A Secure Inter-Domain Handover Authentication Scheme for Wireless Network

Ren Junn Hwang
Department of Computer Science and Information Engineering
Tamkang University
junhwang@ms35.hinet.net

Sheng Hua Shiau
Department of Information Network Technology
Chihlee Institute of Technology
shshiau@mail.chihlee.edu.tw

Kuan Yu Chen
Department of Computer Science and Information Engineering
Tamkang University
696411726@s96.tku.edu.tw

***Abstract*—In wireless network environment, mobile user might perform the procedure of handover. According to the security requirements and convenience, taking mutual authentication and fast handover into account in the process of inter-domain handover is necessary. This paper proposes a secure inter-domain handover authentication scheme for wireless network that provides fast handover to retain the connectivity of network under the security requirement of identity authentication. It considers inter-domain handover to maintain the anonymity of user's identity, replay attack resistance and the forward/backward secrecy of key generation. These are what other studies haven't provided. Among these functionalities, we especially focus on the authentication latency shortened by fast handover. If the authentication latency takes too long, the network connectivity of the user may be affected. Moreover, it may cause disconnection. Our scheme reduces more handover authentication latency than other schemes do. The user may misunderstand that it is disconnected. It is more secure and efficient than other studies.**

***Index Terms*—Anonymity, fast handover, forward/ backward secrecy, inter-domain handover authentication.**

I. INTRODUCTION

Thank to the development of computer, communication, and electronic technologies, various wireless communication technologies are developing well and applied into our daily lives and social mechanisms. Different types of wireless communication are going into next generation to promote the quality of services and capabilities. Figure 1 represents a wireless network environment. There is a user with mobility (Mobile Station, MS). A Base Station (BS) is responsible for provision of wireless network services. A Domain AAA Server administrates the domain. An Access Service Network Gateway (ASN) in is assistance of Domain AAA Server. When the user would like to connect the wireless network, he will connect to the network via BS. Domain AAA Server controls and authorizes the user and deals with billing issues. ASN deals and manages status of users using the network. Besides, due to the mobility of users, the wireless network allows users movement from base station A to base station B when connected. At the moment, wireless network service provider changes from base station A to base station B. This action is called handover. If base stations A and B belong to

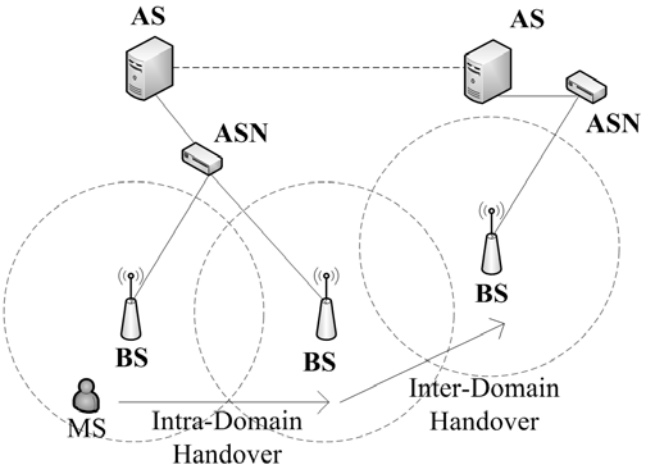

Figure 1. Network Model

the same Domain AAA Server, it is intra-domain handover. On the other hand, different Domain AAA Servers, it is called inter-domain handover. It needs no interruption of service and re-login, but B and user need to authenticate each other to keep the security.

Advantages of wireless network are low-cost infrastructure and user's mobility, but there are some issues. In researches related to wireless network, authentication is the base of network access security and also the most important issue. We can provide proper network services and quality of service to users with efficient and appropriate authentication. Authentication process of wireless network connectivity can be divided into two different issues of authentication:

1. Login authentication: Generally means the login into the domain and access to the network after boot. The information that the user provides can make mutual authentication between the mobile device and the base station. We must consider whether the user logs in either home domain that the user belongs to the Domain AAA Server of the base station or logs in foreign domain that the user doesn't belong to the Domain AAA Server of the base station.
2. Handover authentication: The user has logged in the wireless network and is accessing, due to its mobility, adjacent base stations proceed to handover in order to provide service seamlessly. The process of handover can not interrupt the access but authenticate mutually between the user and the target base station. The biggest challenge is the duration of the authentication; it shouldn't be too long to affect the quality of service. Hence, the tolerance of authentication latency is shorter than the tolerance of login authentication. The user does not participate in the process of handover authentication, no password is asked. The user barely perceives that the base station is changed. That is the transparency is satisfied here.

Except the issue that login authentication needs password to activate, issues that login authentication considered are all included in handover authentication. Moreover, the handover authentication needs higher performance. This paper will propose an efficient inter-domain handover authentication scheme, and also a scheme with respect to login authentication.

Many researchers proposed solutions to handover authentication. There are four kinds of schemes in terms of the way it is solved:

(a) Prediction Based Scheme
(b) Pre-Authentication Based Scheme
(c) Ticket Based Scheme
(d) Group Key Based Scheme

In prediction based approaches [2, 5, 6], the base station that the user is connecting will send authentication information or keys for authentication to the target base stations that the user is going to handover with. Because user and target base station have shared keys and information they can complete the handover in faster way. The advantage of this approach is that the handover is done fast. The disadvantage is that those authentication information or keys are transferred via the base station or Domain AAA Servers before handover. Therefore, how to predict the next base station is an issue. If we send the authentication information to all neighbor base stations, performance is another issue. Moreover, the user may be traced by adversary.

Pre-authentication approaches [1, 7] authenticate the user and the next base station mutually via the current base station. They also generate a session key in the pre-authentication process. When the user moves to the next base station, they can use the session key to encrypt the exchanged messages because the mutual authentication is already done. The advantage of this approach is the process of authentication has finished, so when the user moves to the target base station, only simple authentication is needed for user to start communication with the target base station. The main disadvantage of pre-authentication approaches is to accurate forecast the target base station. If the user does pre-authentication process with all neighbor base stations, it takes a lot of computation and communication costs. But only one of these neighbor base stations will provide service for the user.

Ticket based methods [4, 8, 9] is that when the user handovers to a target base station, he will send some information representing his identity to the

base station. After the base station receives the information, it will make a query to find out the authentication information or authentication keys belong to the user, and the both parties will make use of the information and keys to finish the handover authentication rapidly. The pros of this kind of methods are that the ticket based approaches can rapidly complete the process of handover authentication and there is not much to do in advance. But the query on the base station side might take some communication and computation costs to find out the ticket corresponding to the user. It causes longer latency. In addition, during the inter-domain handover, whether the information in the ticket could be figured out by the base station and query out the user is also a difficult problem.

The last one type of handover authentication is group key based approach [3]. The user and the base stations in the domain establish a group key. When the user wants to make a handover authentication, the group key is the one thing needed for handover authentication. The plus of this type of method is that the group key finishes the process of authentication. The minus is the maintenance and update of the group key needs Domain AAA Server. In terms of intra-domain handover, a new group is needed to be created to proceed to handover authentication. These are causing severe authentication delay and computation overhead.

Seeing the strategies of handover authentication technologies of scholars, they all have pros and cons. This paper considers integrate prediction based approach and ticket based approach to propose a new scheme. It makes use of the rapidness of prediction based approach and the convenience of ticket based approach to solve login authentication and inter-domain handover these network access authentication issues in wireless network. The proposed scheme provides the following functionality:

(a) Login mutual authentication
(b) Inter-domain handover mutual authentication
(c) Replay attack resistance
(d) Forward/backward secrecy of key generation
(e)Anonymity of user's identity (Only the user's registered Domain AAA Server knows user's real identity)

The remainder of the paper is organized as follows. Section II presents the proposed scheme in detail. Section III analyzes the security of scheme. The performance analysis is given in Section IV. Finally, Section V makes some conclusions.

II. THE PROPOSED SCHEME

The proposed scheme can be categorized into three major components: Register Phase, Login Authentication Phase, and Inter-Domain Handover Authentication Phase. Table 1 defines symbols in the scheme. We assume that the following secure channels are established in wireless network.

(a) Domain AAA servers trust and secure channels exist.
(b) Domain AAA servers and ASN in the domain trust and secure channels exist.
(c) ASN and BSs managed by the ASN trust and secure channels exist.

Table 1. Notations

Notation	Definition
MS	The user (Mobile Station)
sBS	The base station currently connected to
tBS	Target base station after handover
sASN	Access Service Network Gateway of the base station of the user connected to
tASN	Access Service Network Gateway of the target base station in inter-domain handover
nASN	The ASN that is adjacent to sASN (Neighbor ASNs)
sAS	Domain AAA Server of the sBS
tAS	New Domain AAA Server of tBS in inter-domain handover
nAS	The AS that is adjacent to sAS
hAS	The AS that the user registered at (Home AS)
$TempID_i$	Pseudo Name
BS_Rand, MS_Rand, x	Random Number
PUK_A	Public Key of A
AK_i	The Authentication Key for the i-th intra-domain handover authentication or login authentication
IAK_j	The Authentication Key for the j-th inter-domain handover authentication
SK	Session Key that the user exchange messages with the base station while using the network service after authentication
GK_A	Group Key Shared between AS and ASNs
$E_{SK}<>$	Symmetric Encryption with SK
$E_{PUK\_A}\{\}$	Asymmetric Encryption with A's Public Key
h()	One-way Hash function

A. Register Phase

The user has to go through this phase to register at a Domain AAA Server before he requests for

wireless network services at first time. This server is named the user's home Domain AAA Server (hAS). Register phase is executed in a secure channel. MS will complete registration at hAS according to following steps. In this phase, MS will attain the pseudo name and authentication key. Figure 2 shows the flow diagram of register phase.

Step 1: MS proposes a register request to hAS, the request contains user's identification, and information needed for payment.

Step 2: hAS confirms the identity and replies $TempID_1$, AK_1, and IAK_0 to MS. These three numbers are selected in random by hAS.

B. Login Authentication Phase

A user (MS) would like to access the network services via wireless connection, he has to authenticate with the base station (sBS) and the Domain AAA Server (sAS)at the scene. In this phase, there will be mutual authentication, pseudo name update, and key update. MS holds a pseudo name $TempID_i$ and log in with following steps and access to the network service. Figure 3 shows steps to be done in Login Authentication Phase of the proposed scheme. The dotted line represents transmission under secure channel.

Step 1: MS proposes an EAPOL Start to sBS in order to have network access.

Step 2: sBS replies with EAP ID Request message to MS.

Step 3: MS gives {$TempID_i$, hAS} to sBS in response.

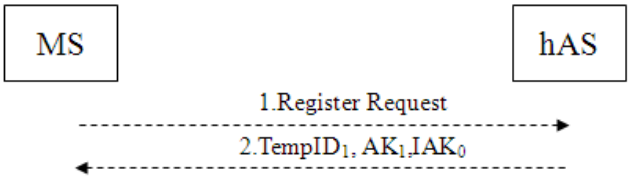

Figure 2. The flow diagram of Register Phase

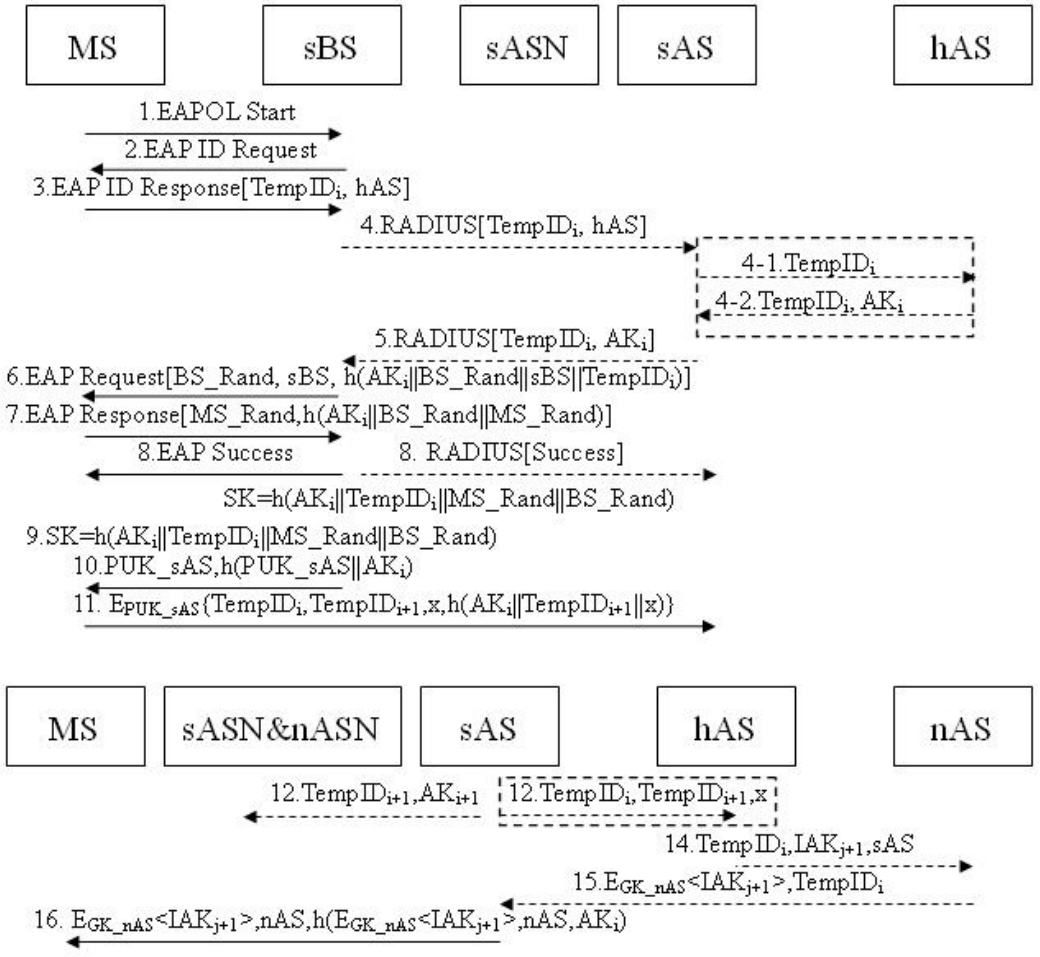

Figure 3. The flow diagram of Login Authentication Phase

Step 4: sBS forwards {$TempID_i$, hAS} to sAS via sASN. If sAS is not hAS, sAS gets MS' AK_i from hAS by the following substeps.

Step 4-1:sAS ask hAS for the AK_i of MS that $TempID_i$ represents.

Step 4-2: hAS tells sAS the corresponding AK_i of $TempID_i$.

Step 5: sAS sends {$TempID_i$, AK_i} through sASN to sBS.

Step 6: sBS selects BS_Rand and creates h(AK_i|| BS_Rand|| sBS||$TempID_i$). And then, sends {BS_Rand, sBS, h(AK_i||BS_Rand||sBS|| $TempID_i$)} to MS.

Step 7:MS verifies h(AK_i||BS_Rand||sBS||$TempID_i$) with AK_i and generates MS_Rand and h(AK_i||BS_Rand|| MS_Rand). And then, sends {MS_Rand, h(AK_i||BS_Rand|| MS_Rand)} to sBS.

Step 8: sBS verifies h(AK_i||BS_Rand||MS_Rand) with AK_i and tells sAS via sASN that the MS is authenticated with the identity. Meanwhile, sends EAP Success to MS. sBS will generate the session key SK=h(AK_i|| $TempID_i$||MS_Rand||BS_Rand) shared with MS for securing the future communication.

Step 9: MS generates the session key SK= h(AK_i||$TempID_i$ || MS_Rand || BS_Rand).

Step 10: sBS sends PUK_sAS and h(PUK_sAS|| AK_i) to MS.

Step 11: MS generates information for next authentication by following substeps.

Step 11-1: makes sure the correctness of PUK_sAS with h(PUK_sAS||AK_i).

Step 11-2: randomly generates the pseudo name $TempID_{i+1}$ and a number x.

Step 11-3: encrypts $TempID_i$, $TempID_{i+1}$, x, and h(AK_i|| $TempID_{i+1}$||x) with PUK_sAS and send it via sBS and sASN to sAS.

Step 11-4: generates AK_{i+1}= h(AK_i||$TempID_{i+1}$|| x) and IAK_{j+1}= h(IAK_j|| $TempID_{i+1}$|| x|| hAS). AK_{i+1} is the authentication key for next intra-domain handover or the key for next login authentication. IAK_{j+1} is the authentication key for next inter-domain handover.

Step 12: sAS generates information of MS' next authentication using following substeps.

Step 12-1: decrypts the message of Step 11-3 to get $TempID_i$, $TempID_{i+1}$, x, and h(AK_i||$TempID_{i+1}$||x).

Step 12-2: generates AK_{i+1}= h(AK_i||$TempID_{i+1}$||x) and check correctness using the corresponding parameter in Step 12-1.

Step 12-3: sends {$TempID_{i+1}$, AK_{i+1}} to the sASN and nASN.

Step 12-4: If the sAS is not hAS of MS, sAS will send $TempID_i$, $TempID_{i+1}$, and x to MS' hAS.

Step 13: hAS generates and records MS' next authentication key AK_{i+1}= h(AK_i|| $TempID_{i+1}$||x) and pseudo name $TempID_{i+1}$.

Step 14: hAS generates IAK_{j+1} =h(IAK_j|| $TempID_{i+1}$ || x||hAS), and sends { $TempID_i$, $TempID_{i+1}$, IAK_{j+1}} and sAS' identity to nAS of MS by secure channel.

Step 15: nAS encrypts IAK_{j+1} with GK_nAS and sends {E_{GK_nAS}<IAK_{j+1}>, $TempID_i$} to sAS.

Step 16: sAS sends {E_{GK_nAS}<IAK_{j+1}>,nAS, h(E_{GK_nAS}<IAK_{j+1}>|| nAS||AK_i)} to MS.

Step17: MS checks and records E_{GK_nAS}<IAK_{j+1}> and nAS.

C. Inter-Domain Handover Authentication

When the user is connected, it is possible to move from the network serving of one base station (sBS) to another (tBS) which are belongs to Domain AAA Servers sAS and tAS respectively. The proposed scheme makes use of the information that the user completed at the preceding authentication phase to reduce the authentication delay and lower the impact to the usage of user's network connection. The user uses the pseudo name $TempID_i$ at sBS and will use the other pseudo name $TempID_{i+1}$ at tBS. In the proposed scheme, the user performs the following step to finish the inter-domain handover authentication. Figure 4 shows steps in an Inter-Domain Authentication. Arrow with dotted line represents transmission under secure channel.

Step 1: MS sends EAPOL Start message to the tBS. In the meantime, generates Inter-Token=

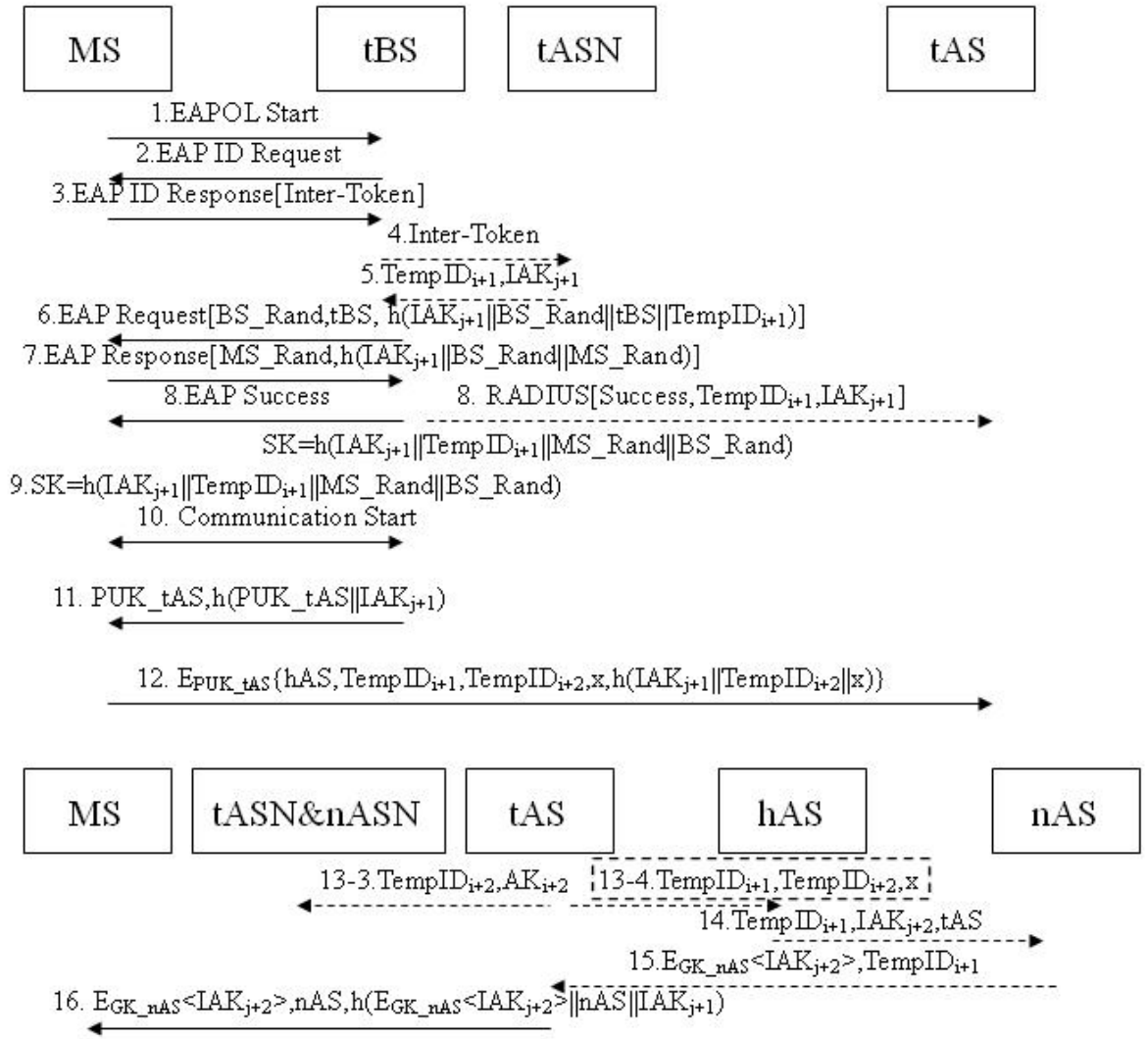

Figure 4. The flow diagram of Inter-Domain Handover Authentication

[TempID$_{i+1}$,E$_{GK_tAS}$<IAK$_{j+1}$>, h(TempID$_{i+1}$|| IAK$_{j+1}$)].

Step 2: tBS sends EAP ID Request to MS in response of the message received.

Step 3: MS responds with Inter-Token to tBS.

Step 4: tBS forwards Inter-Token to tASN.

Step 5: tASN decrypts E$_{GK_tAS}$<IAK$_{j+1}$> to gets IAK$_{j+1}$ and verifies h(TempID$_{i+1}$||IAK$_{j+1}$). If it is true, sends TempID$_{i+1}$ and IAK$_{j+1}$ to tBS. Otherwise, tASN notifies the tBS to stop the connection.

Step 6: tBS generates and sends {BS_Rand, h(IAK$_{j+1}$||BS_Rand||tBS||TempID$_{i+1}$) to MS.

Step 7: MS verifies h(IAK$_{j+1}$|| BS_Rand|| tBS|| TempID$_{i+1}$). If it is correct, MS will generates and sends {MS_Rand, h(IAK$_{j+1}$|| BS_Rand|| MS_Rand)} to tBS.

Step 8: tBS verifies h(IAK$_{j+1}$||BS_Rand||MS_Rand) with IAK$_{j+1}$. If correct, tBS will tell tAS via tASN that the MS is authenticated with the identity. Meanwhile, sends EAP Success to MS. tBS generates the session key SK=h(IAK$_{j+1}$||TempID$_{i+1}$||MS_Rand||BS_Rand) shared with MS for securing the network services.

Step 9: MS generates the session key SK= h(IAK$_{j+1}$|| TempID$_{i+1}$|| MS_Rand|| BS_Rand).

Step 10: tBS begins to provide MS with network service and encrypts exchanged messages with SK when needed.

Step 11: tBS sends {PUK_tAS, h(PUK_tAS|| IAK_{j+1})} to MS.

Step 12: MS generates information for next authentication by following substeps.

Step 12-1: makes sure the correctness of PUK_tAS with h(PUK_tAS||IAK_{j+1}).

Step 12-2: randomly generates the pseudo name $TempID_{i+2}$ and a number x.

Step 12-3: encrypts $TempID_{i+1}$, $TempID_{i+2}$, x, and h(IAK_{j+1}||$TempID_{i+2}$||x) with the public key of tAS and sends it via tBS and tASN to tAS.

Step 12-4: generates AK_{i+2}= h(IAK_{j+1}||$TempID_{i+2}$ || x) and IAK_{j+2}= h(IAK_{j+1}|| $TempID_{i+2}$|| x|| hAS). AK_{i+2} is the authentication key for next login or intra-domain handover. IAK_{j+2} is the authentication key for next inter-domain handover authentication.

Step 13: tAS generates MS' next authentication information by following substeps.

Step 13-1: decrypts the message of Step12-3 to derive $TempID_{i+1}$, $TempID_{i+2}$, x, and h(IAK_{j+1}||$TempID_{i+2}$||x).

Step 13-2: generates AK_{i+2}=h(IAK_{j+1}||$TempID_{i+2}$|| x) and make sure its correctness by the corresponding parameter in Step 13-1.

Step 13-3: sends {$TempID_{i+2}$, AK_{i+2}} to the tASN where MS is at and the tASN's nASN.

Step 13-4: If the tAS is not hAS of MS, tAS will send {$TempID_{i+1}$, $TempID_{i+2}$, x} to hAS.

Step 14: hAS generates MS' next authentication keys AK_{i+2}= h(IAK_{j+1}||$TempID_{i+2}$|| x) and IAK_{j+2}= h(IAK_{j+1}|| $TempID_{i+2}$|| x|| hAS). And then sends MS' pseudo name $TempID_{i+1}$ and IAK_{j+2} to nAS of tAS and notify nAS with the current MS' tAS by secure channel.

Step 15: nAS encrypts IAK_{j+2} with GK_nAS. And then, sends {E_{GK_nAS}<IAK_{j+2}>, $TempID_{i+1}$} to tAS by secure channel.

Step 16: tAS finds h(E_{GK_nAS}<IAK_{j+2}>||nAS|| IAK_{j+1}) and sends {E_{GK_nAS}<IAK_{j+2}>, nAS, h(E_{GK_nAS}<IAK_{j+2}>||nAS|| IAK_{j+1})} via tBS to MS.

Step 17: MS checks and records {E_{GK_nAS}<IAK_{j+2}>, nAS}.

In the procedure of inter-domain handover, the user and the base station finish mutual authentication and derive session key SK before Step 9. Hence, the base station can continue providing user with network connection service at Step 10. That is to say, authentication latency is ended at Step 9. Following Step 11 to Step 17 are the information exchange and update of preparation of next authentication, it will not affect the result of this inter-domain handover authentication. These seven steps do not cause authentication delay, they can be processed when the user using the network. The base station doesn't have to wait until these steps completed to provide user with network connectivity service. Meanwhile, from Step 1 to Step 9, the user and the base station need no Domain AAA Server's assistance to authenticate each other. Thus, authentication latency is shortened obviously. Naturally, he time taken from the beginning to the time the base station start to provide user with service is shorter than login authentication phase.

III. Security Analysis

This section analyzes and demonstrates that the proposed scheme achieves with following four functionalities:

(a) Mutual authentication
(b) Replay attack resistance
(c) Forward/backward secrecy
(d) Anonymity

A. Mutual Authentication

Mutual authentication is the essential and important functionality needed before accessing the network. In the proposed scheme, there will be two kinds of authentication to make the user with mobility have wireless network service: login authentication and inter-domain handover authentication. In Login Authentication Phase, Domain AAA Server checks the identity of the user through mutual authentication between the user and the base station; the user can also ensure the identity of Domain AAA Server and the base station in the same way. Inter-domain handover authentication is the mutual authentication directly between the user and the base station. The user and

Domain AAA server can verify the identity of each other by the process and result of inter-domain handover authentication between the user and the base station.

In Login Authentication Phase, the user sends the pseudo name $TempID_i$ used this time and the identity of hAS to the base station (sBS) and the Domain AAA server (sAS) in current domain. Afterward, Domain AAA Server can request hAS for the authentication key AK_i corresponding to the pseudo name. sAS sends the pseudo name of the user and authentication key as a pair to the base station. The base station generate and send a random number BS_Rand and $h(AK_i|| BS\_Rand|| sBS|| TempID_i)$ to the user. The user make sure the identity of the base station by verifying $h(AK_i||BS\_Rand||sBS||TempID_i)$. The pseudo name $TempID_i$ is randomly selected by the user and changed at each authentication phase, it also can be recognized as a challenge to sBS. If sBS sends the corrected $h(AK_i||BS\_Rand||sBS||TempID_i)$, the user makes sure it gets the corrected AK_i. If and only if the real sAS can obtain corresponding authentication key AK_i from hAS and sends it to the base station. Only the true hAS can provide the authentication key to the sAS. The user authenticates the identities of sAS and hAS while authenticating the base station. The user generates and sends a random number BS_Rand and $h(AK_i||BS\_Rand||MS\_Rand)$ to the base station also. The base station verifies the identity of the user by checking $h(AK_i|| BS\_Rand|| MS\_Rand)$. Only the real user owns the authentication key AK_i. Domain AAA Server and the base station trust each other. If the user passes the authentication process of the base station, Domain AAA Server also convinces the user is authenticated.

In inter-domain handover authentication, the user passes Inter-Token to ASN via base station. If tASN receives Inter-Token (= $[TempID_{i+1}$, $EGK\_tAS<IAK_{j+1}>$, $h(TempID_{i+1}||IAK_{j+1})]$), then tASN decrypts the inter-domain handover authentication key IAK_{j+1} by the group key GK_tAS. And then checks $h(TempID_{i+1}||IAK_{j+1})$ to verify the user with respect to the pseudo name. tASN will then send the pseudo name and the corresponding authentication key to the base station. The base station generates and sends {BS_Rand, $h(IAK_{j+1}|| BS\_Rand||tBS||TempID_{i+1})$} to the user. The pseudo name $TempID_{i+1}$ is randomly selected by the user and changed at each authentication phase, it also can be recognized as a challenge to tBS. The user compares $h(IAK_{j+1}||BS\_Rand||tBS|| TempID_{i+1})$ to authenticate the identity of base station, meanwhile, confirms that only the true tASN sends correct key IAK_{j+1} to the base station. The user also generates and sends {MS-Rand, $h(IAK_{j+1}||BS\_Rand||MS\_Rand)$} to the base station. The base station confirms the identity of the user in the same way. To sum up, the user can authenticate with the base station and Domain AAA Servers with his pseudo name in login phase and inter-domain handover authentication phase. Even though the base station and tAS doesn't know his real name, the user is still authenticated a legal and authorized user.

B. Replay attack resistance

If an attacker catch messages during the communication between the user and the base station and make use of the messages to succeed replay attack, the attack will be able to be fraudulent to the identity of users [7].

At the part that an attacker attempts to launch replay attack, he will send the pseudo name of the user and the identity of hAS to the base station. In the proposed scheme, no matter it is login phase or inter-domain handover authentication phase, the user will update his pseudo name and change authentication key for next authentication via the secure communication to hAS through the base station. If the attacker replay the old pseudo name, sAS can not retrieve corresponding authentication key from user's hAS to the attacker and fail in the authentication.

At the other part, the attacker collects the message of the user's inter-domain handover and replays on another domain, the Token verification will pass, but the probability is negligible for the new base station to choose the same random number BS_Rand as preceding inter-domain handover random number. Under the circumstance that the attacker doesn't own the authentication key of inter-domain handover, he is unable to generate and send the correct

$h(IAK_{j+1}||BS\_Rand||MS\_Rand)$ to the base station. Thus, handover authentication is fail.

C. Forward/Backward Secrecy

Backward secrecy means the attacker with the authentication key of this time and all the collectible information in the network cannot find preceding authentication key. [2] When the attack attempts to derive preceding authentication key from the current authentication key reversely, the first hard problem is to break the one-way hash function. To derive AK_i or IAK_j from $h(AK_i||TempID_{i+1}||x)$ or $h(IAK_i||TempID_{i+1}||x||hAS)$ is as difficult as to compromise one-way hash function h().

In terms of forward secrecy, if the attacker attempts to find the next authentication key from information collected currently, he must have the next pseudo name of the user and the random number for the key. The collectible information and related information are encrypted by the public keys of Domain AAA Servers such as $E_{PUK\_tAS}\{hAS,TempID_{i+1},TempID_{i+2},x, h(IAK_{j+1}||TempID_{i+2}||x)\}$. If the attacker tries to derive the random number for key generation, he needs capability of compromising the public key cryptosystem. The attacker is unable to generate the next authentication key.

D. Anonymity

The pseudo name for the user is generated in random in the proposed scheme. There is no link between each pseudo name [1]. It is changed at each authentication. The pseudo name the user uses next time is encrypted using the public key of Domain AAA Server and sent to Domain AAA Server, the attacker is unable to find the next pseudo name. Therefore, it is untraceable. The pseudo name has nothing to do with user's identity, is generated randomly, the attacker cannot derive the real identity of the user. If the serving Domain AAA Server is not user's home Domain AAA Server and the user is always mobile within the coverage of Domain AAA Server, then the user is traceable by the serving Domain AAA Server without knowing his real identity. Accepting wireless network service has payment issue, so the user's home Domain AAA Server is responsible for tracing the user. One who can derive user's identity from user's pseudo name is user's home Domain AAA Serve. Other parties can not guess user's identity from the pseudo name.

IV. Performance Analysis And Comparison

The main contribution of the proposed scheme is to provide inter-domain handover authentication. This section compares and analyzes in functionality, communication frequencies, and computation costs with other recent works respectively.

The proposed scheme provides identity authentication, replay attack resistance, anonymity, and forward/backward secrecy in inter-domain handover functionalities. Table 2 shows the difference between the proposed scheme and other inter-domain handover protocols. Only the proposed scheme includes all the functionality mentioned, while other works provide some. In terms of security, it provides more intact mechanism.

In terms of communication, if it's necessary to communicate between Domain AAA Servers during handover authentication or rely on Domain AAA Servers to make handover authentication, there will be larger latency on overall communications. Especially, communications between Domain AAA Servers have longer latencies than communications between ASN to Domain AAA Servers. Table 3 shows the comparison between the proposed scheme and other inter-domain handovers in communication type and frequency part. In the process of inter-domain handover authentication, authentication latency since handover success to network access is enabled is the most important thing. Communication types and frequencies in Table 3 is the statistical statement that the target base station authorizes the mobile user to access network services. The proposed scheme finishes mutual authentication after Step 9 in inter-domain handover. In Steps 1 to 9, it needs neither communications between Domain AAA Servers nor communications between ASN to Domain AAA Servers while others need them. Clearly, the

proposed scheme causes less latency on communications than other works. Even it still has Steps 11 to 16 in inter-domain handover; those are preparations for future authentication. It will neither affect handover authentication nor authentication latency this time.

Table 2. Security comparison in inter-domain handovers

	Mutual Authentication	Anonymity	Replay Attack Resistance	Forward /Backward Secrecy
Proposed Scheme	Yes	Yes	Yes	Both
Sun et al.[6]	Yes	No	Yes	Forward
Alfandi et al.[1]	Yes	Yes	Yes	Forward
Tuladhar et al.[8]	Yes	No	Yes	Both
Wang et al.[9]	Yes	No	Yes	No

Table 3. Communication frequency of inter-domain handovers

		AS ↔ AS	MS ↔ BS	BS ↔ ASN	ASN ↔ AS
Proposed Scheme		0	6	2	0
Sun et al.[6]	Scheme1	2	10	8	7
	Scheme2	2	7	5	4
Alfandi et al.[1]		7	5	18	18
Tuladhar et al.[8]		0	17	13	13
Wang et al.[9]		2	10	2	2

Table 4. Computation cost comparisons of Inter-Domain Handovers

		MS	BS	ASN	AS
Proposed scheme		1Asym+ (7+m)Hash+ 3Rand	4Hash+1Rand	1Sym+1Hash	1Asym+(m)Sym+ (2+<1>+m)Hash
Sun et al.[6]	Scheme1	6Sym+1Hash+ 2Rand	4Sym+2Rand	N/A	2Sym+1Hash+ 1Rand
	Scheme2	4Sym+2Hash+1Rand	4Sym+2Rand	N/A	2Hash
Alfandi et al.[1]		3Hash+2Rand	4Asym+3Hash+ 1Rand	N/A	N/A
Tuladhar et al.[8]		3Asym+2Sym+ 2Rand+1Hash	2Sym+1Hash+ 1Rand	N/A	3Asym+1Rand
Wang et al.[9]		4Sym+1Hash+ 2Rand	4Sym+1Hash+ 2Rand	N/A	2Sym

Note:
1.m: Number of Domain AAA Server of the domain that the user is at.
2.Other symbols please refer to Table IV

Table 4 lists the proposed scheme and other researches in computation cost of inter-domain

handover authentication. The proposed scheme is primarily costing spent 2 times of asymmetric encryption operations after Step 9. They affect no authentication latency. These operations are because that we offer anonymity and forward/backward secrecy. In terms of overall computation, Alfandi et al.[1] and Tuladhar et al.[8] take more computations than ours does. Even though Sun et al.[6] and Wang et al.[9] in overall computations has two times less in asymmetric encryption computations, they didn't offer anonymity and backward secrecy. In exclusion of those two security functionality, the proposed scheme is superior in computational cost.

V. CONCLUSION

The proposed scheme offers authentication technologies in login and inter-domain handover in wireless networks. In inter-domain handover process of completing the mutual authentication and generating the session key between the user and the base station, it need no support of user's Domain AAA Server and the Domain AAA Servers of the serving network. It causes low latency and makes faster handover authentication than other studies do. In terms of functionality, the proposed scheme provides mutual authentication, replay attack resistance, anonymity, and forward/backward secrecy. It takes less computation cost than other researches. In privacy part, by the proposed scheme, no parties know user's identity other than user's Domain AAA Server due to following billing issues, even the information of the base station couldn't make it keep track of the user. In summary, the proposed scheme has not only shorter authentication latency, but also more intact security functionality than other researches. It is superior to other studies.

Acknowledgements

This work was partially supported by the National Science Council, Taiwan, under the grants no. NSC 98-2221-E-032 -019.

REFERENCE

[1] O. Alfandi, H. Brosenne, C. Werner, D. Hogrefe, "Fast re-authentication for inter-domain handover using context transfer," in Proc. Information Networking, 2008. International Conference. Jan. 2008, pp. 1–5.

[2] Jaeduck Choi, Souhwan Jung, "A secure and efficient handover authentication based on light-weight Diffie-Hellman on mobile node in FMIPv6," IEICE Trans. Commun., vol.E91–B, NO.2 Feb. 2008, pp. 605–608.

[3] Changyong Lee, Heekuck Oh,Sangjin Kim, "A new authentication protocol for IEEE 802.11 using a group key supporting fast handover, " Convergence Information Technology, 2007. Nov. 2007, pp. 269–272.

[4] L. Maccari, R. Fantacci, T. Pecorella, F. Frosali, "Secure, fast handhoff techniques for 802.1X based wireless network," in Proc. 2006 IEEE International Conference on vol 9, Jun. 2006, pp. 3917–3922.

[5] A. Mishra, M. ho Shin, and W. A. Arbaugh, "Pro-active key distribution using neighbor graphs," Wireless Communications, IEEE Personal Communications. vol 11, Issue 1, Feb. 2004, pp. 26–36.

[6] H-M Sun, S-Y Chang, Y-H Lin, S-Y Chiou, "Efficient authentication schemes for handover in Mobile WiMAX," in Proc. ISDA '08. Eighth International Conference on vol 3, Nov. 2008, pp. 235–240.

[7] H-M Sun, Y-H Lin, S-M Chen, Y-C Shen, "Secure and fast handover scheme based on pre-authentication method for 802.16/WiMAX infrastructure networks," in Proc. 2007 IEEE Region 10 Conference. Nov. 2007, pp. 1–4.

[8] S.R. Tuladhar, C.E. Caicedo, J.B.D. Joshi, "Inter-domain authentication for seamless roaming in heterogeneous wireless networks," in Proc. Sensor Networks, Ubiquitous and Trustworthy Computing, 2008. IEEE International Conference. Jun. 2008, pp. 249–255.

[9] Hongchao Wang, Ping Dong, Hongke Zhang, "An identity based secure and fast authentication protocol in wireless mobile networks," in Proc. WiCOM '08. 4th International Conference. Oct. 2008, pp.1–4.