On AAA Based on Brokers and Pre-encrypted Keys in MIPv6*

Hoseong Jeon, Min Young Chung, and Hyunseung Choo

School of Information and Communication Engineering
Sungkyunkwan University
440-746, Suwon, Korea +82-31-290-7145
{liard,mychung,choo}@ece.skku.ac.kr

Abstract. For providing mobility services for users through the global Internet, Mobile IP (MIP) has been standardized by IETF. Since conventional MIP has been investigated without the support of the security, IETF suggests that the current servers capable of performing the authentication, authorization, and accounting (AAA) be used for secure services. However the quality of service (QoS) may be degraded due to inefficiency on integrating the conventional MIP and AAA. For this, we propose a fast and secure handoff mechanism based on IDentification Key (IDK) along with Authentication Value (AV). Also we evaluate the performance of the proposed scheme in terms of the probability of handoff failure and average latency. The results show that our proposed mechanism yields better performance than session key exchange mechaism [11] and ticket based one [12] while maintaining the similar level of security.

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) [1, 2]. However, Mobile IP does not extend properly to highly mobile users. Moreover, the term mobility implies higher security risks than static operation in wired 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 [3].

By combining Mobile IP and AAA structure [4], the message on the Mobile IP network can be provided with additional security through AAA protocol. However, while an Mobile Node (MN) roams in foreign networks, a continuous exchange of control messages is required with the AAA server in the home network [5–8]. The control message contains the confidential information to identify the privilege of the mobile user for the service. Standard AAA handoff mechanism has inefficient authenticating procedures that limit its quality of service (QoS). To resolve such problems, session key exchange mechanism [11] and ticket based mechanism [12] are proposed in the literature.

* This paper was supported in parts by Brain Korea 21 and the Ministry of Information and Communication, Korea. Corresponding author: H. Choo.

J.C. Cunha and P.D. Medeiros (Eds.): Euro-Par 2005, LNCS 3648, pp. 1130–1139, 2005.

The session key exchange mechanism, basically, reuses the previously assigned session key. In this mechanism, the handoff delay can be decreased importantly. However, it requires that the trusted third party should support key exchanges between Access Routers (ARs). For this reason, it uses only the intra-handoff within the same domain. The ticket based mechanism using an encrypted ticket that can support authentication and authorization for the MN has been proposed. It reduces the delay and the risk on MN authentication in Mobile IPv6 (MIPv6). However, it generates additional signalings and overheads of AAA server.

In order to reduce signaling delay required for performing authentication procedures we have proposed an IDK mechanism based on a pre-encrypted key [13]. However, it just uses service requests due to the mobility of MNs. For improving this shortage, an extended IDK mechanism (EIDK) has been proposed [14]. EIDK mechanism uses single AV to extend the effectiveness of IDK into the handoff process. EIDK with single AV compared with previous mechanisms is up to about 20-40% better in terms of average latency that considers handoff latency and service latency. However, it is vulnerable to the 'replay attack.' To handle this problem, we propose EIDK mechanism with multiple AVs and evaluate its average handoff latency for the reasonable number of AVs.

The rest of the paper is organized as follows. In Section 2, an overview of the Mobile IP and AAA protocol is presented. And the session key exchange mechanism and the ticket based AAA mechanism are given. Our proposed EIDK based AAA mechanism is discussed in Section 3. After that the performance is evaluated along with previous methods in Section 4. Finally we conclude the paper in Section 5.

2 Preliminaries

The IETF AAA Working Group has worked for several years to establish a general model for authentication, authorization, and accounting. AAA in mobile environments is based on a set of clients and servers (AAA Foreign and AAA Home) located in the different domains. It operates based on the security associations (SAs) (SA_s: $SA_1, SA_2, SA_3,$ and SA_4) as shown in Fig. 1. 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 Foreign Agent (FA), between MN and Home Agent (HA), and between HA and FA, respectively. Once the session keys have been established and propagated, the mobility devices can securely exchange data [9, 10].

Session Key Exchange Mechanism

The session key exchange mechanism is based on a variant of Diffie-Hellman key agreement protocol instead of asymmetric key cryptography [11].The protocol has two system parameters p and g. They are both public and may be used by all the users in a system. The p is a prime number and g (usually called a generator) is an integer less than p with the following property: for every number n between 1 and $p-1$ inclusive, there is a power k of g such that $n = g^k$ mod

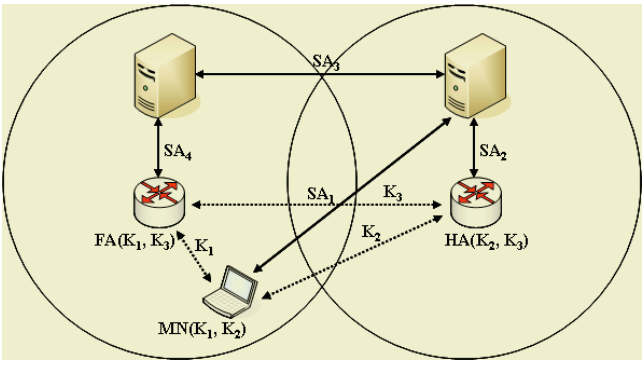

Fig. 1. AAA security association in Mobile IPv6

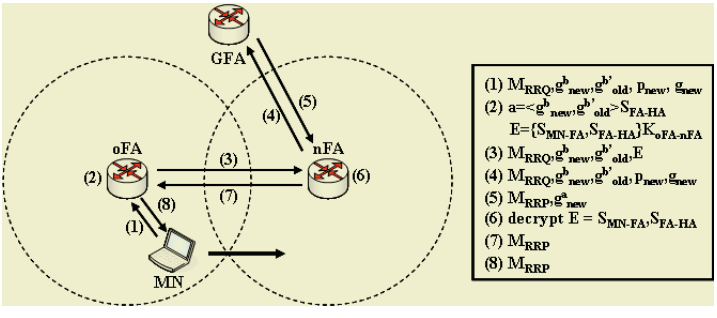

Fig. 2. Secure session key exchange procedure

p. The protocol depends on the discrete logarithm problem for its security. It assumes that it is computationally infeasible to calculate the shared secret key $k = g^a b \bmod p$ given the two public values ($g^a \bmod p$) and ($g^b \bmod p$) when the prime p is sufficiently large.

For the 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.

Ticket Based AAA Mechanism

A ticket based AAA mechanism reduces the overhead on the service request by utilizing the pre-encrypted ticket without intermediate encryptions and decryptions. If the MN wants to request a service, it sends a ticket to AAAH for its authentication. The authentication of MN is performed by the Ticket Granting Service ASM (TGS ASM) in the AAA server. The result of authentication is returned to the MN, which allows the MN to request the service [12].

However, this mechanism has four additional signaling messages for the ticket issue. Fig. 3 describes exchanged additional signaling messages on initial registration. Four messages added are ticket/service request message, AAA ticket/

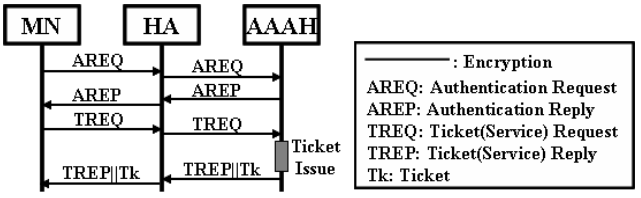

Fig. 3. Initial registration in ticket based AAA model

service request message, AAA ticket/service reply message, and ticket/service reply message. The messages between MN and HA are based on the general Mobile IP protocol, and the messages between HA and Home AAA server (AAAH) are based on the extended AAA protocol in Mobile IP networks.

EIDK Based AAA Mechanism with single AV
This mechanism reduces handoff and service signaling cost using IDK and AV [14]. However, it is vulnerable to the 'replay attack' due to a single AV its on use. It means that the malicious node traps the authentication sequence that has been transmitted by an authorized user through the network, and then has replayed the same sequence to get himself authenticated. In this case, the authorized user is attacked by the malicious one.

3 EIDK Based AAA Mechanism with Multiple AVs

This section deals with the secure enhanced EIDK mechanism using multiple AVs. Basically, this modified mechanism is identical to the previous EIDK proposed in [14], except using multiple AVs. For the proposed mechanism, we assume as follows: 1) an AAA server authenticates and authorizes subscribers, and verifies IDK. It also creates AV; 2) an AAA client is either HA or FA, which has the functionality to generate and to deliver AAA messages; 3) an AAA broker (AAAB) authenticates MN instead of AAA Home (AAAH); and 4) an MN generates IDK and delivers it.

In order to reduce the time for repeated encryptions and decryptions, an MN generates an encrypted information called IDK using authentication time (AT). This value represents the time at the initial registration of the MN. The IDK consists of the following [13]:

- Network Access Identifier (NAI) of MN
- Address of the AAA server that provides services to the MN
- Service identifier allowed for the MN
- Home network address and IP address of the MN
- IDK lifetime
- A random number (128 bits)
- The session key shared by the MN and the AAA server
- CoA of next possible area expected to be moved (optional)
- Authentication time (AT).

The proposed mechanism reduces the authentication delay and signalings at the foreign domain by using AV. The AV contains an information for MN and session keys in FA for the session key reuse. They are encrypted based on SA between AAAH and AAAB [4]. It consists of following:

$$AV = SA_{AAAH-AAAB} \{ MN\ information \,||\, FA's\ session\ keys \,||\, Nonce \}$$

Initial Registration to AAAH

As indicated in Fig. 4, the sequence of message exchanges for each authentication mechanism is performed for the initial registration in the home network. We assume that there is no security associate between MN and HA. This is because we do not consider the pre-shared key distribution in AAA protocol in this work.

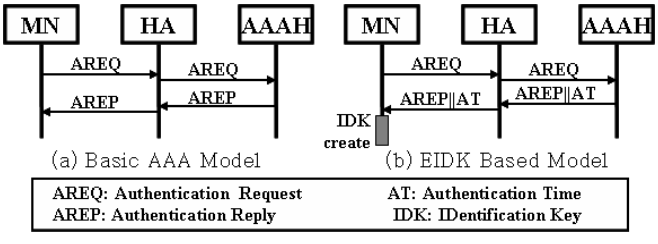

Fig. 4. Initial registration

Fig. 4(a) shows the initial registration of the basic AAA model. And both the ticket based model and the proposed EIDK based one follow the basic AAA model in the initial registration. However, as you see in Fig. 3, additional signaling for issuing a ticket is required for faster services on requests in the ticket based model.

Fig. 4(b) shows the initial registration procedure for the EIDK based mechanism. In the authentication reply phase, AT is delivered to MN together with authentication reply message (AREP). Accordingly, both the MN and AAAH server share a secret value. This one is the arrival time of the request message for the MN at AAAH. The AT would be used as a part of the encryption key value on IDK by MN and later it is used as the decryption key in AAAH. Unlike the ticket based model scheme, MN receives AT along with the authentication reply message without further additional signaling in our scheme.

Service Requests

The procedure routine of message exchanges for the service request in the home domain is in Fig. 5. The service request message (SREP) is encrypted and decrypted by the key distributed from AAAH on the authentication process in the basic AAA model. As you see in Fig. 5(a), service request message (SREQ) and SREP are encrypted and decrypted at MN, HA, and AAAH whenever they are exchanged, and these can be a significant overhead. Ticket based model in Fig. 5(b) reduces the overhead on the service request by utilizing the pre-encrypted ticket without intermediate encryptions and decryptions. This can be done by the extended AAA server structure. Also the model assumes that the

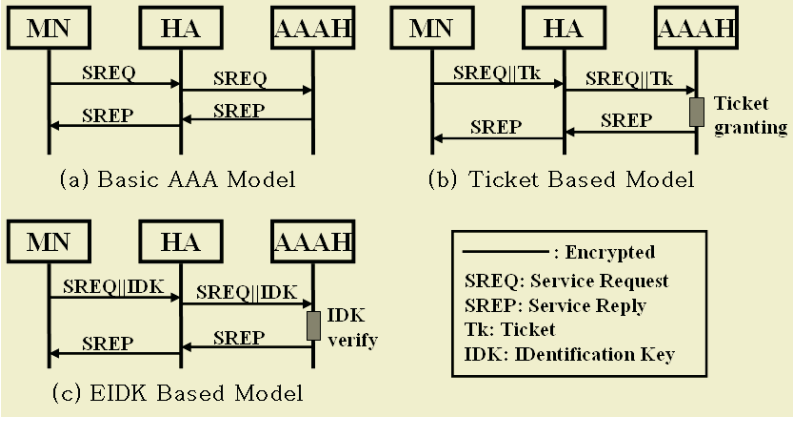

Fig. 5. Service request

time for ticket issuing and granting is not significant. However, this may not guarantee its superiority in the real world.

In Fig. 5(c), the proposed EIDK based model does not need the extended AAA server structure, but just maintains the current one. Intermediate encryptions and decryptions are not necessary on the service request in our scheme. Since we employ the pre-encrypted IDK which is created by MN beforehand. Unlike the basic AAA model, the EIDK based AAA model requires IDK creation and the time for it. But this scheme reduces the total delay since it eliminates the time for intermediate encryptions and decryptions.

Handoff Procedures Using Multiple AVs

The purpose of multiple AVs is to improve previous EIDK mechanism. We propose the usage of multiple AVs for the preventing 'replay attack.' Each AV is used only once and then it is no longer valid, so eavesdropping and replay attack are not our concern.

Fig. 6 represents the proposed handoff mechanism. It eliminates encryption and decryption delay in the authentication procedure by using pre-encrypted AV, and reduces the number of signalings due to the AAAB. When MN moves to a foreign network, AAAH creates AVs that are delivered to the AAAB. After

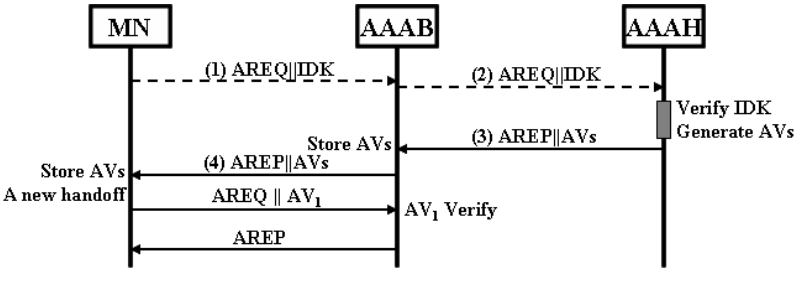

Fig. 6. Description of handoff mechanism using AVs

that operation, the AAAB authenticates MN instead of AAAH. As a result, the MN reduces authentication procedure and its delay in the foreign network since AAAB takes care of authentication job for MN on behalf of its AAAH. If there is no AVs in AAAB, the proposed scheme should perform the procedure from (1) to (4) once more. According to the number of AVs, the performance of this scheme is affected. It is considered as factors in performance analysis in the following section.

4 Performance Evaluation

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

- $T_{MN-AR}/T_{AR-AAAH(F)}/T_{AAAH(F)-AAAB}$: time required for transfer in a message between MN and AR/AR and AAAH(F)/AAAH(F) and AAAB.
- E_{se}/E_{sd}: time required for symmetric key encryption/decryption of a message at MN/AR/AAAH/AAAF/AAAB
- BU: binding update time
- AS: authentication time in AAAH
- Tk: ticket issuance and verification time in AAAH
- IDK: IDK creation and verification time in MN/AAAH/AAAB
- AV: authentication time using AV in AAAB
- $B_{IR}/T_{IR}/E_{IR}$: time required for initial registration as basic AAA scheme/as ticket based scheme/as EIDK based scheme.
- $B^{H/F}_{Intra}/S^{H/F}_{Intra}/E^{H/F}_{Intra}$: time required for intra handoff as basic AAA scheme/ as session key exchange scheme/as EIDK based scheme in home(foreign) domain
- $B_{Inter}/S_{Inter}/E_{Inter}$: time required for inter handoff as basic AAA scheme/ as session key exchange scheme/as EIDK based scheme
- $B^{H/F}_{Serv}/T^{H/F}_{Serv}/E^{H/F}_{Serv}$: time required for service request as basic AAA scheme/ as ticket based scheme/as EIDK based scheme in home(foreign) domain

Authentication procedures can be classified into three cases: initial registration, handoff and service request. And then handoff can be also classified into another three cases by the position of the MN: intra handoff in home/foreign domain and inter handoff. Lastly, service request can be classified into two cases: service request in home/foreign domain. We calculate times required in schemes we discuss (Figs. 2–6) for performance evaluation based on the following equations:

- [Initial Registration]
  $B_{IR} = 2 \cdot T_{MN-AR} + 2 \cdot T_{AR-AAAH(F)} + 4 \cdot E_{se} + 4 \cdot E_{sd} + AS + BU$
  $T_{IR} = 2 \cdot (2 \cdot T_{MN-AR} + 2 \cdot T_{AR-AAAH(F)} + 4 \cdot E_{se} + 4 \cdot E_{sd}) + AS + Tk + BU$
  $E_{IR} = 2 \cdot T_{MN-AR} + 2 \cdot T_{AR-AAAH(F)} + 4 \cdot E_{se} + 4 \cdot E_{sd} + AS + BU + IDK$
- [Intra Handoff in the home domain]
  $B^{H}_{Intra} = 2 \cdot T_{MN-AR} + 2 \cdot T_{AR-AAAH(F)} + 4 \cdot E_{se} + 4 \cdot E_{sd} + AS + BU$
  $S^{H}_{Intra} = 4 \cdot T_{MN-AR} + 4 \cdot T_{AR-AAAH(F)} + 4 \cdot E_{se} + 4 \cdot E_{sd} + BU$
  $E^{H}_{Intra} = 2 \cdot T_{MN-AR} + 2 \cdot T_{AR-AAAH(F)} + 2 \cdot E_{se} + 2 \cdot E_{sd} + 2 \cdot IDK + BU$

- [Intra Handoff in the foreign domain]
  $B^F_{Intra} = 2 \cdot T_{MN-AR} + 4 \cdot T_{AR-AAAH(F)} + 4 \cdot T_{AAAH(F)-AAAB} + 10 \cdot E_{se} + 10 \cdot E_{sd} + AS + BU$
  $S^F_{Intra} = 4 \cdot T_{MN-AR} + 4 \cdot T_{AR-AAAH(F)} + 4 \cdot T_{AAAH(F)-AAAB} + 4 \cdot E_{se} + 10 \cdot E_{sd} + AS + BU$
  $E^F_{Intra} = 2 \cdot T_{MN-AR} + 2 \cdot T_{AR-AAAH(F)} + 2 \cdot T_{AAAH(F)-AAAB} + 3 \cdot E_{se} + 3 \cdot E_{sd} + 2 \cdot IDK + BU$
- [Inter Handoff]
  $B_{Inter} = 2 \cdot T_{MN-AR} + 4 \cdot T_{AR-AAAH(F)} + 4 \cdot T_{AAAH(F)-AAAB} + 10 \cdot E_{se} + 10 \cdot E_{sd} + AS + BU$
  $S_{Inter} = 4 \cdot T_{MN-AR} + 4 \cdot T_{AR-AAAH(F)} + 4 \cdot E_{se} + 4 \cdot E_{sd} + BU$
  $E_{Inter} = 2 \cdot T_{MN-AR} + 2 \cdot T_{AR-AAAH(F)} + 2 \cdot T_{AAAH(F)-AAAB} + 3 \cdot E_{se} + 3 \cdot E_{sd} + 2 \cdot IDK + BU$
- [Service request in home domain]
  $B^H_{Serv} = 2 \cdot T_{MN-AR} + 2 \cdot T_{AR-AAAH(F)} + 4 \cdot E_{se} + 4 \cdot E_{sd} + AS + BU$
  $T^H_{Serv} = 2 \cdot T_{MN-AR} + 2 \cdot T_{AR-AAAH(F)} + 2 \cdot E_{se} + 2 \cdot E_{sd} + Tk + BU$
  $E^{Home}_{Serv} = 2 \cdot T_{MN-AR} + 2 \cdot T_{AR-AAAH(F)} + 2 \cdot E_{se} + 2 \cdot E_{sd} + IDK + BU$
- [Service request in foreign domain]
  $B^F_{Serv} = 2 \cdot T_{MN-AR} + 4 \cdot T_{AR-AAAH(F)} + 4 \cdot T_{AAAH(F)-AAAB} + 10 \cdot E_{se} + 10 \cdot E_{sd} + AS + BU$
  $T^F_{Serv} = 2 \cdot T_{MN-AR} + 4 \cdot T_{AR-AAAH(F)} + 4 \cdot T_{AAAH(F)-AAAB} + 5 \cdot E_{se} + 5 \cdot E_{sd} + Tk + BU$
  $E^F_{Serv} = 2 \cdot T_{MN-AR} + 4 \cdot T_{AR-AAAH(F)} + 4 \cdot T_{AAAH(F)-AAAB} + 5 \cdot E_{se} + 5 \cdot E_{sd} + IDK + BU$

Using these equations and the system parameter in Table 1 [10, 13, 14], we compute the handoff probability and the average latency.

Table 1. System parameters

Bit rates		**Processing time**	
Wire links	100 *Mbps*	Routers (HA,FA)	0.5 *msec*
Wireless links	2 *Mbps*	Nodes (MN)	0.5 *msec*
Propagation time		Tk	3.0 *msec*
Wire links	500 μ*sec*	IDK	3.0 *msec*
Wireless links	2 *msec*	AS	1.0 *msec*
Data size		AV	1.0 *msec*
Message size	256 *bytes*	E_{se} *and* E_{sd}	1.0 *msec*
		BU	0 *msec*

We analyze the handoff procedure to obtain the handoff failure rate for each handoff mechanism. It is influenced by few factors that are the velocity of MN and the radius of a cell. Figs. 7 and 8 show probability of handoff failure and average latency for various cell radii, respectively. From the results, secure exchange scheme shows the better performance for frequent handoff situations and ticket-based one has better result for frequent service requests. However, EIDK

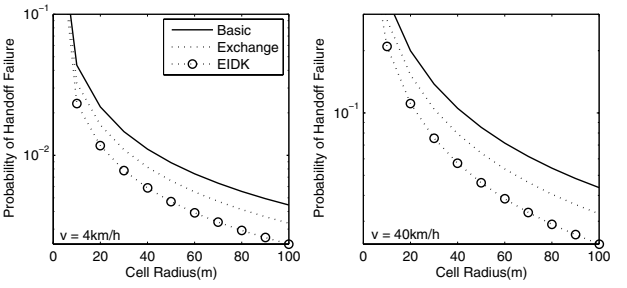

Fig. 7. The probability of handoff failure

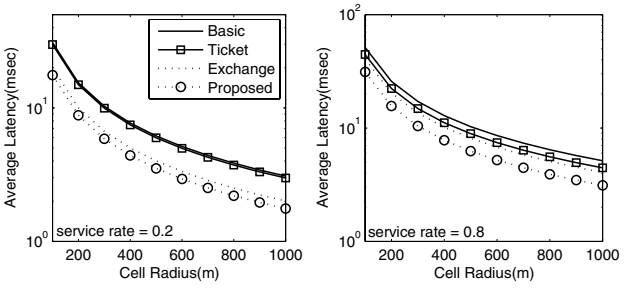

Fig. 8. Average handoff latency

based mechanism shows even better performance than previous mechanisms because it considers two factors the handoff latency and service latency at the same time.

Fig. 9 shows average latency of EIDK mechanism according to the number of AVs. It is indicated that the average latency for the modified scheme increases

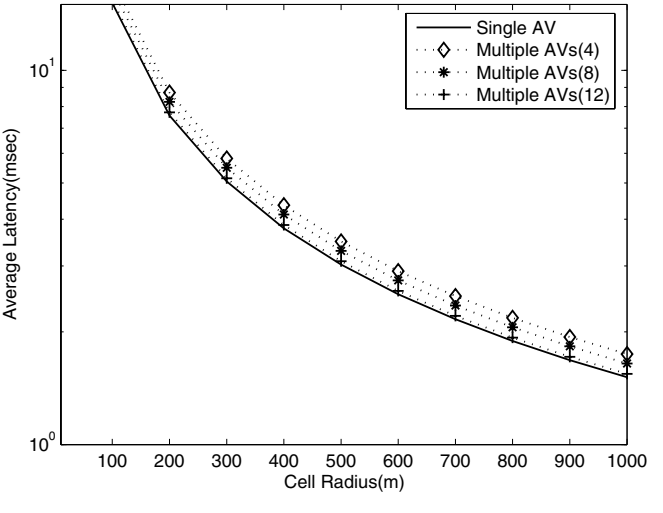

Fig. 9. Single AV versus multiple AVs

as the number of AVs is increases. For given cell radius, average latency of EIDK mechanism decreases as the number of AVs increases. However excessive number of AVs may cause additional overheads. Therefore it is important to select the appropriate number of AVs in this modified scheme.

5 Conclusion

In this paper, we proposed the EIDK based AAA mechanism with multiple AVs. This scheme prevents 'replay attack' for malicious users and reduces the latency due to handoffs and services. The performance comparison shows that the EIDK based mechanism is superior to previous schemes we disscuss in this paper in terms of latency while maintaining the same security level. Also, the performance of the proposed mechanism depends on the number of AVs employed. For further studies, researches on the optimal number of AVs are underway.

References

1. C.E. Perkins, "IP Mobility Support," IETF RFC 2002.
2. B. David, C. Perkins, and J. Arkko,"Mobility Support in IPv6," IETF draft, Internet Draft draft-ietf-mobileip-ipv6-17.txt, May 2002.
3. C. Perkins, "Mobile IP Joins Forces with AAA," IEEE Personal Communications, vol. 7, no. 4, pp. 59–61, August 2000.
4. J. Vollbrecht, P. Cahoun, S. Farrell, and L. Gommans, "AAA Authorization Framework," RFC 2904, 2000.
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. S. Farrell, J. Vollbrecht, P. Calhoun, and L. Gommans,"AAA Authorization Requirements," RFC 2906, August 2000.
7. S. Glass, T. Hiller, S. Jacobs, and C. Perkins, "Mobile IP Authentication, Authorization, and Accounting Requirements," RFC 2977, 2000.
8. A. Hasan, J. Jahnert, S. Zander and B. Stiller, "Authentication, Authorization, Accounting and Charging for the Mobile Internet," Mobile Summit, September 2001.
9. C. Yang, M. Hwang, J. Li, and T. Chang, "A Solution to Mobile IP Registration for AAA," Springer-Verlag Lecture Notes in Computer Science, vol. 2524, pp. 329–337, November 2002.
10. A. Hess and G. Schafer, "Performance Evaluation of AAA/Mobile IP Authentication," 2nd Polish-German Teletraffic, 2002.
11. 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.
12. J. Park, E. Bae, H. Pyeon, and K. Chae "A Ticket-based AAA Security Mechanism in Mobile IP Network," Springer-Verlag Lecture Notes in Computer Science 2003, vol. 2668, pp. 210–219, May 2003.
13. 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.
14. H. Jeon, M. Chung, and H. Choo, "On AAA with Extended IDK in Mobile IP Networks," ICCSA 2005 vol. 3480, pp. 538–539, May 2005.