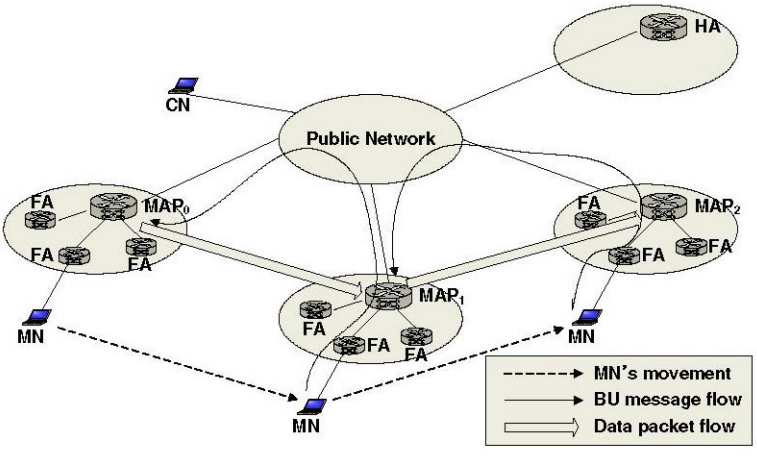

Fig. 1. The forwarding scheme

AAA Protocol: The IETF AAA Working Group has worked for several years to establish a general model for: Authentication, Authorization, and Accounting. AAA in a mobile environment is based on a set of clients and servers (AAAF and AAAH) located in the different domains. AAA protocol operates based on the security associations (SA_s: SA_1, SA_2, SA_3, and SA_4) as shown in Fig. 2.

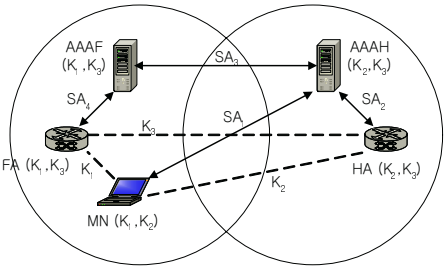

Fig. 2. AAA security associations

For the support regarding the secure communication, MN requires dynamic security associations. They are defined by sharing the session keys such as K_1, K_2, and K_3 between MN and HA, between HA and FA, and between FA and MN, respectively. Once the session keys have been established and propagated, the mobile devices can securely exchange data [8].

Session Key Exchange Mechanism: The Diffie-Hellman key agreement protocol depends on the discrete logarithm using two system parameters p and g. This scheme is based on a variant of Diffie-Hellman key agreement protocol instead of public key cryptography. Fig. 3 shows the session key exchange procedures. In fast operations, this scheme reuses the previously assigned session keys: the session keys for FA (S_{MN-FA} and S_{FA-HA}). To ensure the confidentiality and integrity of the session keys, it uses the encryption and decryption under a short lived secret key, $K_{oFA-nFA}$, between oFA and nFA. The key is dynamically shared between them and can be created by only two entities. However, there is a significant defect only applicable to intra-handoff [7].

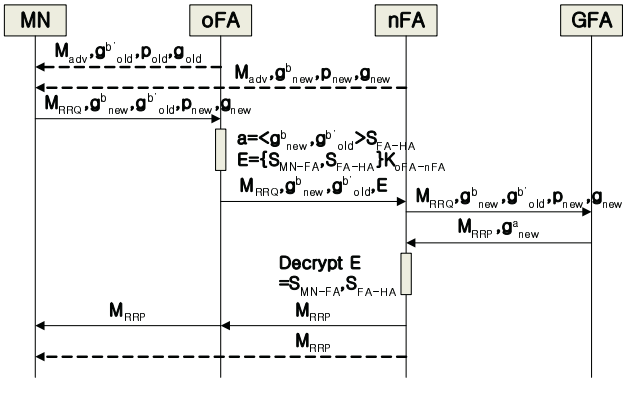

Fig. 3. Session key exchange mechanism

3 Proposed Mechanism

In this section, we describe the forwarding scheme for fast and secure handoff based on session key reuse. In this mechanism, the following assumptions are made:

- To prevent eavesdropping, all messages should be encrypted and exchanged in a secure process
- FAs related to the intra-handoff are trusted, that is, MAP authenticates them. Thus impersonating attack is not considered
- For the fast and secure inter-handoff, the AAA server can exchange session keys between FAs

The proposed mechanism improves the shortage of the previous authentication and binding update. The proposed scheme is divided into two parts according to the handoff type: 1) In the intra-handoff, our proposed scheme uses the session key reuse scheme by MAP and the micro-mobility management of HMIPv6. 2) In the inter-handoff, it uses the session key reuse scheme by AAA server and the forwarding mechanism.

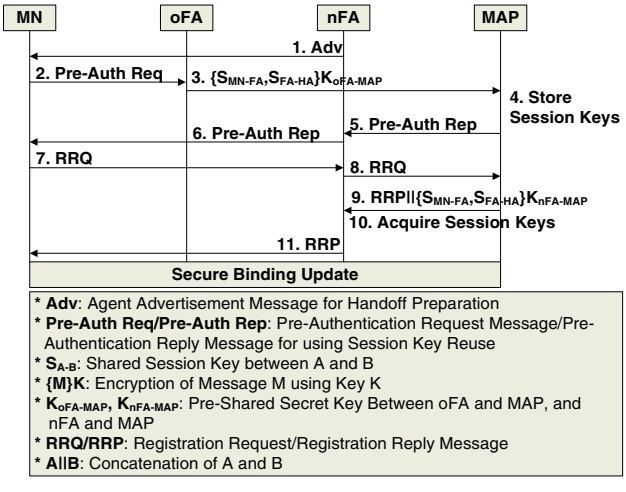

Fig. 4. The message procedure at intra-handoff

Fig. 4 shows the message procedure during intra-handoff. When the MN receives the agent advertisement message of nFA, it requests to the oFA for the reuse of the session key by sending Pre-Auth Req. After that, the oFA encrypts the session keys of itself by $K_{oFA-MAP}$ and then delivers them to the MAP. The MAP stores these session keys until it receives the registration request from the MN for the intra-handoff. If the MAP receives a RRQ message from the nFA, it sends a RRP message with $\{S_{MN-FA}, S_{FA-HA}\}K_{nFA-MAP}$. Finally, the nFA acquires these session keys and then sends a RRP message to the MN. Hence, the MN can send a binding update message in a secure fashion.

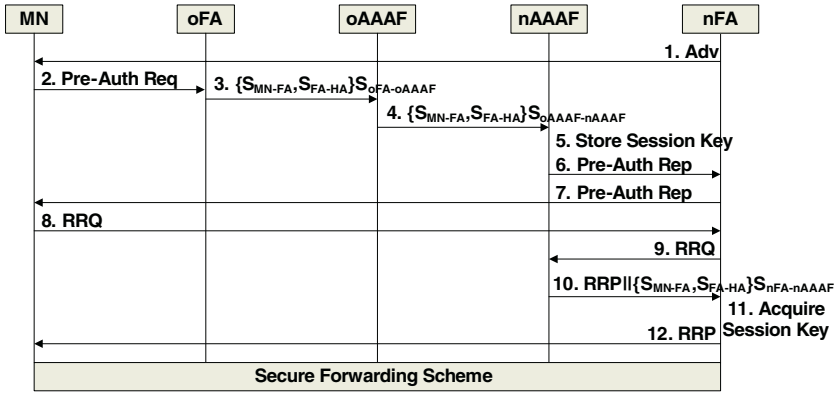

Fig. 5. The message procedure at inter-handoff

Fig. 5 shows the message procedure during inter-handoff. When the MN moves towards the region of nFA, it receives an agent advertisement message. Now the MN sends a pre-authentication request message. The oFA encrypts its session keys by the security association between the oFA and the oAAAF server, subsequently delivering it to the oAAAF server. The oAAAF server delivers it to the nAAAF server. The nAAAF server stores these session keys until it receives the registration request from the MN for the inter-handoff. If the nAAAF server receives a RRQ message from the nFA, it sends a RRP message with $\{S_{MN-FA}, S_{FA-HA}\}S_{nFA-nAAAF}$. Finally, the MN reduces the binding update time by using forwarding scheme while maintaining the security.

4 Performance Evaluation

4.1 Modeling

In order to evaluate the performance of our proposed algorithm, we make the following notations:

- $T_{MN-AR}/T_{AR-MAP}/T_{HA-MAP}/T_{MAP-MAP}/T_{MAP-AAA}/T_{AAA-AAA}$: The transmisson time between the MN and AR/the AR and MAP/the HA and MAP/MAPs/the MAP and AAA server/AAA servers, respectively.
- $P_{AR}/P_{HA}/P_{MAP}/P_{AAA}$: The processing time at the AR/the MAP/the HA/ the AAA server, respectively.
- T_H/T_R: The registration time of the home registration time/the regional registration time, respectively.
- T_M: The time to establish a link between MAPs
- $A_H/A_R/A_M$: The authentication time based on the basic AAA protocol/the session key reuse scheme by MAP/the session key reuse scheme by AAA server, respectively.

We calculate times required for the performance evaluation using the following equations as above notations. First of all, the HMIPv6 binding update time (BU) is represented as:

$$BU_{Intra}^{HMIPv6} = 2T_{MN-AR} + 2T_{AR-MAP} + 2P_{AR} + 2P_{MAP} \quad (1)$$

$$BU_{Inter}^{HMIPv6} = 2T_{MN_AR} + 2T_{AR-MAP} + 2T_{MAP-HA} + 2P_{AR} + 2P_{MAP} + P_{HA} \quad (2)$$

In the proposed scheme, we assume that the MN moves between the MAPs, and thus the binding update time is calculated as:

$$BU^{Proposed} = 2T_{MN-AR} + 2T_{AR-MAP} + 2T_{MAP-MAP} + 2P_{AR} + 3P_{MAP} \quad (3)$$

The total authentication time (AT) in the standard AAA protocol is acquired as follows:

$$\begin{aligned} AT^{Std} = {} & 2T_{MN-AR} + 2T_{AR-MAP} + 2T_{MAP-AAA} + 2T_{AAA-AAA} + \\ & AS + 2T_{MAP-AAA} + 2T_{MAP-HA} + 2P_{AR} + 4P_{MAP} + 2P_{HA} \end{aligned} \quad (4)$$

Finally, the total authentication time in the proposed scheme is calculated as shown below.

$$AT_{Intra}^{Proposed} = 2T_{MN-AR} + 2T_{AR-MAP} + 2P_{AR} + 2P_{MAP} \quad (5)$$

$$\begin{aligned} AT_{Inter}^{Proposed} = {} & 2T_{MN-AR} + 2T_{AR-MAP} + 2T_{MAP-AAA} \\ & + 2T_{AAA-AAA} + 2P_{AR} + 4P_{MAP} + 2P_{AAA} \end{aligned} \quad (6)$$

The probability (P_f) in which the MN leaves the boundary cell before the required time T_{req} is represented as $Prob(T < T_{req})$, where we assume T is exponentially distributed. Thus, the handoff failure rate as follows: $P_f = 1 - exp(-\lambda \cdot T_{req})$. λ is the arrival rate of MN into the boundary cell and its movement direction is uniformly distributed on the interval [0, 2π). Thus λ is calculated by the equation $\lambda = V \cdot L \ / \ \pi \cdot S$ [10]. Here V is the velocity for MN and L is the length of the boundary and S is the area of boundary. Hence we obtain the handoff failure rate by T_{req} and λ.

4.2 Analytical Results

Using above equations and the system parameters in Table 1 [5, 9, 10], we compute the cumulative handoff delay and the handoff failure rate. As shown in Fig. 6, our proposed scheme does not limit the number of forwardings as it always shows the better performance in the cumulative handoff latency. Consequently, our proposed scheme is limited by the freshness of the session key.

We perform an analysis of the handoff procedure to obtain the handoff failure rate according to each handoff mechanism. The handoff failure rate is influenced by few factors: the velocity of MN and the radius of a cell. Fig. 7 shows the result of the handoff failure rate. The proposed scheme consistently shows the better handoff failure rate in comparison with previous mechanisms.

Table 1. System parameters

Bit rates		**Processing time**	
Wire/Wireless	100/2 *Mbps*	MN/AR/MAP/AAA	0.5 *msec*
Propagation time		3DES	0.5 *msec*
Wire/Wireless	0.5/2 *msec*	MAC (Message Authentication Code)	0.5 *msec*
Data size		AS (Authentication time in server)	6.0 *msec*
Message size	256 *bytes*		

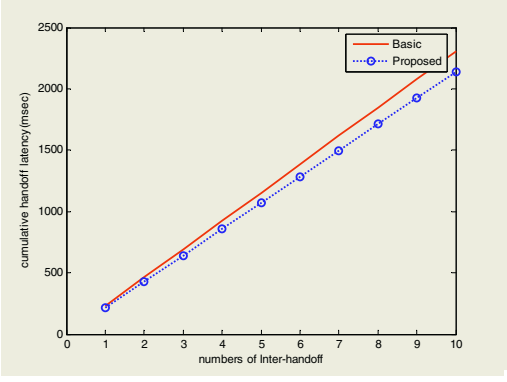

Fig. 6. The cumulative handoff latecny

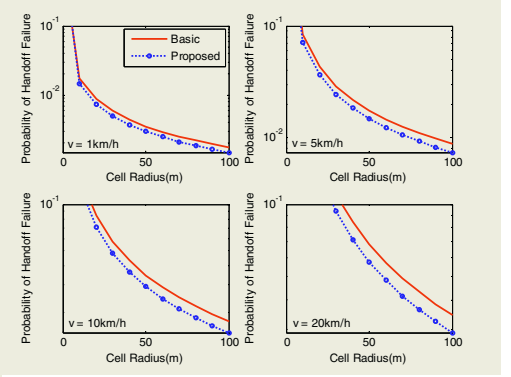

Fig. 7. The handoff failure rate

5 Conclusions

In this paper, we have proposed the forwarding scheme extension for fast and secure handoff employing a forwarding scheme and session key exchange mechanism in order to provide reduced handoff latency while maintaining the previous mechanism's security level. The performance comparison results show that the proposed mechanism is superior to the previous ones in terms of handoff latency while maintaining the security level. We are currently conducting an analysis of the threshold of the session key freshness.

References

1. C. Perkins, "IP Mobility Support," IETF RFC 2002.
2. H. Soliman, "Hierarchical Mobile IPv6 mobility management (HMIPv6)", IETF, October 2004.
3. C. Perkins, "Mobile IP Joins Forces with AAA," IEEE Personal Communications, vol. 7, no. 4, pp. 59–61, August 2000.
4. D. Johnson, "Mobility Support in IPv6", RFC 3775, IETF, June, 2004.
5. J. Vollbrecht, P. Calhoun, S. Farrell, L. Gommans, G. Gross, B. debruijn, C.de Laat, M. Holdrege, and D. Spence, "AAA Authorization Application Examples," IETF RFC 2905.

6. D. Choi, H. Choo, J. Park, "Cost Effective Location Management Scheme Based on Hierarchical Mobile IPv6," Springer-Verlag Lecture Notes in Computer Science, vol. 2668, pp. 144–154, May, 2003.
7. H. Kim, D. Choi, and D. Kim, "Secure Session Key Exchange for Mobile IP Low Latency Handoffs," Springer-Verlag Lecture Notes in Computer Science, vol. 2668, pp. 230–238, January 2003.
8. C. de Laat, "Generic AAA Architecture," RFC 2903, IETF, August, 2000.
9. H. Jeon, H. Choo, and J. Oh, "IDentification Key Based AAA Mechanism in Mobile IP Networks," ICCSA 2004 vol. 1, pp. 765–775, May 2004.
10. J. McNair, I.F. Akyildiz, and M.D Bender, "An inter-system handoff technique for the IMT-2000 system," INFOCOM 2000, vol. 1, pp. 203–216, March 2000.