A framework of hybrid authentication for link access under MIH environments

Kangsuk Chae, Jiman Mun, Souhwan Jung
(*School of Electronic Engineering, Soongsil University, Seoul 156-743, Korea*)

Abstract: A unified hybrid authentication framework was proposed to provide proactive authentication and re-authentication for media independent handover(MIH)-based multi-wireless access. In addition, a specific protocol distributing a hierarchical key after the proactive authentication from key holder to base station has been proposed. The proposed hybrid authentication framework not only performs proactive authentication with credentials based on Chameleon hashing, which removes the authentication procedures that exchanges messages with a authentication server, but also performs re-authentication with EAP re-authentication protocol(ERP) that distributes the hierarchical key on the basis of the root key generated by the proactive authentication.

Key words: hybrid authentication; vertical handover; media independent handover(MIH); chameleon hashing; extensible authentication protocol(EAP); EAP re-authentication protocol(ERP)

CLD number: TN926 **Document code**: A
Article ID: 1674-8042(2012)04-0362-08 **doi**: 10.3969/j.issn.1674-8042.2012.04.013

0 Introduction

Recently, as mobile communications rapidly grow, demands for high-speed data service supporting mobility are increasing. Responding to such demands, a number of studies have focused on providing seamless mobility service during handover among heterogeneous wireless networks. In particular, IEEE formed the 802.21 working group(WG) in March, 2004, to begin the standardization of the technology that provides independent handover among heterogeneous wireless networks. The IEEE 802.21 media independent handover(MIH) standard[1] supports media-independent handover of the mobile nodes(MNs) that have two or more link access interfaces. The media independent handover function(MIHF), one of the components for the MIH service, supports the media-independent handover among heterogeneous networks by providing three major services such as media independent event service(MIES), media independent command service(MICS), and media independent information service(MIIS).

On the other hand, the IEEE 802.21 security group has been working on standardizing the proactive authentication scheme for handover in MIH and the protocol to protect the messages exchanged among the MIH nodes by transport layer security (TLS)[2]. The MIH protocol for proactive authentication scheme standardized by the IEEE 802.21 security group belongs to a family of the extensible authentication protocol (EAP)-based authentication protocols, which includes EAP-TLS[3-4], EAP-Kerberos Ⅱ[5], and EAP re-authentication protocol (ERP)[6-7], etc. Though the IEEE 802.21 security group standardized only the EAP-based scheme for proactive authentication, the public key infrastructure(PKI)-based scheme[8] might also be used for proactive authentication in the MIH environment. The EAP or PKI-based authentications causes latency problems during frequent handovers because the authentication procedure has to go through authentication, authorization and accounting(AAA) servers far away in general. In addition, even though IEEE 802.21 security group introduces the proactive authentication scheme for handover, the specific protocol that distributes the hierarchical key after the proactive authentication from the key holder to the point of attachment(PoA) has not been standardized.

In this paper, a hybrid authentication framework was proposed, which combines the MIH proactive authentication scheme based on the chameleon hashing[9] and the hierarchical key distribution scheme using ERP[6] based on the shared root key generated

* **Received data**: 2012-08-14
Foundation item: The KCC(Korea Communications Commission), Korea, under the R&D program supervised by the KCA(Korea Communications Agency) (KCA-2012-08-911-05-001)
Corresponding author: Souhwan Jung (souhwanj@ssu.ac.kr)

by the proactive authentication. The proactive authentication in the proposed authentication framework uses the Chameleon hashing-based credential that provides the authentication of the DH (Diffie-Hellman) public key which generates a credential at every handover[9]. It means that the proactive authentication is carried out only between the MN and the MIH key holder without going through the AAA server, since the Chameleon hashing-based credentials work it out. The root key shared by proactive authentication before handover is used as the re-authentication root key(rRK) to perform ERP when the MN attaches to a new network. The MN moved to a new network performs ERP with key holder for access authentication and shares the hierarchical key with the network to protect the relevant wireless channel[6-7]. The proposed hybrid authentication framework reduces latency caused by the authentication procedures with AAA servers since the DH key exchange is executed via the Chameleon hashing-based credential, and also provides improved security services such as perfect forward secrecy(PFS) and perfect backward secrecy(PBS). In addition, the hierarchical keys are distributed from key holder to PoA using ERP when MN gets access to the link.

This paper consists of the following sections. Section 1 describes the related works to the framework proposed in this paper. The operation of the proposed framework is explained in section 2. In section 3, the efficiency of the proposed framework and the security aspects of the applied scheme are analyzed. Concluding remarks are made in section 4.

1 Related work

1.1 Positioning

Fig. 1 shows indirect proactive authentication model in MIH architecture. IEEE 802.21 security group recommends the model performing EAP proactive authentication for handover under MIH environment[2]. Two different proactive authentication models that are direct and indirect were introduced. The direct model is to deliver the message directly to the candidate point of service(PoS) by using higher-layer communication, while the indirect model is to forward the MIH message through the serving PoS. Fig. 1 shows the indirect proactive authentication model. The network elements for the proactive authentication include media specific authenticator and key holder(MSA-KH) and media independent authenticator and key holder(MIA-KH). The MN executes the EAP-based MIH proactive authentication with the candidate network(CN) MIA-KH.

A number of authentication schemes can be applied to the MIH proactive authentication, though IEEE 802.21 security group considers only EAP-based proactive authentication schemes. In this paper, we assume that EAP-based authentication messages as well as the other authentication messages can perform the MIH proactive authentication protocol. We will review not only the existing EAP-based authentication schemes[3-7], but also the PKI-based pre-authentication scheme[8] that can be executed without connecting to AAA server in order to evaluate the efficiency of our scheme.

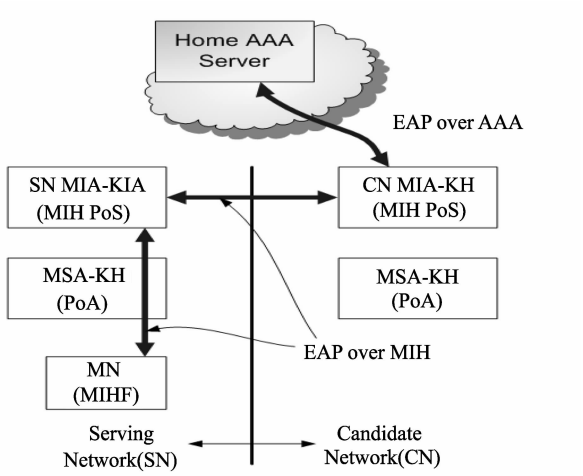

Fig. 1 Indirect proactive authentication model in MIH architecture

1.1.1 EAP-based authentication schemes

EAP-TLS is a sort of authentication schemes used in IEEE 802.11i technology where mutual authentication is carried out between MN and AAA server using PKI-based certificate[4]. The MN and AAA server go through mutual authentication by including TLS messages in EAP protocol, and following certificate-based TLS procedures. Once MN authentication is successful, AAA server sends a generated master key with the AUTHENTICATION SUCCESS message to access point(AP). Then, MN and AP perform 4-way handshake procedure with the shared master key and generate a key for the protection of relevant data in wireless area. However, authentication procedure is complicate, and authentication is delayed since EAP-TLS performs TLS procedure with the AAA server. Furthermore, it gets more complicated for distributing and managing certificates securely since PKI-based certificates are used.

Eun et al. proposed EAP-Kerberos II scheme for reducing latency caused by complicated authentication procedure of EAP-TLS[5]. In the scheme, private keys are shared between MN and AAA server and also between AP and AAA server. Then AAA server generate a ticket and send it to MN in order to carry out mutual authentication fast between MN

and target network. However, the latency problem still remains in the scheme because authentication is performed with AAA server whenever it works.

ERP is a sort of re-authentication schemes, which uses hierarchical key structure to reduce frequent authentication procedure with home AAA server so that authentication is carried out fast[6-7]. After initial authentication with a home AAA server located at home domain, home AAA server sends a hierarchical key to a local re-authentication server administrating local domain. Later, MN directly executes authentication with a local re-authentication server without connecting to the home AAA server if handover occurs within the local re-authentication server domain. However, ERP should be executed with home AAA server if domain is changed during handover.

1.1.2 PKI-based pre-authentication scheme

Fig. 2 shows message flows for initial and proactive authentications Sun et al. proposed a pre-authentication scheme performed between MN and handover target network, of which procedure worked without AAA server[8]. In the scheme, MN performs authentication based on certificate with authenticator of the handover target network before handover. A certificate used here is the certificate of MN and authenticator of the handover target network, and there is no work with AAA server. The whole procedure is so simplified that network latency is reduced as well. However, it still has overhead such as distribution and management of the certificates due to using PKI.

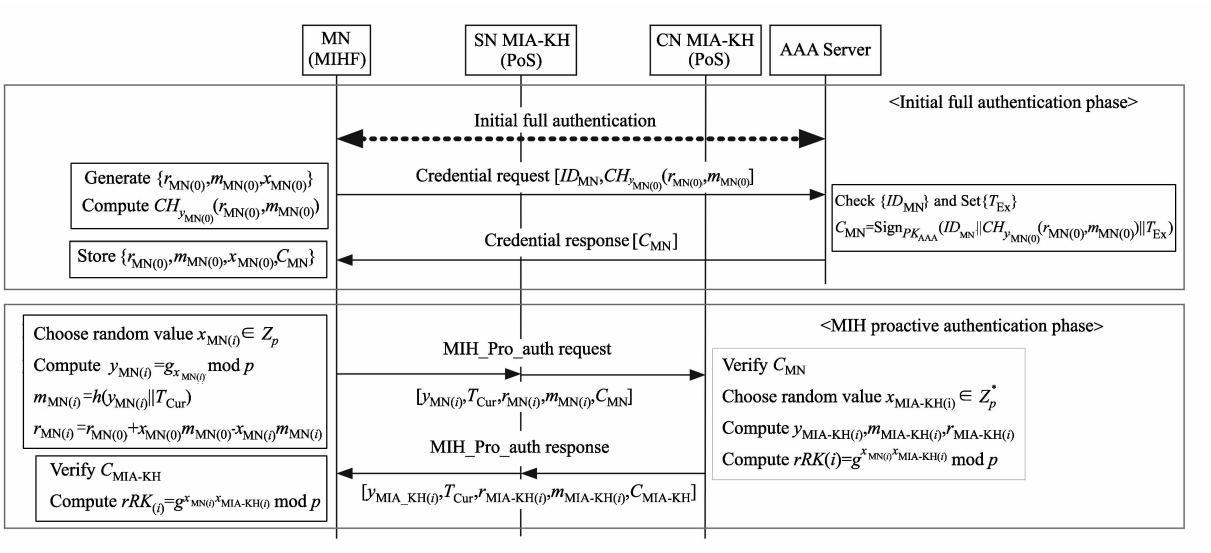

Fig. 2 Message flows for initial and proactive authentications

1.2 Other problem of MIH security

Although IEEE 802.21 security group suggested a simple framework where the hierarchical key is generated and distributed from CN MIA-KH to CN MSA-KH following mutual authentication between MN and CN MIA-KH and the generation of the shared key, the protocol has not been standardized for distributing the hierarchical key from CN MIA-KH to CN MSA-KH. Actually, the methods for distribution of the hierarchical key are being discussed in recent standardization process.

1.3 Chameleon hashing

Krawczyk et al. defined a special trapdoor hashing function via a Chameleon hashing function[10]. Chameleon hashing value is computed through 2 variables such as message and collision value with Chameleon hashing public key. The Chameleon hashing value computed always has the same result even if the new message comes up. The collision value for the new messages is able to be computed via Chameleon hashing private key. Therefore, the user who knows Chameleon hashing private key can only get the collision value. The good point of this scheme is that the signature of message can be done before sending message. One problem of Chameleon hashing is that if the same Chameleon hashing value is used constantly, Chameleon hashing private key could be disclosed. To solve this problem, our scheme takes DH private key which is newly generated every time as Chameleon hashing private key, so that Chameleon hashing value initially generated can be kept being used for authentication.

2 Hybrid authentication framework

This paper proposes a hybrid authentication framework combining the proactive authentication

scheme using Chameleon hashing-based credential[9] under MIH environment and the ERP[6] for rapid re-authentication and hierarchical key distribution. The proposed framework includes authenticated DH key exchange and authentication scheme[11-12] through a Chameleon hashing to perform proactive authentication under MIH environment, and enable rapid re-authentication, hierarchical key distribution via ERP after handover. The proactive authentication in our proposed framework is operated by using the MIH message standardized by IEEE 802.21 security group[2].

The proposed protocol consists of three steps: the initial authentication and credential distribution step, the MIH proactive authentication step and the handover re-authentication & key distribution step. The protocol notations used are listed in Table 1.

Table 1 Notations

Notation	Definition
ID_{Node}	Node identifier, identity information
$PK^{-}_{\text{Node}}/PK^{+}_{\text{Node}}$	RSA private key / public key of Node
C_{Node}	Credential of Node
T_{Ex}	Expiration time of credential
T_{Cur}	Message generation time / Current time
$x_{\text{Node}(i)}/y_{\text{Node}(i)}$	Node Diffie-Hellman private key / public key, also used as chameleon hashing private key / public key
$r_{\text{Node}(i)}$	Collision, $r_{\text{Node}(0)}$ is a random private value
$m_{\text{Node}(i)}$	Hashing message of public key, $m_{\text{Node}(0)}$ is a random private value
$h(\cdot)$	One-way hashing function (e.g. SHA-1, SHA-256, MD5, ···)
$CH_y(r,m)$	Chameleon hashing function, $CH_y(r,m) = g^r g^{xm} \bmod p$

2.1 Initial authentication and credential distribution step

Fig. 2 shows the flow chart of the initial authentication and credential distribution step, and the MIH proactive authentication step protocol.

As MN initially accesses the wireless network, initial bootstrapping authentication is carried out by the AAA server using EAP-TLS. After the initial authentication is completed and a secured channel is formed between the MN and AAA server, the MN proceeds to receive the allocated credential from AAA server.

The MN chooses random private values $r_{\text{MN}}(0)$, $m_{\text{MN}(0)}$ and $x_{\text{MN}(0)}$. Then, Chameleon hashing is computed using Eq. (1). The credential request message including the computed Chameleon hashing value and identity of the MN is transmitted to the AAA server through the secured channel

$$y_{\text{MN}(0)} = g^{x_{\text{MN}(0)}} \bmod p,$$

$$CH_{y_{\text{MN}(0)}}(r_{\text{MN}(0)}, m_{\text{MN}(0)}) = g^{r_{\text{MN}(0)}} g^{x_{\text{MN}(0)} m_{\text{MN}(0)}} \bmod p. \quad (1)$$

The AAA server that has received the credential request message from the MN checks the MN's identity and determines a credential expiration time according to billing policy. Then, the AAA server generates a MN's credential C_{MN} signing ID_{MN}, $CH_{y_{\text{MN}(0)}}(r_{\text{MN}(0)}, m_{\text{MN}(0)})$ and T_{Ex} that are included in the credential generated by using its RSA private key PK^{-}_{AAA} as in Eq. (2). The MN's credential C_{MN} generated in this way is transmitted to the MN through the credential response message.

$$C_{\text{MN}} = \text{sign}_{PK^{-}_{\text{AAA}}}(ID_{\text{MN}} \parallel CH_{y_{\text{MN}(0)}} \cdot (r_{\text{MN}(0)}, m_{\text{MN}(0)}) \parallel T_{\text{Ex}}). \quad (2)$$

2.2 MIH proactive authentication step

When handover to a new wireless network occurs, the MN selects a handover candidate network through the MIH protocol and reserves resources. Since the MN can determine a handover candidate network through this procedure, authentication and key exchange can be done before handover using the MIH proactive authentication protocol.

The MN generates information for authentication and key exchange. Firstly, new DH private key $x_{\text{MN}(i)}$ and public key $y_{\text{MN}(i)} = g^{x_{\text{MN}(i)}} \bmod p$ are generated by the MN. The DH public key generated here serves as Chameleon hashing public key for message authentication. Then, to protect against replay attack, the MN generates a one-way hashing value $m_{\text{MN}(i)}$ with message generation time and DH public key T_{Cur}. Besides, the MN also computes a collision value $r_{\text{MN}(i)}$ using the initial random private values $r_{\text{MN}(0)}$, $m_{\text{MN}(0)}$, $x_{\text{MN}(0)}$, the newly generated $x_{\text{MN}(i)}$ and $m_{\text{MN}(i)}$ as in Eq. (3). This collision value $r_{\text{MN}(i)}$ can only be generated by a person who knows the initial random values and the newly generated DH private key.

$$m_{\text{MN}(i)} = h(y_{\text{MN}(i)} \parallel T_{\text{Cur}}),$$
$$r_{\text{MN}(i)} = r_{\text{MN}(0)} + x_{\text{MN}(0)} m_{\text{MN}(0)} - x_{\text{MN}(i)} m_{\text{MN}(i)}. \quad (3)$$

The MN transmits MIH_Pro_auth Request message that is the MIH proactive authentication request message, including the generated information $y_{\text{MN}(i)}$, T_{Cur}, $r_{\text{MN}(i)}$ and $m_{\text{MN}(i)}$ for authentication and key exchange, and also sends the credential C_{MN} to the CN MIA-KH. Depending on the type of models.

Proposed by the IEEE 802.21 security group, the MIH proactive authentication request message can be either directly transmitted to the CN MIA-KH or

indirectly transmitted through the serving network (SN) MIA-KH.

The CN MIA-KH that has received MIH proactive authentication request message from the MN computes a Chameleon hashing value, which takes $y_{MN(i)}$, $r_{MN(i)}$ and $m_{MN(i)}$ included in the message. By comparing this value with the Chameleon hashing value included in the credential and verifying whether they are the same or not, the MN is authenticated. Firstly, to check replay attack, it is examined whether a one-way hashing value for the DH public key $y_{MN(i)}$ of the MN and for the message generation time T_{cur} are the same as $m_{MN(i)}$ or not, as shown in Eq. (4)

$$m_{MN(i)} = h(y_{MN(i)} \| T_{Cur}). \tag{4}$$

Then, the MIA-KH computes the Chameleon hashing value $CH_{y_{MN(i)}}(r_{MN(i)}, m_{MN(i)})$ using information $y_{MN(i)}$, $r_{MN(i)}$, and $m_{MN(i)}$ included in the received message as Eq. (5), and compares it with $CH_{y_{MN(0)}}(r_{MN(0)}, m_{MN(0)})$ that has been obtained by verifying the credential C_{MN} with the RSA public key of AAA server PK^{+}_{AAA} to check if they are the same, as in Eq. (6). The MN is authenticated when those values are the same, as in Eq. (7).

$$CH_{y_{MN(i)}}(r_{MN(i)}, m_{MN(i)}) = g^{r_{MN(i)}} g^{x_{MN(i)} m_{MN(i)}} \bmod p, \tag{5}$$

$$\text{Verify}_{PK^{+}_{AAA}}(C_{MN}) \equiv (ID_{MN} \| CH_{y_{MN(0)}}(r_{MN(0)}, m_{MN(0)}) \| T_{Ex}), \tag{6}$$

$$CH_{y_{MN(i)}}(r_{MN(i)}, m_{MN(i)}) = CH_{y_{MN(0)}}(r_{MN(0)}, m_{MN(0)}). \tag{7}$$

If only $y_{MN(i)}$, T_{Cur}, $r_{MN(i)}$ and $m_{MN(i)}$ have been generated by a legal MN, it can be examined that the computed Chameleon hashing value $CH_{y_{MN(i)}}(r_{MN(i)}, m_{MN(i)})$ is the same as the Chameleon hashing value $CH_{y_{MN(0)}}(r_{MN(0)}, m_{MN(0)})$ included in the credential by

$$CH_{y_{MN(i)}}(r_{MN(i)}, m_{MN(i)}) = g^{r_{MN(i)}} g^{x_{MN(i)} m_{MN(i)}} \bmod p = g^{r_{MN(0)} + x_{MN(0)} m_{MN(0)} - x_{MN(i)} m_{MN(i)}} g^{x_{MN(i)} m_{MN(i)}} \bmod p = g^{r_{MN(0)}} g^{x_{MN(0)} m_{MN(0)}} \bmod p = CH_{y_{MN(0)}}(r_{MN(0)}, m_{MN(0)}). \tag{8}$$

After authenticating the MN and obtaining DH public key of the MN, CN MIA-KH generates its own DH private key and public key $y_{MIA\text{-}KH(i)} = g^{x_{MIA\text{-}KH(i)}} \bmod p$. Then, CN MIA-KH generates information for authentication in the same manner of the MN. CN MIA-KH transmits MIH _ Pro _ auth Response message which is MIH proactive authentication response message including $y_{MIA\text{-}KH(i)}$, T_{Cur}, $r_{MIA\text{-}KH(i)}$ and $m_{MIA\text{-}KH(i)}$ generated in this manner and its own credential $C_{MIA\text{-}KH}$, to the MN. The MN that has received the response message authenticates the DH public key of the CN MIA-KH in the same manner described above.

As the MN and CN MIA-KH performs mutual authentication in this way, they now share the identical re-authentication root key $rRK_{(i)}$ through the DH algorithm, as shown in Eq. (9). The re-authentication root key shared in this way is used to rapidly re-authenticate using ERP when MN is attached to a new network.

$$rRK_{MN(i)} = (g^{x_{MIA\text{-}KH(i)}} \bmod p)^{x_{MN(i)}} \bmod p,$$

$$rRK_{MN(i)} = (g^{x_{MN(i)}} \bmod p)^{x_{MIA\text{-}KH(i)}} \bmod p,$$

$$rRK_{(i)} = rRK_{MN(i)} = rRK_{MIA\text{-}KH(i)} = g^{x_{MN(i)} x_{MIA\text{-}KH(i)}} \bmod p. \tag{9}$$

2.3 Prompt handover re-authentication and key distribution step

When the MN is attached to a new network, re-authentication is executed fast by the ERP procedure based on the re-authentication root key $rRK_{(i)}$ shared through the CN MIA-KH and MIH proactive authentication procedure. It also shares the hierarchical key $rMSK_{(i)(j)}$ for generating the protection key of the relevant wireless area with the new PoA, CN MSA-KH. In addition, when the handover occurs between the MSA-KHs in a network that is administrated by the same MIA-KH, re-authentication can be done fast using the ERP procedure based on the re-authentication root key $rRK_{(i)}$ shared between the MN and the MIA-KH. Fig. 3 shows the flow chart of the protocol.

The MN and the MIA-KH derive the re-authentication integrity key $rIK_{(i)}$ from the shared re-authentication root key $rRK_{(i)}$, as in Eq. (10). Here, rIK Label is an 8-bit ASCII string.

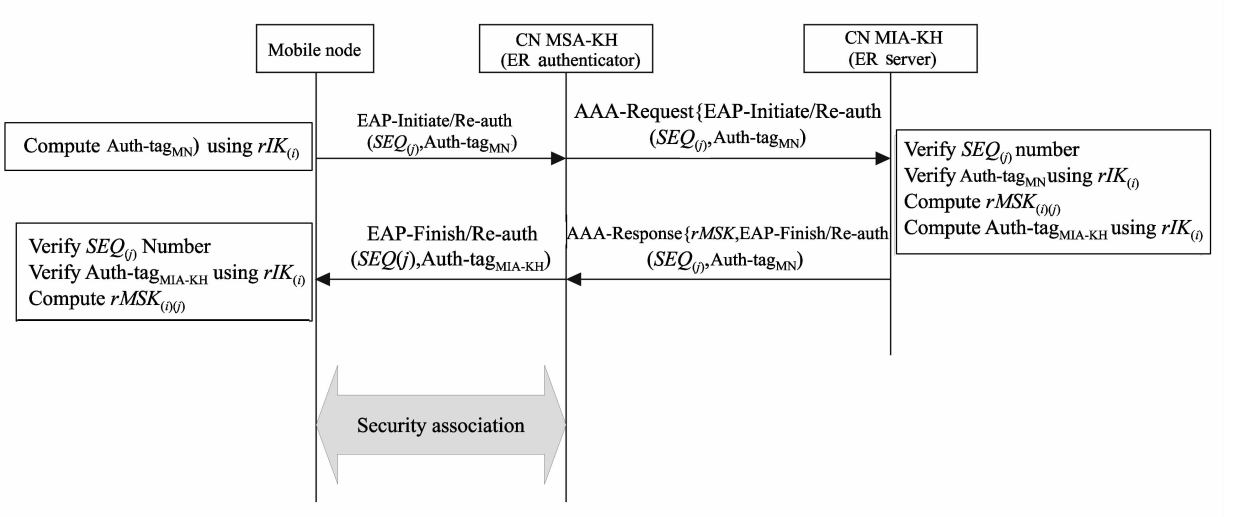

Fig. 3 Handover re-authentication and key distribution protocol using ERP

$$rIK_{(i)} = KDF(rRK_{(i)}, rIK\ Label \mid LULLoctet, \mid crypto\ suite \mid length). \quad (10)$$

The EAP-Initiate/Re-auth message that includes the sequence number $SEQ_{(j)}$ and the authentication tag Auth-tag$_{MN}$ is transmitted to MIA-KH by MN. The 16-bit sequence number $SEQ_{(j)}$ is used to protect against replay attack. Auth-tag$_{MN}$ which is generated by the re-authentication integrity key $rIK_{(i)}$ is used to provide message integrity and authentication. After MIA-KH receives the EAP-Initiate/Re-auth message, it will check the sequence number $SEQ_{(j)}$ and verify the authentication tag Auth-tag$_{MN}$ with the re-authentication integrity key $rIK_{(i)}$. If the authentication is successful, MIA-KH will derive the hierarchical key $rMSK_{(i)(j)}$ from the shared re-authentication root key $rRK_{(i)}$, as in Eq. (11). Here, *rMSK Label* is an 8-bit ASCII string.

$$rMSK_{(i)(j)} = KDF(rRK_{(i)}, rMSK\ Label \mid LULLoctet \mid SEQ \mid length). \quad (11)$$

MIA-KH transmits the EAP-Finish/Re-aut message including the sequence number $SEQ_{(j)}$ and the message authentication tag to the MN. In this procedure, the hierarchical key $rMSK_{(i)(j)}$ is distributed to the PoA from the MIA-KH. The MN that has received the message authenticates the MIA-KH by certificating the message authentication tag Auth-tag$_{MIA-KH}$ and generates the identical hierarchical key $rMSK_{(i)(j)}$ in the same manner in Eq. (11). Then, the association process for wireless area key security is performed using the shared hierarchical key $RMSK_{(i)(j)}$ between the MN and PoA.

3 Discussion

The Chameleon hashing-based proactive authentication scheme used in our handover authentication framework can not only reduce the authentication delay with the AAA server, but also removes the necessity of the PKI environment, since it uses the authenticated DH public key newly generated every time using the credential allocated just once. Therefore, the proposed framework has the effect of reducing the network latency and the communication overhead compared to the existing schemes. Moreover, the proposed framework provides a solution for the problem of the hierarchical key distribution occurred after pre-authentication from MIA-KH to MSA-KH. It also provides the handover authentication and hierarchical key distribution procedures between the MSA-KHs in the network administrated by the same MIA-KH.

In this section, analytic discussion is carried out on the network efficiency and the security strength of the proactive authentication scheme of the proposed framework.

In addition, we discuss the security in terms of the key escrow and revocation problems, and describe how the proposed scheme satisfies the security requirements

3.1 Analysis of efficiency

In this section, to discuss the efficiency of each scheme with regards to network latency, the total communication cost was calculated by the whole communication costs of each relevant network area for transmitting the authentication message, and the total communication costs of each scheme was compared. For the comparison, it is assumed that the authentication schemes perform the proactive authe-

ntication between the MN and the MIA-KH of the handover candidate network under the MIH environment. The cost of transmitting messages between the MN and the serving network (SN), between the serving network and the handover candidate network (CN), and between the handover candidate network and the AAA server are denoted as $T_{\text{MN-SN}}$, $T_{\text{SN-CN}}$ and $T_{\text{CN-AAA}}$ respectively.

Eq. (12) shows how the total communication cost of all the messages for each authentication schemes is calculated.

$$T_{\text{Total}} = T_{\text{MN-SN}} + T_{\text{SN-CN}} + T_{\text{CN-AAA}}. \tag{12}$$

We set the communication costs in each interval for unit authentication message $T_{\text{MN-XN}}$, $T_{\text{SN-CN}}$, and $T_{\text{CN-AAA}}$ as to be α, β and γ respectively, the total communication costs of the individual authentication method for all the proactive authentication messages, T_{Total} are listed in Table 2. It is verified from Table 2 that the communication cost of the proposed scheme is less than the conventional methods.

Table 2 Comparison of communication costs

	EAP-TLS	EAP-Kerberos	ERP	PKI based	Proposed scheme
$T_{\text{MN-SN}}$	10α	7α	2α	3α	2α
$T_{\text{SN-CN}}$	10β	7β	2β	2β	2β
$T_{\text{CN-AAA}}$	8γ	2γ	2γ	–	–
T_{Total}	$10\alpha+10\beta+8\gamma$	$7\alpha+7\beta+2\gamma$	$2\alpha+2\beta+2\gamma$	$3\alpha+2\beta$	$2\alpha+2\beta$

3.2 Analysis of security strength

3.2.1 Guessing attack for the Chameleon hashing private key

If message authentications are repeatedly carried out with the same Chameleon hashing value initially generated, then an guessing attack for the Chameleon private key is possible through the collected messages since the existing Chameleon hashing function uses the same Chameleon hashing private key. As shown in the process in Eq. (13), after calculating the Chameleon hashing value $CH_y(r_{(1)}, m_{(1)})$ through $r_{(1)}, m_{(1)}$, and the Chameleon public key y included in the first message and the one $CH_y(r_{(2)}, m_{(2)})$ through $r_{(2)}, m_{(2)}$ and the Chameleon public key y included in the second message, an attacker can guess the Chameleon hashing private key x from two identical hashing values.

$$CH_y(r_{(1)}, m_{(1)}) = CH_y(r_{(2)}, m_{(2)}) \Rightarrow \begin{cases} CH_y(r_{(1)}, m_{(1)}) = g^{r_{(1)}} g^{xm_{(1)}} \bmod p \\ CH_y(r_{(2)}, m_{(2)}) = g^{r_{(2)}} g^{xm_{(2)}} \bmod p \end{cases} \Rightarrow$$
$$r_{(1)} + m_{(1)}x = r_{(2)}m_{(2)}x \Rightarrow x = \frac{r_{(2)} - r_{(1)}}{m_{(1)} - m_{(2)}}. \tag{13}$$

Since the proposed scheme takes the DH private keys newly generated each time as Chameleon hashing private key is generated, the private key guessing attack does not work. On the other hand, our scheme has two variables $x_{(1)}$ and $x_{(2)}$ that are so-called simultaneous linear equation problem, shown in Eq. (14). Thus, the Chameleon hashing private key is hard to guess.

$$CH_{y(1)}(r_{(1)}, m_{(1)}) = CH_{y(2)}(r_{(2)}, m_{(2)}) \Rightarrow \begin{cases} CH_{y(1)}(r_{(1)}, m_{(1)}) = g^{r_{(1)}} g^{x_{(1)}m_{(1)}} \bmod p \\ CH_{y(2)}(r_{(2)}, m_{(2)}) = g^{r_{(2)}} g^{x_{(2)}m_{(2)}} \bmod p \end{cases} \Rightarrow$$
$$r_{(1)} + m_{(1)}x_{(1)} = r_{(2)}m_{(2)}x_{(2)}. \tag{14}$$

In addition, because the chameleon hashing and the DH public key are generated by the discrete exponentiation of the private key, guessing the private key from the public key is very hard as it is a general discrete logarithm problem. Therefore, the proposed scheme is secure against the private key guessing attack.

3.2.2 Provision of PFS/PBS

In the proposed scheme, the transmitter sends the authentication message including the valid collision value $r_{(i)}$, hashing value $m_{(i)}$, and DH public key $y_{(i)}$ newly generated each time after calculating them, while the receiver compares the Chameleon hashing value $CH_{y(i)}(r_{(i)}, m_{(i)})$ with the signed Chameleon hashing value $CH_{y(0)}(r_{(0)}, m_{(0)})$ included in the credential to verify and authenticate DH public key . The proposed scheme provides a perfect forward and backward secrecy. Even though the master key which is used in the previous step is exposed, the communication contents before and after the exposure are still secured since an arbitrary master key is newly generated at each time by exchang-

ing the authenticated DH key.

3.2.3 Man-in-the-middle attack

An attacker may attempt the man-in-the-middle attack which is the defect of the DH key exchange algorithm between the MN and the MIA-KH. However, the proposed scheme is secure from the man-in-the-middle attack because the authentication of the DH public key is provided by using the Chameleon hashing-based credential.

3.2.4 Impersonation attack

An attacker may attempt the authentication message generation for spoofing himself as an arbitrary user. However, for the generation of the valid collision value of the DH public key generated newly cannot be calculated since he/she does not know the initial private values, and for credential generation. Hence, the proposed scheme is secure against impersonation attack.

3.2.5 Replay attack

An attacker may attempt the replay attack that provides fake authentication by collecting and re-using the authentication messages of MN. However, the proposed scheme is secure against replay attack because the authentication message of the scheme includes $m_{(i)} = h(y_{(i)} \| T_{\mathrm{Cur}})$, the one-way hashing result value of the message generation time T_{Cur} and the DH public key $y_{(i)}$, as the authentication elements.

3.2.6 Solid identification

The credential is distributed to each node. The credential includes the following information of node ID / user ID, chameleon hashing value, and the expiration time, which are singed by AAA server. Each node authenticates each other using the credential. Since the credential includes the ID information of each node, and verifies the ID each other, our scheme provides a solid identification function.

4 Conclusion

In this paper, the framework for the handover authentication under MIH environment is proposed. In the existing handover authentication frameworks, network latency problem is caused due to the procedure with the AAA server during handover to a new network, and also the procedure for the hierarchical key distribution is not standardized yet. These problems are solved in the proposed hybrid framework as the authentication procedure with the AAA server is eliminated from the proactive authentication process by using the Chameleon hashing-based credential and the re-authentication, and the hierarchical key distribution procedure are rapidly performed by means of the ERP based on the root key shared through the proactive authentication. The proposed scheme for proactive authentication requires neither the authentication procedure with the AAA server nor the PKI-environment. The authentication is carried out using the Chameleon hashing-based credential, which allows the authentication of the DH public key generated each time. By performing the ERP procedure based on the root key shared by the proactive authentication during handover, the proposed framework provides mutual authentication between the MN and network. Therefore, it solves the hierarchical key distribution problem. In addition, the scheme applied to the proposed framework satisfies the basic security requirements as well as guarantees a strong security by providing PFS and PBS of the master key. Consequently, the proposed framework can be conveniently applied to the environment where PKI is hard to be established such as heterogeneous wireless networks. It also has the effect of reducing network latency. It provides a complete procedure for the handover authentication under MIH environment.

References

[1] IEEE Std 802.21-2008. Media independent handover services, January 2009.

[2] IEEE 802.21a, Proactive authentication and MIH security. [2012-07-10]. https://mentor.ieee.org/802.21/documents.

[3] Aboba B, Blunk L, Vollbrecht J, et al. Extensible authentication protocol (EAP), IETF RFC 3748, 2004.

[4] IEEE Std 802.11i-2004, Medium access control (MAC) security enhancements, 2004.

[5] Eum S, Choi H. EAP-Kerberos II: An adaptation of kerberos to EAP for mutual authentication. Proc. of ITST 2008, Phuket, Thailand, 2008.

[6] Narayanan V, Dondeti L. EAP extensions for EAP re-authentication protocol (ERP). IETF RFC 5296, 2008.

[7] Salowey J, Dondeti L, Narayanan V, et al. Specification for the drivation of root keys from an extended master session key (EMSK). IETF RFC 5295, 2008.

[8] Sun H, Lin Y, Chen S, Shen Y. Secure and fast handover scheme based on pre-authentication method for 802.16 / WiMAX infrastructure networks. Proc. of TENCON 2007, Taipei, Taiwan, 2007.

[9] Choi J, Jung S. A handover authentication using credentials based on chameleon hashing. IEEE Communications Letters, 2010, 14(1): 54-56.

[10] Krawczyk H, Rabin T. Chameleon signatures. Proc. of NDSS 2000, San Diego, California, USA, 2000: 143-154.

[11] Diffie W, Hellman M. New directions in cryptograhpy. IEEE Trans. on Information Theory, 1976, 22(6): 644-654.

[12] Rescorla E. Diffie-Hellman key agreement method. IETF RFC 2631, 1999.