ID-Based Secure Session Key Exchange Scheme to Reduce Registration Delay with AAA in Mobile IP Networks *

Kwang Cheol Jeong[1], Hyunseung Choo[1], and Sang Yong Ha[2]

[1] School of Information and Communication Engineering,
Sungkyunkwan University,
440-746, Suwon, Korea +82-31-290-7145
{drofcoms, choo}@ece.skku.ac.kr
[2] BcN Team IT Infrastructure Division,
National Computerization Agency, Korea

Abstract. Due to an increasing number of portable devices, a support for quality of service (QoS) and security becomes an main issue in Mobile IP networks. However Authentication, Authorization, and Accounting (AAA) protocol has inefficient authenticating procedures that limit its QoS. That is, a mobile node (MN) should be distributed new session keys whenever it performs a handoff. As computing power of mobile devices becomes greater, a key distribution using a symmetric key cannot guarantee the security. Hence, we employ an ID-based cryptography to intensify the security and when the MN moves to a new domain, a foreign agent (FA) reuses previous session keys encrypted by a public key for the fast handoff. Our proposed scheme reduces handoff delay and maintains high security by exchanging previous session keys between FAs. The performance results show that the proposed scheme reduces the latency up to about 63% compared to the previous ID-based AAA.

1 Introduction

Based on mobility as the essential characteristic for mobile networks, the Mobile IP de facto standard solution for use with the wireless Internet was developed by the Internet Engineering Task Force (IETF). Because the mobility implies higher security risks than static operations in fixed networks, there is a need to develop technologies which will jointly enable IP security and the mobility over wireless links, and thus adapting Mobile IPv6 to AAA protocol is suggested [2].

In the basic AAA protocol, AAA server distributes the session keys to MNs and agents to guarantee the security when they transmit data. Currently AAA protocol guarantees the security by using symmetric keys for information protection. Due to the drastically increasing computing power of devices, reliability

* 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. 510–518, 2005.

on transmitting data based on symmetric keys can be threatened. Hence it is desirable to consider AAA protocol using asymmetric keys to enhance the security level. However when we consider Mobile IP networks which should support high mobility patterns, it seems hard to apply due to heavy operations. In the previous works whenever an MN arrives at a new domain, it performs a registration with its home network and after the MN is successfully authenticated and authorized, AAA server generates Mobile IP session keys (Mobile-Foreign, Foreign-Home, and Mobile-Home session key), but these processes need lots of operation time. In typical public key cryptography, the user's public key is explicitly encoded in a public key certificate. Therefore, the Public Key Infrastructure (PKI) model requires universal trust among the certificate issuers such as Certificate Authorities (CAs). This also has some well-known side effects such as cross-domain trust and certificate revocation. Moreover, PKI should maintain the structures such as CAs, Registration Authorities (RAs), and a directory servers containing certificates. Therefore, Shamir introduces an ID-based cryptography concept which simplifies certification management process [8].

In this paper, we propose an ID-based session key reuse mechanism which enhances the security in forwarding session keys and reduces the handoff time. In Section 2, an overview of the Mobile IP with AAA protocol, modern data encryption, and Identity (ID)-based cryptography are presented. We discuss the proposed ID-based session key reuse mechanism in Section 3. After that its performance is evaluated with previous methods in Section 4. Finally we conclude the paper in Section 5.

2 Related Works

2.1 AAA Protocol in Mobile IP

Within the Internet, an MN in an administrative area called a home domain often needs to use resources provided by another administrative zone called a foreign domain. An agent in the foreign domain that attends to the MN's request is likely to require that the MN provide some credentials that can be authenticated before the access to foreign resources. The agent may not have direct access to the data that is needed to complete the transaction. Instead, the agent is expected to consult a foreign AAA server (AAAF) in the same foreign domain in order to obtain the proof that the MN has acceptable credentials. Since the agent and the AAAF are part of the same administrative domain, they are expected to have security relationships that enable to transact information securely.

Since the AAAF itself may not have enough information to verify the credentials of the MN, it is expected to configure the verification process of MN credentials with home AAA server (AAAH). Once the authorization has been obtained by the AAAF and the authority has notified the agent for the successful negotiation, the agent can provide the requested resources to the MN [7]. AAA protocol operates based on the security associations which are defined by sharing the session keys [9].

2.2 Identity (ID)-Based Cryptography

The concept of ID-based encryptions and signatures is first introduced by Shamir in [8]. The motivation is to simplify certificate management and the essential idea of the ID-based cryptosystem is that any string ID consisting of $\{0,1\}^*$ can be the public key, and the author explains this by giving the example of the e-mail system [8]. The users should contact the Private Key Generator(PKG) to obtain a private key. Hence the ID-based cryptosystem does not need to access the public key directory and that means there is no need of PKI. Fig. 1 shows the comparison between a public key cryptosystem and an ID-based cryptosystem. For the secret communication in the public key cryptosystem, a sender should access to the public key directory for acquiring a public key. However in the ID-based cryptosystem, there is no need to access to the directory because an identity which is opened in the public channel is also a public key.

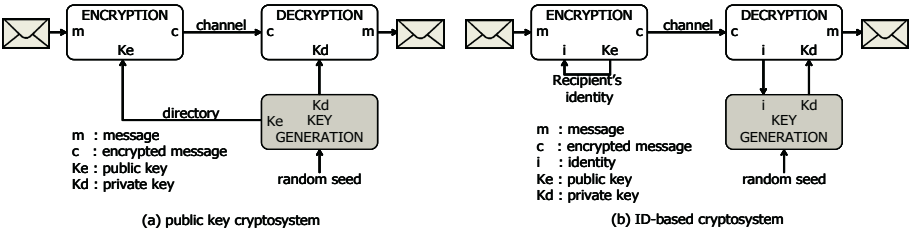


Fig. 1. Comparison between two cryptosystems

3 Session Key Reuse with ID-Based Cryptography

In this section, we describe the session key reuse mechanism with ID-based cryptography. In the proposed mechanism, we assume as follows:

- All nodes involved in Mobile IP with AAA protocol can calculate ID-based cryptography operations.
- Registration REPly (RREP) message includes the validity of MN without session keys.
- Private Key Generator (PKG) should have a master key to generate a private key corresponding to a public key for agents and MNs.

Fig. 3(a) and (b) show a Mobile IP registration procedure in AAA protocol [7] and a procedure of AAA protocol with an ID-based mechanism [4], respectively. The ID-based mechanism uses a digital signature for implementing mutual authentication which is one of main characteristics for the public key cryptosystem. In this case, because it is mutual authentication between the MN and Home Agent (HA), the authentication should occur at each entity (HA, FA, and AAAH) between the MN and the HA.

Fig. 3(c) shows the proposed AAA protocol with the ID-based mechanism which has modified procedure in the registration. The most remarkable difference

is that a new FA (nFA) receives previous session keys from an old FA (oFA). As you see in fig 3(b), the previous ID-based mechanism [4] should provide the signature verification at each entity between the MN and the HA because the MN should receive new session keys from the HA. As we all know, new session keys are issued by the AAAH and delivered through the HA. Meanwhile, the proposed mechanism provides the mutual authentication between oFA and nFA in the delivery of session keys. This minimizes the usage of the public key cryptography by using the previous session keys between oFA and HA at the registration reply from the HA and also provides the security from various attacks such as man in the middle attack. However, permanent using of issued previous session keys may cause another security problem. So there is a need to issue new session keys periodically based on timeout.

Registration Procedure in MIP with AAA Protocol

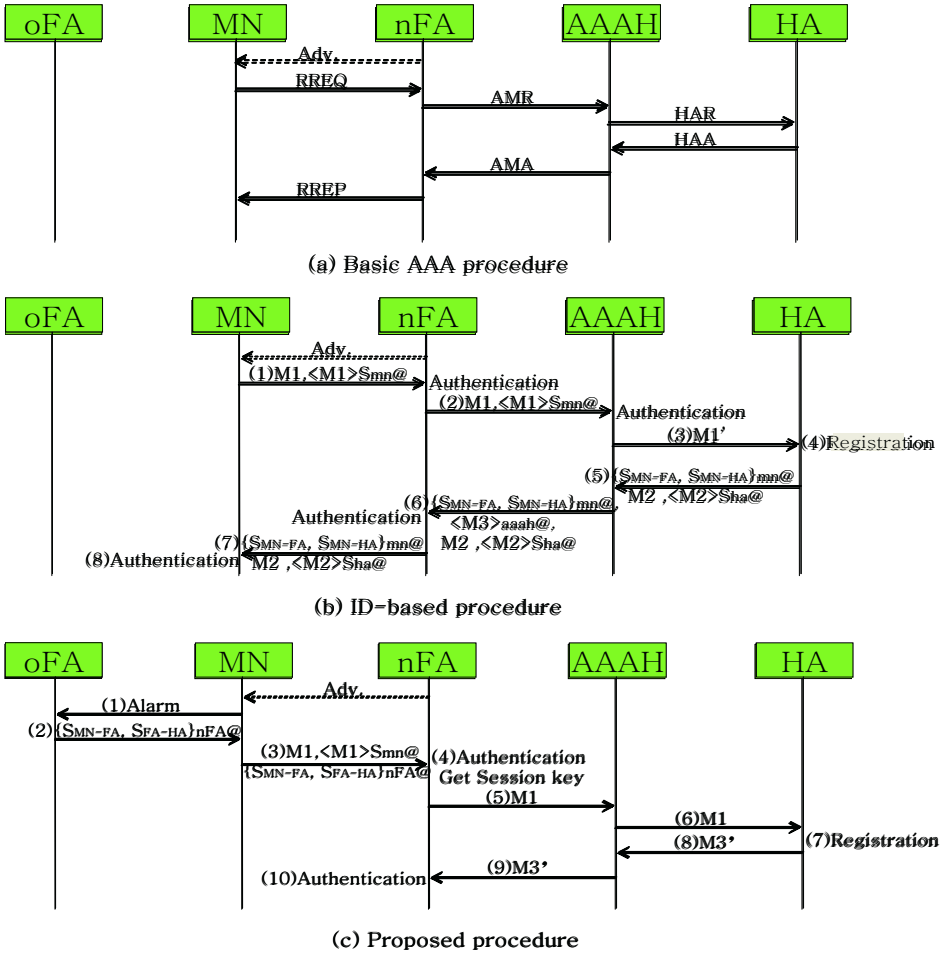
The following steps describe a process for the registration and authentication procedures in the ID-based mechanism. Refer to Fig. 3(b) and Table 1.

(1) When the MN detects the handoff is impended, it generates $M1$(corresponding to RREQ in Basic AAA procedure) and $<M1>S_{mn@}$ which is a signature for $M1$ based on the MN's ID, then sends them to an nFA. (2) The nFA authenticates the $M1$ based on the MN's ID and forwards messages to AAAH. (3) The AAAH also authenticates the $M1$ and sends $M1'$ ($M1$ with new session keys generated by AAAH) to HA. (4) After the HA registers a new CoA, (5) it encrypts two session keys S_{MN-FA} and S_{MN-HA} based on the MN's ID, and generates $M2$(corresponding to HAA in Basic AAA procedure) and its signature based on the HA's ID. Then it sends them to the AAAH. (6) The AAAH generates the signature of $M3$ and sends it along with all received messages to the nFA. (7) The nFA authenticates the $M3$ and sends all received messages except for $<M3>S_{mn@}$. (8) The MN authenticates the $M2$ based on the HA's ID and acquires two session keys. However, due to the absence of a security association between the MN and the nFA, it is vulnerable for some attacks at this point.

Table 1. Notation

Notation	Description
ID	Identity (e.g. e-mail address)
S_{ID}	Private Key for ID
aaah@	ID of AAAH
ha@	ID of HA
mn@	ID of MN
M	A message
$<M>S_{ID}$	Signature of M with S_{ID}
$\{M\}_{ID}$	Encryption of M with ID

And the following steps explain a process for the registration and authentication in our proposed ID-based mechanism. Refer also to Fig. 3(c) and Table 1.



RREQ: Registration Request message
RREP: Registration Reply message
AMR: AA-Mobile-Node Request message
AMA: AA-Mobile-Node Answer message
HAR: Home-Agent-MIP-Request message
HAA: Home-Agent-MIP-Answer message
AAAF: Authentication, Authorization and Accounting Server in Foreign Network
AAAH: Authentication, Authorization and Accounting Server in Home Network
M1: RREQ in ID-based Mechanism
M1': M1 with Session Keys
M2: HAA in ID-based Mechanism
M3: AMA with M2, $<M2>_{ha@}$
M3': AMA with Validity of the MN instead of Session Keys

Fig. 2. Registration procedures

(1) When the MN detects that the handoff is impended, it sends an alarm message which contains the nFA's ID to the oFA. (2) The oFA encrypts two session keys, S_{MN-FA} and S_{FA-HA} with a nFA's public key and then sends

it to the MN. (3) The MN creates $M1$(RREQ in ID-based) and its signature $<M1>S_{mn@}$, and sends them along with $\{S_{FA-MN}, S_{FA-HA}\}_{nFA@}$. (4) The nFA authenticates the $M1$ by verifying the $<M1>S_{mn@}$ based on the MN's ID and gets required session keys by decrypting based on its private key. (5) The nFA sends the $M1$ to AAAH. (6) The AAAH sends the $M1$ to HA. (7) The HA confirms a validity of the MN, registers the new CoA, and creates the encrypted $M3$ with a session key between the oFA and the HA. (8) The HA sends the $M3$ to AAAH. (9) The AAAH sends the $M3$ to nFA. (10) At this point, the nFA confirms the $M3$ that means the nFA has right session keys. Hence the nFA verifies the oFA which sends these session keys and also the oFA can verify the nFA which decrypts the encrypted message based on the nFA's ID.

4 Performance Evaluation

The values for the system parameters are directly from previous works, especially from [3] and [5]. And the time for Data Encryption Standard(DES), Message Digest 5(MD5), and Rivest-Shamir-Adlman(RSA) encryption and decryption is obtained from [10]. We compute the registration time with system parameters in Table 2. On the basic AAA procedure, the time for $RREQ_{MN-nFA}$ is computed based on the following simple estimation: 0.5 ms (MN processing time)+2 ms (propagation time in wireless links)+4.096 ms (message transmission time in wireless links)+0.088 ms (DES encryption and decryption)+0.0096 ms (MD5 operation)= 6.69 ms. The registration message size is assumed to 1024 bytes due to the RSA1024 operation [10]. Hence the message transmission time is obtained by multiplying the bit rate in wireless links and the message size.

- Basic AAA Method [7]
  $RREQ_{MN-nFA} + AMR_{nFA-AAAH} + HAR_{AAAH-HA} + HAA_{HA-AAAH} + AMA_{AAAH-nFA} + RREP_{nFA-MN} = 18.10\ ms$

- ID-based Method [4]
  $[M1, <M1>S_{MN@}, Auth.]_{MN-nFA}+$
  $[M1, <M1>S_{MN@}, Auth.]_{nFA-AAAH}+[M1, Registration]_{AAAH-HA}+$
  $[\{S_{MN-FA}, S_{MN-HA}\}_{mn@}, M2, <M2>S_{ha@}]_{HA-AAAH}+$
  $[\{S_{MN-FA}, S_{MN-HA}\}_{mn@}, <M3>_{aaah@}, M2, <M2>S_{ha@}, Auth.]_{AAAH-nFA}+$
  $[\{S_{MN-FA}, S_{MN-HA}\}_{mn@}, M2, <M2>S_{ha@}, Auth.]_{nFA-MN} = 37.62\ ms$

- Proposed Method
  $[\{S_{MN-FA}, S_{FA-HA}\}_{nFA@}]_{oFA-MN}+$
  $[M1, <M1>S_{MN@}, \{S_{MN-FA}, S_{FA-HA}\}_{nFA@}, Authen.]_{MN-nFA}+$
  $M1_{nFA-AAAH}+[M1, Registration]_{AAAH-HA}+$
  $[M3, Auth.]_{AAAH-nFA} = 23.12\ ms$

When we compare our proposed method to AAA with previous ID-based one [4], the registration time of the proposed one is reduced because the former uses the mutual authentication between the oFA and the nFA instead of the

Table 2. System parameters

Bit rates		**Processing time**	
Wire links	100 *Mbps*	Routers (HA,FA)	0.50 *ms*
Wireless links	2 *Mbps*	Nodes (MN)	0.50 *ms*
Propagation time		DES/MD5	0.044 *ms*/0.0048 *ms*
Wire links	500 μs	Signature creation	4.65 *ms*
Wireless links	2 *ms*	Signature verification	0.19 *ms*
Data size		RSA1024 encryption	0.18 *ms*
Message size	1024 *bytes*	RSA1024 decryption	4.63 *ms*

authentication between the MN and the HA. In the mutual authentication between the oFA and the nFA, session keys are delivered to the nFA from the oFA securely and therefore there is no need for the authentication at every related entity. Also the performance comparison shows that the proposed method takes a little bit more time than [7] because of using the public key cryptography, however it means the improved security level. The registration time required for the proposed method has drastically decreased compared to [4].

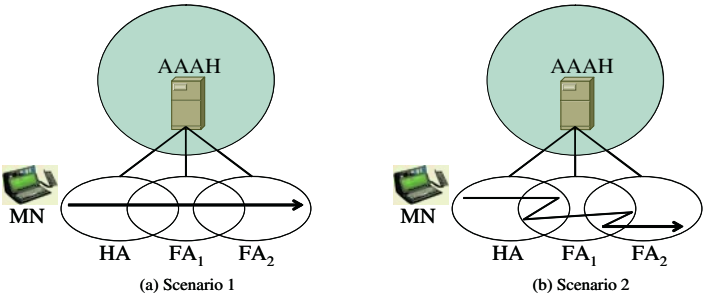


Fig. 3. Virtual network topology

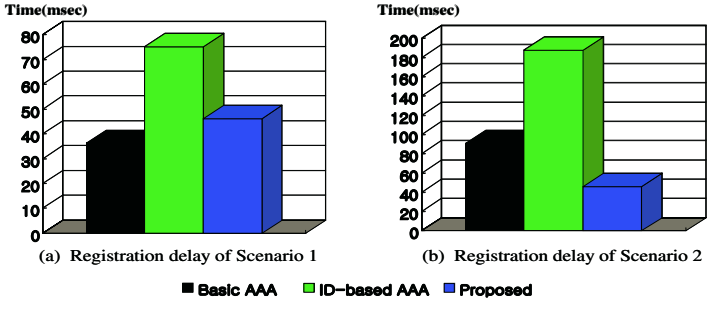


Fig. 4. Registration delays for three methods

As shown in Fig. 3, we have configured a simple virtual network topology for the comparison of various methods. In Fig. 3(a), suppose that an MN moves

directly from HA to FA_2. At this process, the MN performs handoff when it moves to a new area. Fig. 3(b) shows another scenario in the same virtual network topology. We assume that the MN moves zigzag within the overlapped area between adjacent cells in scenario 2. Fig. 4 shows the results. Fig. 4(a) represents a bar graph that shows the delay for the first scenario of the virtual network topology and Fig. 5(b) represents that of the second one. As you see in Fig. 4(a), our proposed scheme shows better performance than the ID-based scheme [4] even though it shows less performance than the basic AAA scheme [7]. And as you see in Fig. 4(b), our proposed scheme shows much better performance than previous two schemes. Even though the connection between the oFA and the MN is completely destroyed while performing the handoff, the proposed scheme shows the better performance since the oFA and the nFA share same session keys for the communication with the MN. Therefore MNs with high mobility patterns in overlapped areas, they do not need frequent authentication steps.

5 Conclusion

In this paper, we have proposed the session key reuse mechanism with ID-based cryptography. Based on the public key cryptography, this mechanism guarantees a higher level of security than the basic AAA mechanism [7] and has reduced registration time comparing to the AAA with the ID-based mechanism [4]. The result of the performance comparison also shows that the proposed mechanism is superior to AAA with the ID-based one [4] in terms of delay up to about 63% in the registration process. But due to heavy operations of public key cryptography, it takes a little bit more time than the basic AAA method. However, by minimizing the procedures which perform the public key cryptography, we can reduce the delay of the registration comparing to [7] while maintaining the similar level of security.

References

1. C. Boyd, "Modern data encryption," Electronic and Communication Engineering Journal, pp. 271–278, October 1993.
2. S. Glass, T. Hiller, S. Jacobs, and C. Perkins, "Mobile IP Authentication, Authorization, and Accounting Requirements," RFC2977, 2000.
3. A. Hess and G. Shafer, "Performance Evaluation of AAA/Mobile IP Authentication," Proceedings of 2nd Polish-German Teletraffic Symposium (PGTS'02), Gdansk, Poland, September 2002.
4. B.-G. Lee, D.-H Choi, H.-G. Kim, S.-W. Sohn, and K.-H. Park, "Mobile IP and WLAN with AAA authentication protocol using identity based cryptography," ICT2003 Proceedings, vol.3, pp. 597–603, February 2003.
5. J. McNair, I.F. Akyldiz, and M.D. Bender, "An inter-system handoff technique for the IMT–2000 system," INFOCOM 2000, vol. 1, pp. 203–216, March 2000.
6. C.E. Perkins, "IP Mobility Support," IETF RFC2002, October 1996.
7. C.E. Perkins, "Mobile IP and Security Issue: an Overview," Proceedings of 1st IEEE Workshop on Internet Technologies and Services, 1999.

8. A. Shamir, "Identity-based cryptosystems and signature schemes," Proceedings of Crypto '84, Springer-Verlag LNCS, vol. 196, pp. 46–53, 1985.
9. J. Vollbrecht, P. Cahoun, S. Farrell, and L. Gommans, "AAA Authorization Application Examples," RFC 2104, February 1997.
10. Wei Dai, "http://www.eskimo.com/weidai/benchmarks.html," Last modified: 13^{th} July 2003.