Wireless Authentication Protocol Preserving User Anonymity

Jaegwan Park[1], Jaeseung Go[2], and Kwangjo Kim[1]

[1]Information Security Group, Information and Communications Univ.,
58-4 Hwaamdong, Yuseoung-gu, Taejon, Korea 305-732
{jgpark, kkj}@icu.ac.kr
[2]Hanaro Telecom, Inc. 470-9, Shindaebang-dong, Tongjak-Gu, Seoul, Korea 156-010
jsgo@hanaro.com

Abstract

We propose an authentication and key agreement protocol while preserving the anonymity of a mobile user in wireless mobile environments. When a mobile user and his visited network mutually authenticate each other, the anonymity of the user should be preserved. In order to provide user anonymity, we introduce new method of computing the temporary identity (TID) during the authentication process. TID is initially computed by a user at the beginning and updated by both user and network side during the execution of the protocol. In addition to guaranteeing user anonymity, we also consider the secure key agreement at the same time.

Keywords

Authentication, Anonymity, Temporary Identity

1. Introduction

1.1. Anonymity in Wireless Systems

When a user is roaming in wireless systems, it is desirable to protect the relevant information about him. Assuring the anonymity of a mobile user prevents unintended parties from associating with the messages to/from him or with the sessions in which he participates. In conventional communications systems, with fixed users and wired networks, anonymity of communicating parties and their location has not been considered. But, it has a great security significance in wireless mobile environments. The disclosure of a mobile user identity allows unauthorized entities to track his moving history and current location. The illegal access to any information related to user location without his notice can be a serious violation of his privacy.

To use the mobile services, a user should identify and authenticate himself to the serving network who provides mobile application services to him. The serving network may be his home network or visited network depending on his current location. We generally assume that visited network is under a different administrative domain from the home network.

A common solution requires that the user authenticates himself to his home network which then confirms the correctness of his identity in the visited network during the authentication process. The user should provide his unambiguous identity to his home network and prove his legality. What is needed is a secure authentication protocol which provides both the authentication and the confidentiality of a mobile user during the execution of the protocol.

1.2. Wireless Authentication Protocols

One of important issues in providing security services under wireless environments is to design the authentication protocol at the beginning of call set-up procedure. With the well-designed authentication protocol, communication partners authenticate each other and agree on the secret session key which will be used to secure the later session [1].

When designing a wireless authentication protocol, we should consider the factors such as the properties of protocol environments and the resources of protocol entities [2]. There are several factors specific to mobile communications systems. Wireless link between user and its serving network is more vulnerable to attack than wired networks. The mobile stations are inherently limited in the computational capability compared with other wired network devices [1].

We also have to consider the security features that should be evaluated in the design of authentication protocol between user and network in wireless systems. These include the following: mutual entity authentication, mutual authenticated key agreement, mutual assurance of key freshness, confidentiality of user identity, non-repudiation of the charging related data, and so on [3, 4, 5]. We focus on the anonymity, i.e., confidentiality of user identity over the wireless and wired links.

In this paper, we propose an authentication and key agreement protocol that satisfies the required security services in wireless systems and especially assures the confidentiality of user identity. This paper is organized as follows. Section 2 reviews previous protocols in which user anonymity is main goal of our design. We describe the design process of authentication and key agreement protocol in Section 3 and evaluate the security features of the proposed protocol in Section 4. Concluding remarks will follow in Section 5.

2. Review of Previous Protocols

We review some previous protocols based on the anonymity mechanism. A basic solution for providing user anonymity is to use the temporary identity (TID) of a mobile user instead of his real one. TID has been called as other terms such as (traveling) alias [8, 9, 10], or subliminal identity [12]. There are several schemes that have been proposed for the generation and computation of TID.

We will use the following notations to describe the protocol throughout this paper unless otherwise specified.

TID_A	Temporary identity of A
$\{X\}_K$	Encryption of a message X using a key K
K_{AB}	Shared secret key between A and B
$PK_A(SK_A)$	Public key (secret key) of A
M	Mobile user and/or his real identity
H	Home network of a mobile user
V	Visited network of a mobile user
T_A	Time stamp generated by A
r_A	Random number generated by A

2.1. Anonymity by using prearranged TID

One method for providing user anonymity is to use the prearranged TID's which have been distributed by the home network. A mobile user stores TID whose mapping real identity is only known to both entities. The same TID is shared between user and his home network on short-term or long-term basis.

The use of TID on long-term basis can be found in the authentication protocol proposed by Molva et al. [8]. They used a unique temporary identity for the identification of a mobile user which is called as traveling alias and has the similar structure to the real identity. When using a long-term based prearranged TID, user and his home network should change the alias at regular intervals in the long time, because unintended third parties, who observe the protocol, happen to infer the relation between the TID and its mapping real identity. They need to run an additional secure protocol to share a new TID used for the next some period.

The identification and authentication procedure in GSM (Global Systems for Mobile communications) is another example using a prearranged TID on short term basis. In GSM, user anonymity is provided by using the temporary identity called $TMSI$ (Temporary Mobile Subscriber Identity) instead of a real identity $IMSI$ (International Mobile Subscriber Identity) assuming that the wired part between home network and visited network is to be secure [7]. When a mobile user M enters a new visited network V, he sends his current $TMSI$ to identify him to the visited network. After the successful identification and authentication process, a new temporary identity $TMSI'$ is given by the network. Figure 1 shows this process. A set of triplet $\langle RAND, SRES, K_{MV}\rangle$ is used to authenticate user and to compute a secret session key, where $RAND$ is a random number for challenge, $SRES$ is the response $\{RAND\}_{K_{MH}}$ using an authentication algorithm A_3 and K_{MV} is a secret session key $\{RAND\}_{K_{MH}}$ using a key generation algorithm A_8.

$M \rightarrow V$	$TMSI$
$V \rightarrow H$	$IMSI, V$
$V \leftarrow H$	a set of $\langle RAND, SRES, K_{MV}\rangle$ triplets
$M \leftarrow V$	$RAND$
$M \rightarrow V$	$SRES$
$M \leftarrow V$	$TMSI'$

Figure 1: Identification and Authentication in GSM

But, when $TMSI$ is not available on account of any reason, M should send his real identity $IMSI$ in the clear through the air interface. This situation arises when a user first turns on his mobile terminal in a new visited network or when the synchronization of TMSI between visited networks is lost. GSM provides a weak security feature in assuring the user anonymity.

2.2. Anonymity by Encrypting the Real identity

Other method is to encrypt the real identity to generate TID during the authentication protocol [6, 9, 10]. A mobile user encrypts his real identity with the public key of his home network which has already given to him and the time variant parameters selected uniquely in each session, such as random number and timestamp, so called "nonce".

Authentication protocol by Samfat et al. is based on shared key cryptosystem [10]. They applied the public key encryption scheme to user anonymity. The computation of TID is performed by the public key encryption of his real identity using the public key of the home network. The protocol is depicted in Figure 2. $AUTH$ is used for message authentication token from originator and receiver. $TICK$ is used for the transport of a secret key which will be shared for secure communication and message authentication between the receiver and other party. They are computed as follows:

$$AUTH_{AB} = [r_A, T_A, Token\{A, T_A, r_A\}_{K_{AB}}]$$

$$TICK\{A, B, C, K_{BC}\}_{K_{AB}} = Token\{r_A \oplus C, r_B, r_A \oplus A\}_{K_{AB}} \oplus K_{BC}$$

where,

$$Token\{A, T_A, r_A\}_{K_{AB}} = \{A \oplus \{T_A \oplus \{r_A\}_{K_{AB}}\}_{K_{AB}}\}_{K_{AB}}$$

$M \rightarrow V$	$H, TID_M, AUTH_{MV}$
$V \rightarrow H$	$TID_M, TID_V, AUTH_{VH}$
$V \leftarrow H$	$\{r_M\}_{P_V}$, $TICK\{H, V, TID_M, K_{MV}\}_{K_{VH}}$
$M \leftarrow V$	$TICK\{V, TID_M, V, P_V\}_{K_{MV}}$

Figure 2: Samfat et al.'s Protocol

In this protocol, the user temporary identity TID_M is computed as $\{r_M, r_M \oplus M\}_{PK_H}$, where $\oplus$ denotes bitwise exclusive-OR operation. To provide anonymity, the real identity M and a random number r_M are encrypted using the public key of the home network PK_H , where r_M is generated independently in each session to compute and renew the TID_M. After the successful establishment of the temporary identity TID_M in the first authentication protocol, a user and his visited network can compute a new temporary identity TID'_M by using the similar computation technique, i.e. $TID'_M = \{r'_M, r'_M \oplus TID_M\}_{PK_V}$, which will be used in the next session.

2.3. Anonymity in ASPeCT

Another method is similar to the previous one in that the real identity is encrypted. But, the authentication protocol is based on public key cryptosystems and user anonymity is provided by symmetric cryptosystems between user and network. ASPeCT protocol [5] shows the example of this case for providing user anonymity.

For the description of the protocol, let G be a group of order q with generator g and r_M, r_V be randomly chosen in group Z_q. Then, ASPeCT protocol is depicted in Figure 3, where V denotes Value-Added Service Provider(VASP).

As shown in Figure 3, identification and anonymity of a user are achieved by the symmetric encryption in the third message. The certificate of a user $cert_M$ is encrypted with the agreed session key $K_{MV} = h1(g^{r_M \cdot SK_V}, r_V)$. But, in this

$$
\begin{array}{ll}
M \rightarrow V & g^{r_M} \\
M \leftarrow V & r_V, h2(K_{MV}, r_V, V), chd, T_V, cert_V \\
M \rightarrow V & \{\{h3(g^{r_M}, g^{SK_V}, r_V, V)\}_{SK_V}, chd, \\
 & T_V, pay, cert_V\}_{K_{MV}}
\end{array}
$$

Figure 3: ASPeCT Protocol

protocol, network does not know if the user is a legal subscriber until it receives his certificate in the last protocol message. We also need to note that the security mechanism between home network and visited network is not considered in this protocol.

ASPeCT provides more enhanced security features than other protocols described above. It obtains a lot of advantages from using public key cryptosystems and public key certificates issued by trusted third parties (TTP's) that can be trusted by all protocol participants. It also provides most of security features required in wireless authentication protocols mentioned in the previous section.

But, ASPeCT has some security problems in session key agreement. It lacks of forward secrecy as already pointed out by Park et al. [11]. Another problem is that it uses the same agreed session key K_{MV} for authentication of message in the second message and for encryption in the third message within the protocol itself. This may results in the disclosure of partial information about the session key that would be used in the following session [13].

3. Wireless Authentication Protocol Preserving User Anonymity

In this section, we propose a wireless authentication protocol which guarantees user anonymity and assures the freshness of temporary identity in each session.

At first, we define some assumptions and the required security goals in wireless authentication protocol. In particular, we place emphasis on user anonymity. Our protocol is based on public key cryptosystems that include digital signature and Diffie-Hellman key exchange. We adopt the challenge-response authentication mechanism by using nonce that is uniquely generated by protocol entities. Also, we try to improve some security problems of ASPeCT protocol discussed in the previous section.

3.1. Assumptions

Assume that our protocol is executed under wireless mobile systems. A user has a mobile terminal equipped with his personal device, user identity module (UIM) such as a smart card that has limited computational capabilities. UIM can store information that includes his real identity and public key certificate. It is also assumed that some portion of security services and their initializations rely on TTP. There may exist some TTP's that each entity can trust. But, we don't consider the hierarchical architecture between TTP's.

The other assumptions for the protocol participants is as follows. Related to public key certificates, every protocol participant has its own certificate issued by TTP and the public key of TTP with which he can verify the certificate of the other party. Upon service subscription, a mobile user is given his real identity and password from his home network, which is stored in his tamperproof storage in his UIM. The public key of the home network is known to all subscribers within its administrative network domain. A visited network will provide services only if the real identity of a user is disclosed and the authenticity of the claimed identity is confirmed by the home network of the user. This assumption is necessary for accounting and billing about using the services between the home network and the visited network. It is also required for the non-repudiation of the user for his service use.

3.2. Protocol Goals

We will consider the security goals which may be achieved after the successful execution of the wireless authentication protocol. They include the following [4]:

- mutual entity authentication
- mutual agreement of shared secret key
- mutual implicit key authentication
- assurance of session key freshness
- user anonymity as a data origin and destination
- non-repudiation of a user for his service use

In particular, we emphasize the user anonymity in designing a protocol. Concerning the generation of temporary identity, Samfat et al. presented the following criteria which should be considered for good anonymity [10].

- *One-time-use*. It is desirable to use a different TID for each security process.
- *No direct relationship between TID's*. It is quite an evident but important requirement.
- *Domain separation*. Even though there were cooperative visited network except home network, the real identity should not be revealed.

These requirements for TID are also considered in the design of authentication protocol. In addition to these requirements, we consider two anonymity features of a user. They also should be evaluated in the design of wireless authentication protocol. We describe them as follows:

- *anonymity of data origin*. When there is a call set-up procedure originating from a mobile user, the user anonymity is preserved.
- *anonymity of data destination*. When there is a call set-up procedure destined for a mobile user, the user anonymity is preserved.

3.3. Design of Authentication Protocol

We assume that any participants can execute the following cyptographic functions:

- A symmetric encryption function where $\{X\}_K$ denotes the encryption of a message X with a key K.
- A signature function where $\{X\}_{SK_A}$ denotes the signature of a message X with a secret key SK of A.
- A pseudorandom number generator
- The cryptographic one way hash functions, h, $h1$ and $h2$, where $h1$ and $h2$ are distinct functions used for key derivation.
- Multiplications in a finite group G of order q with generator g. G is either a subgroup of a multiplicative group ${Z_q}^*$ of a finite field in which the Discrete Logarithm Problem is hard.

Our protocol is shown in Figure 4. The used keys in this protocol are computed as follows.

- $K_{MH} = g^{SK_H \cdot r_M}$, is used to encrypt the information about real identity of a user M and generate his initial temporary identity $TID_M = \{h(M), h(password) \oplus g^{r_M}\}_{K_{MH}}$. It can be computed with the random number selected by M and the public key of the home network H, $PK_H = g^{SK_H}$, already given to the user.
- $K_{VH} = h1(g^{r_V \cdot r_H}, g^{r_H \cdot SK_V})$, is used for message encryption between V and H. It can be computed with the random numbers chosen by both parties and the public key of V.
- $K_{MV} = h1(g^{r_M \cdot r_V}, g^{SK_V \cdot r_M})$, is used for the message encryption and authentication between M and V. It can be computed with the random numbers chosen by both parties and the public key of V
- $K'_{MV} = h2(g^{r_M \cdot r_V}, g^{SK_V \cdot r_M})$, is a shared secret session key after the successful protocol run and will be used for the following session. It is different from the encryption key K_{MV} by applying the different hash function for key derivation.

$M \rightarrow V$	g^{r_M}, TID_M, H	[*i*]
$V \rightarrow H$	$g^{r_V}, g^{r_M}, TID_M,$ $\{h(g^{r_V}, g^{r_M}, TID_M, V)\}_{SK_V}, T_V, cert_V$	[*ii*]
$V \leftarrow H$	$g^{r_H}, [\{h(g^{r_H}, g^{r_V}, h(M) \oplus g^{r_M}, H)\}_{SK_H},$ $h(M) \oplus g^{r_M}]_{K_{VH}}, T_H, cert_H$	[*iii*]
$M \leftarrow V$	$g^{r_V}, \{h(g^{r_V}, g^{r_M}, TID'_M, V), T_H\}_{K_{MV}},$ $T'_V, cert_V$	[*iv*]
$M \rightarrow V$	$[\{h(g^{r_M}, g^{r_V}, T_H, V)\}_{SK_M}, T'_V, cert_M]_{K_{MV}}$	[*v*]

Figure 4: Authentication Protocol

Next, we present the scheme for the computation of temporary identities during the protocol. The TID computation scheme can be subdivided into two steps. The initial temporary identity $TID_M = \{h(M), h(password) \oplus g^{r_M}\}_{K_{MH}}$ is used for the identification of a user by his home network. It proves that the user in the visited network is a legal subscriber. TID'_M is the newly established temporary identity for use in the next session between M and V. It can be changed in each session using the following computation method: $TID'_M = h(g^{r_M \cdot r_V}, h(M))$.

3.4. Detailed Description

We describe the proposed protocol according to the order of message exchange and also discuss the security goals which can be achieved during the execution of each protocol message.

(1) When a mobile user M enters a new visited network V, he begins a registration process with V to identify himself to be a legal subscriber of his home network H. M does the following :

- Generate a secret random number r_M and compute g^{r_M}.

- Compute an agreed key $K_{MH} = (PK_H)^{r_M} = g^{SK_H \cdot r_M}$ and initial temporary identity $TID_M = \{h(M), h(password) \oplus g^{r_M}\}_{K_{MH}}$.

- Send g^{r_M}, TID_M and home network identity H to V. where TID_M is used for the user identification between M and H.

(2) The identification procedure of a mobile user M is performed in both protocol messages [*ii*] and [*iii*]. The encrypted message TID_M containing the real identity information of M is passed from V to H. On receiving the message from M, V identifies the home network H. V does the following :

- Generate a secret random number r_V and compute g^{r_V}.

- Compute its signature using his certified secret key SK_V, i.e. $\{h(g^{r_V}, g^{r_M}, TID_M, V)\}_{SK_V}$.

- Generate its timestamp T_V.

- Send g^{r_V}, g^{r_M}, TID_M, signature, T_V and $cert_V$.

The signature over the hashed value of message provides the implicit entity authentication and implicit authentication of the agreed key which will be shared between V and H. The certificate $cert_V$ provides explicit entity identification. T_V provides the timeliness of the message.

(3) On receiving protocol message [*ii*] from V, H decides if the certificate $cert_V$ is valid or not and the timestamp T_V is within some allowable range compared with its current time. If the verification is positive, H does the following :

- Compute K_{MH} with g^{r_M} and decrypt TID_M to get $h(M), h(password) \oplus g^{r_M}$,

- Identify M from $h(M)$ and verify $h(password)$ with the password of the user M.

- Obtain PK_V from $cert_V$ and identify V.

- Compute $h(g^{r_V}, g^{r_M}, TID_M, V)$ and verify V's signature, if the verification succeeds,

- Generate a secret random number r_H and compute g^{r_H}.

- Compute its signature using his certified secret key SK_H, i.e. $\{h(g^{r_H}, g^{r_V}, h(M) \oplus g^{r_M}, H)\}_{SK_H}$.

- Compute an agreed key K_{VH} and encrypt the signature and $h(M) \oplus g^{r_M}$.

- Generate its timestamp T_H.

- Send g^{r_H}, encrypted message, T_H and $cert_H$.

In this process, the computation of shared key K_{VH} using the fresh random values g^{r_H} and g^{r_V} provides mutual key agreement and key freshness. The signature over hashed value of message also provides implicit key authentication and entity authentication of H to V. The encryption of message using that key provides confidentiality of user identity information.

(4) Messages [*iv*] and [*v*] show the process of the mutual authentication, key agreement and key authentication between M and V. And a new temporary identity of the user TID'_M is computed for use in the next session.

On receiving the message [*iii*] from H, V decides if the certificate is valid or not and the timestamp T_H is within some allowable range compared with its current time. If the verification is positive, V does the following :

- Compute agreed key K_{VH} with g^{r_H} and decrypt the message to get identity information about M, $h(M) \oplus g^{r_M}$.

- Compute $h(g^{r_H}, g^{r_V}, h(M) \oplus g^{r_M}, H)$, obtain PK_H from $cert_H$ and verifies H's signature. If the verification succeeds,

- Compute $TID'_M = h(g^{r_M \cdot r_V}, h(M))$ and store it.

- Compute a hashed value $h(g^{r_V}, g^{r_M}, TID'_M, V)$.

- Compute an agreed key K_{MV} for encryption and a shared key K'_{MV} for the next session.

- Generate a new timestamp T'_V and encrypt hashed value and T_H received from H.

- Send g^{r_V}, encrypted message, T'_V, $cert_V$.

The timestamp T_H within a encrypted message is a piece of information that H has identified M. Also it will be a proof for the future accounting and billing. Symmetric message encryption using K_{MV} provides key agreement, entity authentication and key authentication of V to M.

(5) On receiving the message [*iv*] from V, M decides if the certificate is valid or not and the timestamp T'_V is within some allowable range compared with its current time. If the verification is positive, M does the following :

- Compute an agreed key K_{MV} for decryption and a shared key K'_{MV} for the next session by using g^{r_V} and PK_V from $cert_V$.

- Decrypt the message to get $h(g^{r_V}, g^{r_M}, TID'_M, V)$, T_H and confirm that the time difference $(T'_V - T_H)$ is within the allowable range.

- Compute $TID'_M = h(g^{r_M \cdot r_V}, h(M))$, check if the hashed value is correct and then store TID'_M.

- Compute its signature using his certified secret key SK_M, i.e. $\{h(g^{r_M}, g^{r_V}, T_H, V)\}_{SK_M}$.

- Encrypt the signature, T'_V and $cert_M$.

- Send the encrypted message to V.

The confirmation of the time difference $(T'_V - T_H)$ provides a proof of identification procedure between H and V to M. If the comparison is successful, He consider that V is the right partner with whom he wants to communicate and to whom his home network provides the relevant information about his identity. Encryption of $cert_M$ provides the protection of his real identity from outsiders. Symmetric message encryption using K_{MV} provides key agreement, entity authentication and key authentication of M to V. It also provides non-repudiation of the user for his used service in V.

On receiving the last protocol message, V decrypts the message from M and verifies his certificate and T'_V. Then, he can verify the signature and identify M by comparing the identity information of $cert_M$ with $h(M)$ received from H .

4. Evaluation of Proposed Protocol

4.1. Security Goals and TID Requirements

We evaluate our protocol in view point of security goals. Our proposal satisfies the security goals in wireless authentication protocol that are discussed in the previous section.

Related to the user anonymity, our proposal satisfies the requirements for the use of TID during protocol execution. The temporary identities used in our proposal, TID_M and TID'_M, are computed by using the random numbers chosen by each participant as described in the design of the protocol. They are computed as follows.

$$TID_M = \{h(M), h(password) \oplus g^{r_M}\}_{K_{MH}},$$
$$TID'_M = h(g^{r_M \cdot r_V}, h(M)).$$

- The change of the random numbers g^{r_M} and g^{r_V} selected in each session assures the freshness of the temporary identity in corresponding session. Therefore, a certain temporary identity is used one time only in the session.
- By the same reason, there is no direct relationship between temporary identities of a user. The random numbers chosen by M and V in one session is independent to those in other session. Temporary identities should be changed as the random numbers changed.
- There is also domain separation between visited networks. When user enters a new visited network, he sends a new TID_M, which is an encrypted identity information. The encryption key changes according to the random number r_M generated by M. In a new visited network, a new initial temporary identity is used. So, even though there is a cooperation between visited networks, a new visited network cannot know the real identity until it receives the relevant identity information about the user from home network in protocol message [*iii*]. V has to send his certificate and signature firstly in order to receive the information from H.

We also improve the security about the key agreement in ASPeCT protocol by choosing a different key computation method from ASPeCT to enhance the security feature of forward secrecy. The session key K'_{MV} in our protocol is differently computed from the message encryption key K_{MV} within the protocol. Even if the adversary knows the secret key SK_V of network V, he can not compute a shared secret key of the session, because he doesn't know the secret random value r_V.

And also we can remove the possibility of revealing the partial information about the session key resulting from the use of the same key as an encryption key within the protocol itself. The encryption key within the protocol can be generated apart from the session key by applying a different key derivation function. In our protocol, the encryption key is computed as follows.

encryption key $K_{MV} = h1(g^{r_M \cdot r_V}, g^{SK_V \cdot r_M})$

session key $K'_{MV} = h2(g^{r_M \cdot r_V}, g^{SK_V \cdot r_M})$

4.2. Computational Loads on User Part

Let us consider a computational load on user part. Our protocol is based on the public key cryptosystems, so it is difficult to compare with other previous protocols described in Section 2. Instead, we compare the proposed protocol with ASPeCT [5] as below.

	ASPeCT	Proposed Protocol
Integers modular exponentiation	1	2
Pre-computable exponentiation	1	2
Signature generation	1	1

Table 1: Computational Loads on User Part

The most significant computational operation depends on the number of exponentiation. Considering the number of pre-computable exponentiation, two pre-computable exponentiations, two exponentiations and one signature are required in our proposal. One pre-computable exponentiation is for the computation of initial temporary identity TID_M and one exponentiation is for enhanced key agreement. After the successful execution of the authentication protocol, one pre-computable exponentiation for TID_M can be removed. On the other hand, in ASPeCT, one pre-computable exponentiation, one exponentiation and one signature are required. There are more computational loads required in the proposed protocol than ASPeCT.

The increase of computational load results from the anonymity and key agreement scheme to provide the enhanced security that are not considered in ASPeCT.

4.3. Comparison with Previous Protocols

ASPeCT does not consider the security mechanism between home network and visited network. Though it provides the anonymity in case of the call setup originated from user, it does not consider the anonymity of the call setup terminated at user in visited network. The previous protocols based on shared key cryptosystems [7, 8, 10] provide the limited security features because of their basic cryptographic scheme. They do not offer a part of security goals that are possible in the those protocols based on public key cryptosystems, e.g. mutual key agreement and non-repudiation of service use. Regarding the user anonymity requirements described in the previous section, we try to compare the proposed protocol with the previous protocols [5, 7, 10]. Table 2 shows the comparison of the anonymity requirements and security in key agreement between protocols.

	GSM	SMA95	ASPeCT	Proposed Protocol
Anonymity of data origin	$\surd$	$\surd\surd$	$\surd\surd$	$\surd\surd$
Anonymity of data destination	$\surd$	$\surd\surd$	$\neg$	$\surd\surd$
One-time use of TID	$\neg$	$\surd\surd$		$\surd\surd$
No direct relationship between TID's	$\neg$	$\surd\surd$		$\surd\surd$
Domain separation between TID's	$\surd$	$\surd\surd$		$\surd\surd$
Mutual entity authentication	$\neg$	$\neg$	$\surd\surd$	$\surd\surd$
Mutual key authentication	$\neg$	$\neg$	$\surd\surd$	$\surd\surd$
Mutual key agreement	$\neg$	$\neg$	$\surd\surd$	$\surd\surd$
Forward secrecy			$\neg$	$\surd\surd$
Prevention the leak of partial key information			$\neg$	$\surd\surd$
Computational loads on user part	$\surd\surd$	$\surd$	$\surd$	$\neg$

†† Notation
blank no relation $\surd$ partially satisfied
$\neg$ not satisfied $\surd\surd$ satisfied

Table 2: Comparison between Protocols

5. Concluding Remarks

We proposed an authentication and key agreement protocol that preserve the anonymity of mobile users in wireless communications. In order to provide user anonymity, we presented the computation method of temporary user identity in protocol design. We also improve ASPeCT protocol to provide anonymity and enhanced security concerning key agreement. We evaluate the proposed protocol according to the security features and anonymity requirements. Proposed protocol has some more computational complexity on user part than ASPeCT. And also, we don't consider the key recovery mechanism required to investigate serious crime on communication path and to protect national security by law enforcement agency. The reduction of computational loads and the consideration of key recovery need for further study.

6. References

[1] C. Boyd and A. Mathuria, "Key Establishment Protocols for Secure Mobile Communications: A Selective Survey", *Information Security and Privacy(ACISP98), LNCS 1438*, pp. 344-355, 1998.

[2] L. Chen, D. Gollmann and C. Mitchell, "Tailoring Authentication Protocols to Match Underlying Mechanisms", *Information Security and Privacy, LNCS 1172*, pp.121-133, 1996.

[3] C.J. Mitchell, "Security in Future Mobile Networks", *Proceedings of the Second International Workshop on Mobile Multi-Media Communications (MoMuC-2)*, Bristol, April 1995.

[4] G. Horn, K.M. Martin and C.J. Mitchell, "Authentication Protocols for Mobile Network Environment Value Added Services", a full version is available at `http://isg.rhbnc.ac.uk/cjm/ - Listof-publications`.

[5] G. Horn and B. Preneel, "Authentication and Payment in Future Mobile Systems", *Computer Security - ESORICS'98, LNCS 1485*, pp. 277-293, 1998.

[6] H.Y. Lin and L. Harn, "Authentication Protocols for Personal Communication Systems", *Proceedings of ACM SIGCOMM'95*, pp. 256-261, August 1995.

[7] A. Mehrotra and L.S. Golding, "Mobility and Security Management in the GSM System and some Proposed Future Improvements", *Proceedings of the IEEE, Volume 86, Issue 7,* pp. 1480-1497, July 1998.

[8] R. Molva, D. Samfat and G. Tsudik, "An Authentication Protocol for Mobile Users", *IEE Colloquium on Security and Cryptography Applications to Radio Systems*, pp. 4/1 -4/7, 1994.

[9] N.Asokan, "Anonymity in a mobile computing environment", *Proceedings of Workshop on Mobile Computing Systems and Applications*, pp. 200-204, 1994.

[10] D.Samfat, R.Molva and N.Asokan, "Untraceability in mobile networks", *Proceedings of the First Annual International Conference on Mobile Computing and Networking*, pp. 26-36, 1995.

[11] D.G.Park, C.Boyd and S.J.Moon, "Forward secrecy and Its Application to Future Mobile Communications Security", *Proceedings of the Third International Workshop on Practice and Theory in Public Key Cryptosystems, PKC2000, LNCS 1751*, pp. 433-445, 2000.

[12] V. Varadharajan and Y. Mu, "Preserving Privacy in Mobile Communications: a Hybrid Method", *IEEE International Conference on Personal Wireless Communications*, pp. 532-536, 1997.

[13] V. Shoup, "On Formal Models for Secure Key Exchange", *IBM Research Report RZ 3120*, 1999, A full version is available at `http://www.shoup.net/papers`