A New Roaming Authentication Framework For Wireless Communication

Xiaowei Li[1], Yuqing Zhang[1,2], Xuefeng Liu[1], Jin Cao[1] and Qianqian Zhao[1]
[1] State Key Laboratory of Integrated Services Networks, Xidian University
Shaanxi, Xi'an - China
[e-mail: lixw@nipc.org.cn, zhangyq@gucas.ac.cn, liuxf@mail.xidian.edu.cn, caoj897@gmail.com]
[2] National Computer Network Intrusion Protection Center, University of the Chinese Academy of Sciences
Beijing - China
*Corresponding author: Yuqing Zhang

Received January 16, 2013; revised June 25, 2013; revised June 16, 2013; accepted July 31, 2013; published August 30, 2013

Abstract

Roaming authentication protocol is widely used in wireless network which can enable a seamless service for the mobile users. However, the classical approach requires the home server's participation during the authentication between the mobile user and the foreign server. So the more the roaming requests are performed the heavier burden will be on the home server. In this paper, we propose a new roaming authentication framework for wireless communication without the home server's participation. The new roaming authentication protocol in the new framework takes advantage of the ID-based cryptography and provides user anonymity. It has good performance compared with the roaming authentication protocols whose authentication do not need the home server's participation in terms of security and computation costs. Moreover, a new User-to-User authentication protocol in the new framework is also present. All the authentications proposed in this paper can be regarded as a common construction and can be applied to various kinds of wireless networks such as Cellular Networks, Wireless Mesh Networks and Vehicle Networks.

Keywords: Roaming authentication, wireless network, home server, User-to-User authentication

An early version of this paper which entitled "A Lightweight Roaming Authentication Protocol for Anonymous Wireless Communication" was presented in Globecom 2012. This work was supported by the National Natural Science Foundation of China (NSFC) under Grant 60970140 and Beijing Natural Science Foundation (4122089). The authors would like to thank the editor and all the anonymous reviewers for their useful suggestion..

http://dx.doi.org/10.3837/tiis.2013.08.018

1. Introduction

Ubiquitous mobility and seamless roaming are highly desirable features in the next generation wireless networks. The convergence of diverse but complementary wireless access technologies make this requriement come true. Generally speaking, there are three entities involving in a roaming scenario: a mobile user *U*, a visited foreign server *F* and a home server *H*. The mobile user must firstly register in a server to get the services from this server. After that this server is called the home server of the mobile user. Once the mobile user is outside of his/her home server and roams into a foreign server, he/she and the foreign server must authenticate each other, then after the successful authentication the mobile user can get services from the foreign server. This process is callled the *roaming authentication*.

In classical authentication protocol for roaming service, the home server is often needed when a mobile user wants to get services from the visited foreign server. **Fig.1** shows the authentication of the classical framework for roaming service.

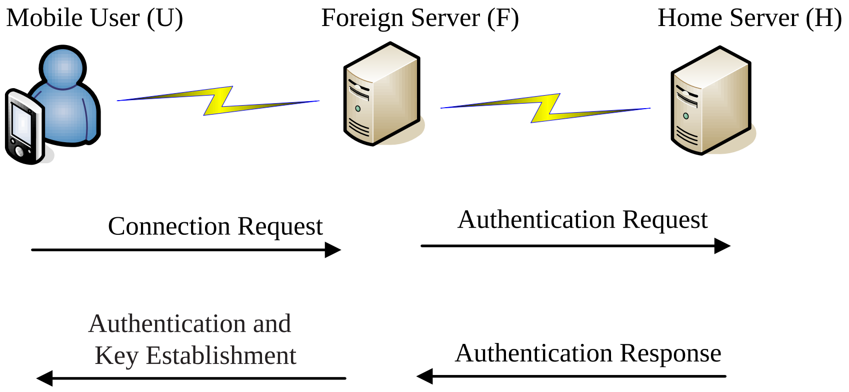


Fig. 1. Authentication of the classical framework for roaming service

Several roaming protocols [1-3] were proposed in this framework. However, since the home server of the mobile user has to participate in every authentication between the foreign server and the mobile user in such framework, a communication delay between the foreign server and the home server is inevitable. When a large number of connection requests between the foreign servers and the mobile users are sent to the home server, the home server may not be able to deal with these requests in time then there might be a delay experienced by the mobile users. This does not meet the goal of the seamless connection. So making the roaming authentication between the mobile user and the foreign server fast and convenient for the mobile user without the home server's participation is a meaningful work in wireless networks. In addition, since more and more people pay much attention to their privacy, how to protect the mobile user's privacy in the roaming authentication framework without the home server's participation is another important problem.

As far as we know, there are two kinds of roaming authentication protocols which can address the problems. One kind is group signature-based authentication, such as the authentication protocol in [4]. The advantage of this method is that the group signature can make the foreign server be sure that the mobile user is legal without the server's participation. Meanwhile, it can provide anonymity for the mobile user against both the unauthorized people and the foreign server. However, the disadvantage of this method is that the group signature is time-consuming and it can not be applied to device which is constrained by processing speed. The other kind is delegation-based authentication, such as the protocol in [5]. The advantage of this method is that it has low computation cost compared with group signature-based method. However, the anonymity property cannot be easily achieved in such case.

In this paper, in order to address the problems presented above and give a seamless connection to the mobile users, we propose a new roaming authentication framework for wireless communication where the home server of the mobile user is not needed to participate when executing the roaming authentication protocol. The main idea is based on delegation-based authentication. The advantages of the new roaming authentication framework are as follows:

- The roaming authentication schemes used in the new framework take advantage of ID-based cryptography.
- It provides privacy-preserving property for the mobile users.
- Compared to classical solutions that relies on the mobile user-foreign server-home server model [1-3], the new authentication protocol in the new framework can achieve a real-time interaction between the mobile user and the foreign server.
- Compared to the similar authentication protocols [4-5] which do not need the home server's participation, the new authentication protocol in the new framework is lightweight and it also has good performance in term of security and efficiency.
- User-to-User authentication can be easily achieved in the new framework without pariticipantion of the users' home servers.

In Section 2, we review the previous work of roaming authentication protocols in wireless networks. In Section 3, we introduce some preliminaries used in this paper. In Section 4, we describe our new roaming authentication protocol. In Section 5, we give two extensions of the protocol proposed in Section 4. We then analyze the security and the performance of the proposed protocol using the tool of AVISPA in Section 6. Finally, in Section 7 we make a conclusion of this paper.

2. Related Work

With the development of the global mobile technique, roaming services have been widely deployed in Cellular Networks such as Global System for Mobile Communications (GSM)

[6], Wireless Mesh Networks (WMNs) [7] and Vehicle Networks [8]. Many researchers focused on this area and did exciting works. Jiang *et al*. [9] proposed a mutual authentication and key exchange protocols for roaming services in wireless mobile networks. In [9], a one-time session key renewal mechanism was proposed which can frequently renew the session key for mobile users and reduce the risk of using a compromised session key to communicate with visited networks. However it has a heavy computational load and is inefficient in the storage rate for mobile user. In order to provide a fast authentication scheme Tang and Wu [10] proposed a novel mobile authentication scheme called EMAS. In EMAS, mobile users can get a pre-shared secret by the trust delegation of his/her home server before he/she visits the foreign server. Compared with the existing delegation-based scheme, EMAS has good performance in term of computation efficiency and communication efficiency. Although EMAS enjoys good performance, Chang and Tsai [11] pointed out the scalability of EMAS was not evident and personal privacy was not protected. To eliminate these weaknesses, Chang and Tsai [11] proposed an anonymous and self-verified mobile authentication scheme. It achieves the anonymity and has high efficiency. However, all these roaming authentication schemes are relying on the mobile user-foreign server-home server model so it might cause delays on the real-time services. Considering the authentication without the participation of the home server, Yang *et al*. [4] proposed universal authentication protocols for anonymous wireless communications using group signature. Each mobile user is issued a private group key after he/she registered in a home server. When roaming into a foreign server, the mobile user only needs to sign the message he/she sends using the corresponding group private key. If the mobile user is a legal user the foreign server can verify the signature using the public key of the user's home server. Group signatures inherently protect the privacy of the mobile user, however, the group signature is not efficient even the best group signature are not efficient either. So Yang *et al*.'s scheme is not efficient in practice. In 2012, He *et al*. [5] proposed a secure and efficient handover authentication based on bilinear pairing functions. The privacy of the mobile nodes is achieved by using a family of pseudo-IDs issued from the authentication server (AS). Meanwhile a batch signature verification scheme is used in [5] which makes the handover authentication become easier. However, the problem of [5] is that the authentication server knows every session key between the mobile nodes and the access points without participating the handover process and it cannot provide forward security. Moreover since pairing operation is used in [5], the computation cost does not seem satisfactory.

3. Preliminaries

3.1 Introduction To ID-based Cryptography (IBC)

ID-based cryptography (IBC) was proposed by Shamir in 1984 [12]. People can use their ID or email address as their public key. IBC eliminates the complicate management of public key certificates and it becomes a powerful alternative to the traditional Public Key Cryptosystem. A trusted third party, called the Key Generation Center (KGC), is involved in IBC. KGC has a master public key and the corresponding master private key. Given an user's identity ID, KGC can issue a private key to the user by using KGC's master private key. The user can use this private key to decrypt a message, sign a message and agree a session key with others. An elliptic curve E/F_q is often used in IBC where F_q denotes a prime finite field. The equation of the elliptic curve used in this paper is $y^2 = x^3 + ax + b$ where $4a^3 + 27b^2 \neq 0$. The points of the elliptic curve form an additive cyclic group *G*. We define a scalar multiplication by $tP = \underbrace{P + P + \cdots + P}_{t}$ where *P* is a point of the elliptic curve.

3.2 Security Goals

A secure authentication protocol for roaming services requires:

- Prevention of impersonation attack. The identity of the mobile user and the servers (foreign or home) should be authentic, that is, the impersonation of the mobile user, the foreign server and the home server should not be possible;
- Providing a private session key. A fresh session key should be agreed on by both participants. Anyone beside the corresponding participants cannot compute the fresh session key except the corresponding participants;.
- Prevention of replay attack. The attacker cannot obtain sensitive data by relaying a previously intercepted message;
- Subscription validation checking. A foreign server is sure about the registration of the mobile user in home server he/she claims.
- Privacy of the mobile user. There are two kinds of privacy involved in roaming authentication. One is the real identity of the mobile user and the other is the roaming line of the mobile user. It is required to provide both kinds of privacy when running the roaming protocols.

In addition, compared with the wired environment the following two factors are more important since the protocols are running on the mobile devices in wireless environment: 1) The low computation cost. The processor and the power of the wireless device are often limited so low computation cost is necessary in wireless environment [13]; 2) The low communication cost. Since the bandwidth is lower and the channel error is higher in wireless networks than that in wired networks, the number of message exchanges should be small.

4. A New Roaming Authentication Protocol

In this section we propose a lightweight roaming authentication protocol based on ID-based cryptosystem. The notations used in the scheme are in **Table 1**. The system consists of multiple servers and multiple subscribers. Each server manages a set of subscribers, and each subscriber could be a mobile user. There are two algorithms in the protocol, i.e., Setup and Roaming authentication protocol.

Table 1. Notations

Notation	Description
q	A large prime number
F_q	A prime field
E	An elliptic curve over a prime finite field F_q
G	A subgroup of F_q
P	A generator of G
$H_1(\cdot)$	A cryptographically secure hash functions from $(0,1)^* \to Z_q^*$
$H(\cdot)$	A cryptographically secure hash functions from $(0,1)^* \to \{0,1\}^l$, where l is a secure parameter
U, F, H	Mobile user, Foreign Server, Home Server
ID_{U_H}	The identity of an entity U who registers in H
mpk_i, msk_i	The public and private key pair of the server i
$\|\|$	The concatenation operator
$\oplus$	The bitwise exclusive-OR operator
$E_k(\cdot) / D_k(\cdot)$	A Symmetric Encryption/Decryption algorithm using a symmetric key k
$MAC_k(\cdot)$	A Message Authentication Code algorithm using a symmetric key k
K_{XY}	The session key between entity X and Y

4.1 Setup

Each server independently acts as a KGC to the users who register in it. All the KGCs share the same parameters such as the elliptic curve, the associated group and the generator. Given a security parameter *k*, KGC does the follows:

1) The system chooses an elliptic curve E / F_q and a generator *P* of the additive group which consists of the points of the elliptic curve. The elliptic curve E / F_q and its generator *P* are public. Then each server *i* chooses its public and private key pair (mpk_i, msk_i), where $mpk_i = s_i P, msk_i = s_i$ and $s_i \in Z_q^*$. mpk_i is known to all the other servers and all of the users within the network controlled by the server. This could be realized by requiring the serving network to broadcast its digital certificate to all the users currently in the network.

2) Whenever a user U_H with identity ID_{U_H} wants to register in the server *H*, *H* issues a private key to the user with its master private key. After the registration *H* is called the home server of the user. Specifically, *H* chooses a random value from $r \in Z_q^*$ and computes $R_{U_H} = rP$ and $h = H_1(ID_{U_H} \| R_{U_H})$. Then, the private key of U_H is computed by

$s_{U_H} = r + h \cdot s_H$, where s_H is the private key of the server *H*. *H* issues the private key (R_{U_H}, s_{U_H}) to U_H via a secure channel. Upon receiving R_{U_H}, s_{U_H} , U_H can verify whether $s_{U_H}P = R_{U_H} + H_1(ID_{U_H} \| R_{U_H})mpk_H$ holds or not, where mpk_H is the public key of the server *H*. If the equation holds, it means the private key is valid; otherwise, it is not valid.

4.2 Roaming Authentication Protocol

Let ($mpk_H = s_H P, msk_H = s_H$) be the public key and private key pair of U_H 's home server *H*, and ($mpk_F = s_F P, msk_F = s_F$) be the public key and private key pair of a foreign server *F*. When U_H roams into *F* the authentication and key agreement is performed as follows. **Fig. 2** shows the process of the roaming authentication.

1) When visiting a foreign server *F*, U_H selects a random value $a \in Z_q^*$ and computes aP . Let $K_1 = a \cdot s_F P$ and $\sigma = E_{K_1}(ID_{U_H}, R_{U_H}, ID_H)$. Then U_H sends (aP, σ) to *F*.

2) Upon receiving (aP, σ), *F* computes $K_1 = s_F \cdot aP$ with its private key s_F and obtains ID_{U_H}, R_{U_H}, ID_H by decrypting σ . Then, *F* finds the public key of *H* and chooses a random value $b \in Z_q^*$ and computes bP . Let $K_2 = b \cdot (R_{U_H} + H_1(ID_{U_H} \| R_{U_H})mpk_H)$ and $Auth_F = MAC_{K_1}(bP)$. *F* sends ($bP, Auth_F$) to U_H .

3) Upon receiving ($bP, Auth_F$), U_H checks whether $Auth_F = MAC_{K_1}(bP)$ holds. If the equation does not hold, he/she halts. Otherwise, U_H computes $K_2 = s_{U_H} \cdot bP$ and $K_3 = a \cdot bP$. Let $Auth_{U_H} = MAC_{K_2}(aP)$ and the session key $K_{U_H F} = H(ID_{U_H} \| ID_F \| K_1 \| K_2 \| K_3)$. U_H sends the authentication message $Auth_{U_H}$ to *F*.

4) Upon receiving $Auth_{U_H}$, *F* checks whether $Auth_{U_H} = MAC_{K_2}(aP)$ holds. If the equation does not hold, it halts. Otherwise, *F* computes $K_3 = b \cdot aP$ and the session key $K_{FU_H} = H(ID_{U_H} \| ID_F \| K_1 \| K_2 \| K_3)$. It is easy to see $K_{U_H F} = K_{FU_H}$.

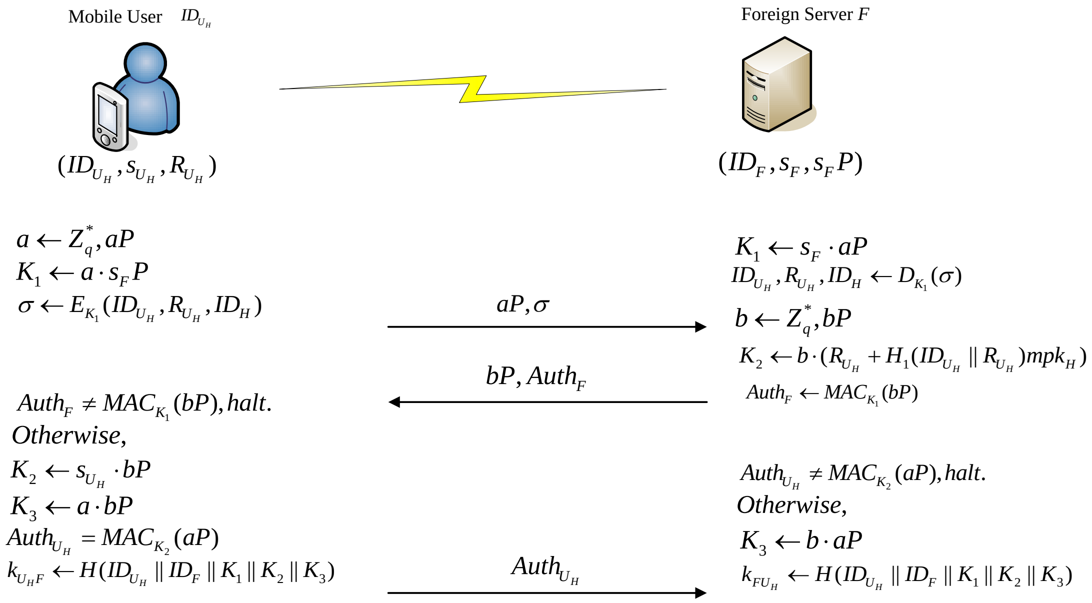

Mobile User ID_{U_H}
Foreign Server F
$(ID_{U_H}, s_{U_H}, R_{U_H})$
$(ID_F, s_F, s_F P)$
$a \leftarrow Z_q^*, aP$
$K_1 \leftarrow a \cdot s_F P$
$\sigma \leftarrow E_{K_1}(ID_{U_H}, R_{U_H}, ID_H)$
aP, σ
$K_1 \leftarrow s_F \cdot aP$
$ID_{U_H}, R_{U_H}, ID_H \leftarrow D_{K_1}(\sigma)$
$b \leftarrow Z_q^*, bP$
$K_2 \leftarrow b \cdot (R_{U_H} + H_1(ID_{U_H} \| R_{U_H}) mpk_H)$
$Auth_F \leftarrow MAC_{K_1}(bP)$
$bP, Auth_F$
$Auth_F \neq MAC_{K_1}(bP), halt.$
$Otherwise,$
$K_2 \leftarrow s_{U_H} \cdot bP$
$K_3 \leftarrow a \cdot bP$
$Auth_{U_H} = MAC_{K_2}(aP)$
$k_{U_H F} \leftarrow H(ID_{U_H} \| ID_F \| K_1 \| K_2 \| K_3)$
$Auth_{U_H}$
$Auth_{U_H} \neq MAC_{K_2}(aP), halt.$
$Otherwise,$
$K_3 \leftarrow b \cdot aP$
$k_{FU_H} \leftarrow H(ID_{U_H} \| ID_F \| K_1 \| K_2 \| K_3)$

Fig. 2. The new authentication protocol for roaming service

5. Two Extensions of the New Roaming Authentication Protocol

In this section, we give two extensions of the new roaming authentication protocol. One extension is on the anonymity. We give an extension version of the proposed authentication protocol in Section 4 to make it provide *strong* anonymity property. The other extension is on the User-to-User authentication. The following two subsections show the details of the extensions.

5.1 Strong Anonymity Extension

Actually from **Fig. 2**, we can see the privacy of the mobile user is protected against the unauthorized person but not the foreign server. The foreign server can know the real identity of every mobile user when performing the authentication. We call the privacy-preserving property against the unauthorized person including the foreign server strong anonymity. The detailed protocol with strong anonymity property is as follows. Fig.3 shows the process of the roaming authentication.

5.1.1 Setup

The parameters used here are the same as that of Section 4. Whenever a user U_H with identity ID_{U_H} wants to register in the server H, H selects a family pseudo-IDs $PID = \{pid_1, pid_2, ...,\}$ where pid_i is not selected before. Then， H issues a family of private keys to the user with its master private key. Specifically, for pid_i, H chooses a random value r_i from Z_q^* and computes $R_{pid_i} = r_i P$ and $h_i = H_1(pid_i \| R_{pid_i})$. Then the private key which matches pid_i is computed by $s_{pid_i} = r_i + h_i \cdot s_H$. H issues the pseudo-ID pid_i and the private key (R_{pid_i}, s_{pid_i}) to U_H through a secure channel. Upon receiving (R_{pid_i}, s_{pid_i}), U_H can verify whether $s_{pid_i} \cdot P = R_{pid_i} + H_1(pid_i \| R_{pid_i}) mpk_H$ holds. If the equation holds it means the private key is valid otherwise it is not valid. Similarly, U_H gets a family of pseudo-IDs $PID = \{pid_1, pid_2, ..., \}$ and the corresponding private keys $\{(R_{pid_1}, s_{pid_1}), (R_{pid_2}, s_{pid_2}), ...\}$.

5.1.2 Roaming Authentication Protocol

When visiting a foreign server F, U_H picks an unused pseudo-ID pid_i and the corresponding private key (R_{pid_i}, s_{pid_i}). Then U_H performs the authentication and establishes a common session key with F using pid_i and (R_{pid_i}, s_{pid_i}). The roaming authentication is similar to the authentication in Section 4.2 except the first message. The first message is changed by $(aP, pid_i, R_{pid_i}, ID_H)$ other than (aP, σ) since every pseudo-ID pid_i is used only once, pid_i does not need to be encrypt. **Fig. 3** shows the detailed authentication process and we do not give the concrete description here.

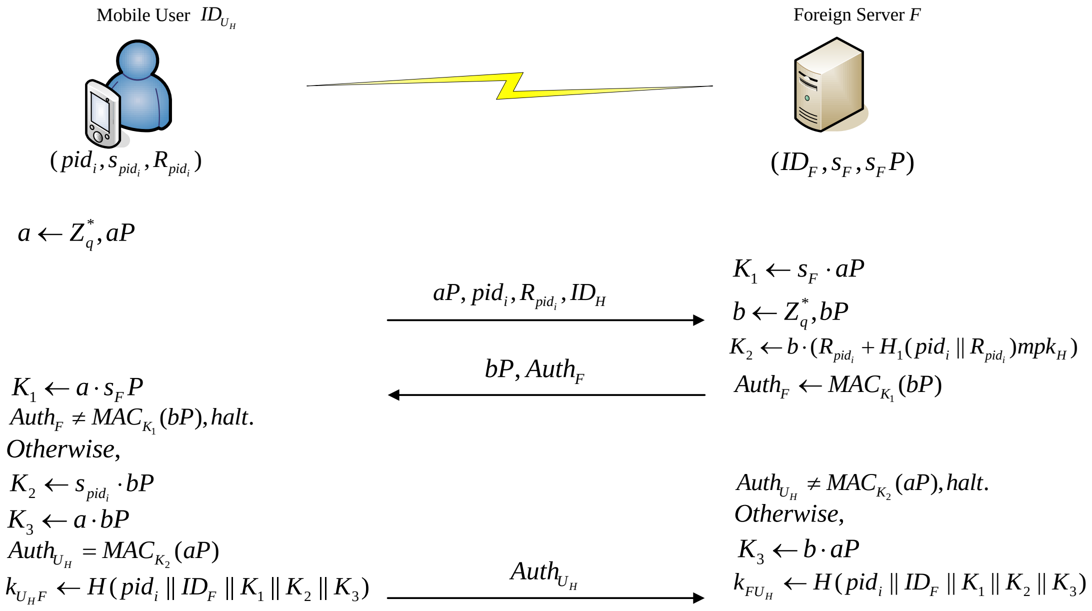

Mobile User ID_{U_H}
Foreign Server F
$(pid_i, s_{pid_i}, R_{pid_i})$
$(ID_F, s_F, s_F P)$
$a \leftarrow Z_q^*, aP$
$K_1 \leftarrow s_F \cdot aP$
$aP, pid_i, R_{pid_i}, ID_H$
$b \leftarrow Z_q^*, bP$
$K_2 \leftarrow b \cdot (R_{pid_i} + H_1(pid_i \| R_{pid_i}) mpk_H)$
$bP, Auth_F$
$Auth_F \leftarrow MAC_{K_1}(bP)$
$K_1 \leftarrow a \cdot s_F P$
$Auth_F \neq MAC_{K_1}(bP), halt.$
$Otherwise,$
$K_2 \leftarrow s_{pid_i} \cdot bP$
$K_3 \leftarrow a \cdot bP$
$Auth_{U_H} = MAC_{K_2}(aP)$
$k_{U_H F} \leftarrow H(pid_i \| ID_F \| K_1 \| K_2 \| K_3)$
$Auth_{U_H}$
$Auth_{U_H} \neq MAC_{K_2}(aP), halt.$
$Otherwise,$
$K_3 \leftarrow b \cdot aP$
$k_{FU_H} \leftarrow H(pid_i \| ID_F \| K_1 \| K_2 \| K_3)$

Fig. 3. The new authentication protocol for roaming service with strong anonymity

5.2 Use-To-User Authentication Extension

User-to-user authentication are often used in Wireless Mesh Networks (WMNs) [7] or in the Vehicle Networks [8] (which is said the Vehicle-to-Vehicle authenticaiton). For example, a mesh user can also serves as a router in WMNs, that is, it can provide peer-to-peer networks among user devices. When a mesh user roams into a foreign domain *F* from his/her home domain *H*, communication between different mesh users may occur such as providing packet forwarding service. The same scenario can be seen in the Vehicle Networks. In vehicle networks, a vehicle equipped with an onboard unit (OBU) makes it can not only communicate with the roadside units (RSU) but also communicate with the other vehicles. So users might need to establish a shared keys to secure traffic between them. In such case a user-to-user authentication scheme is needed. However, authentication between these users is non-trival since there is no shared information between the users. So the corresponding servers are often needed in such scenarios. In order to make the user-to-user authetnication can be completed without interatction with its home server, in this subsection we propsoe a user-to-user authentication scheme in different domains. **Fig. 4** shows the process of the authentication.

5.2.1 Setup

This process is similar to Section 4.1 and we just give a brief introduction. Suppose a user U_H who belongs to *H* wants to communicate with a user U_F who belongs to *F*. U_H has registered in the server *H* and has personal information $(ID_{U_H}, R_{U_H}, s_{U_H})$ while U_F has registered in the server *F* and has personal information $(ID_{U_F}, R_{U_F}, s_{U_F})$.

5.2.2 Roaming Authentication Protocol

1) When U_H roams into the range of the server *F* and he/she wants to communicate with U_F in the same range. U_H will firstly select a random value $a \in Z_q^*$ and computes aP. Then, U_H sends $(ID_{U_H}, R_{U_H}, aP, ID_H)$ to U_F.

2) Upon receiving $(ID_{U_H}, R_{U_H}, aP, ID_H)$, U_F chooses a random value $b \in Z_q^*$ and computes bP . Then, U_F computes $K_1 = b \cdot (R_{U_H} + H_1(ID_{U_H} \| R_{U_H})mpk_H)$ and $K_2 = s_{U_F} \cdot aP$ with its master private key s_{U_F} . The authentication message is $Auth_{U_F} = MAC_{(K_1 \oplus K_2)}(bP)$. U_F sends $(ID_{U_F}, R_{U_F}, bP, Auth_{U_F})$ to U_H.

3) Upon receiving $(ID_{U_F}, R_{U_F}, bP, Auth_{U_F})$, U_H computes $K_2 = s_{U_H} \cdot bP$ and $K_1 = a \cdot (R_{U_F} + H_1(ID_{U_F} \| R_{U_F})mpk_F)$. Then, U_H checks whether $Auth_{U_F} = MAC_{(K_1 \oplus K_2)}(bP)$ holds. If the equation does not hold, he/she halts. Otherwise U_H computes $K_3 = a \cdot bP$ and $Auth_{U_H} = MAC_{(K_1 \oplus K_2)}(aP)$. Finally U_H computes the session key $K_{U_H U_F} = H(ID_{U_H} \| ID_{U_H} \| K_1 \| K_2 \| K_3)$. U_H sends the authentication message $Auth_{U_H} = MAC_{(K_1 \oplus K_2)}(aP)$ to U_F.

4) Upon receiving $Auth_{U_H}$, U_F checks whether $Auth_{U_H} = MAC_{(K_1 \oplus K_2)}(aP)$ holds. If the equation does not hold, it halts. Otherwise U_F computes $K_3 = b \cdot aP$ and the session key $K_{U_F U_H} = H(ID_{U_H} \| ID_{U_H} \| K_1 \| K_2 \| K_3)$. It is easy to see $K_{U_H U_F} = K_{U_F U_H}$.

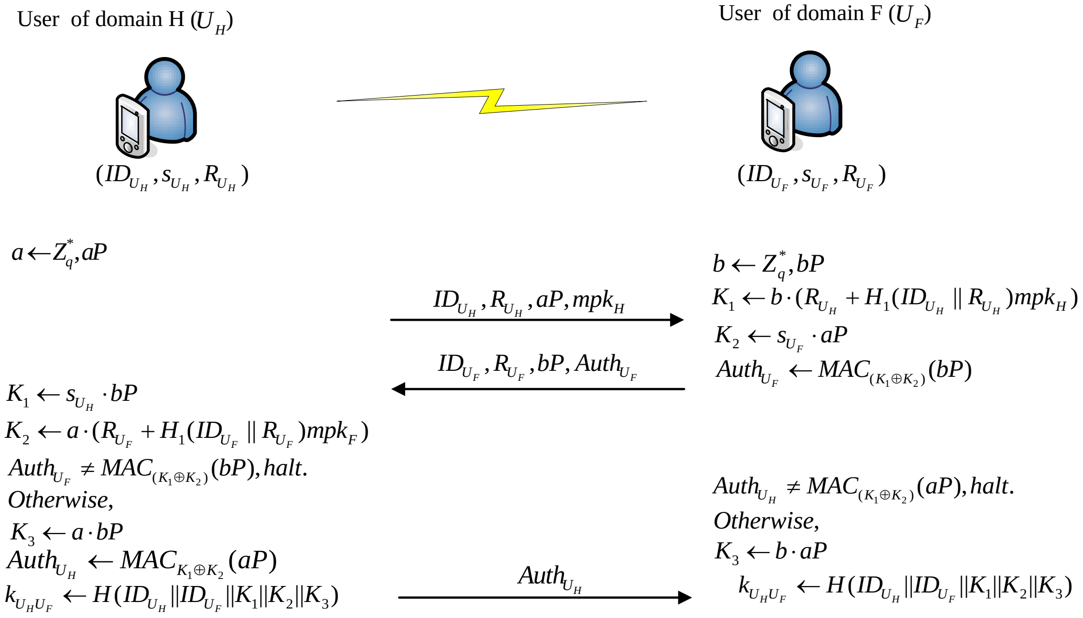

User of domain H (U_H)
User of domain F (U_F)
$(ID_{U_H}, s_{U_H}, R_{U_H})$
$(ID_{U_F}, s_{U_F}, R_{U_F})$
$a \leftarrow Z_q^*, aP$
$b \leftarrow Z_q^*, bP$
$ID_{U_H}, R_{U_H}, aP, mpk_H$
$K_1 \leftarrow b \cdot (R_{U_H} + H_1(ID_{U_H} \| R_{U_H})mpk_H)$
$K_2 \leftarrow s_{U_F} \cdot aP$
$ID_{U_F}, R_{U_F}, bP, Auth_{U_F}$
$Auth_{U_F} \leftarrow MAC_{(K_1 \oplus K_2)}(bP)$
$K_1 \leftarrow s_{U_H} \cdot bP$
$K_2 \leftarrow a \cdot (R_{U_F} + H_1(ID_{U_F} \| R_{U_F})mpk_F)$
$Auth_{U_F} \neq MAC_{(K_1 \oplus K_2)}(bP), halt.$
$Otherwise,$
$K_3 \leftarrow a \cdot bP$
$Auth_{U_H} \leftarrow MAC_{K_1 \oplus K_2}(aP)$
$k_{U_H U_F} \leftarrow H(ID_{U_H} \| ID_{U_F} \| K_1 \| K_2 \| K_3)$
$Auth_{U_H}$
$Auth_{U_H} \neq MAC_{(K_1 \oplus K_2)}(aP), halt.$
$Otherwise,$
$K_3 \leftarrow b \cdot aP$
$k_{U_H U_F} \leftarrow H(ID_{U_H} \| ID_{U_F} \| K_1 \| K_2 \| K_3)$

Fig. 4. User-to-User authentication in WMNs or Vehicle Networks

6. Security Analysis and Performance

In this section, we give the security analysis and performance analysis of the proposed protocols.

6.1 Security Analysis

6.1.1 Formal Security Analysis by AVISPA

We use automated protocol analysis tool to analyze the security properties that our scheme can possess by Automated Validation of Internet Security Protocols and Applications (AVISPA) [14]. AVISPA is widely used in verifying the security of the secure protocol in the communication networks. It provides a modular and expressive formal language (High-Level Protocol Specification Language HLPSL) for specifying protocols and their security properties. We only analysis the security of the protocol proposed in Section 4 since the method and the cryptography assumption used in the three protocols are similar to each other so readers can understand the security of the second protocol and the third protocol on the basis of the analysis of the first one. We first describe the protocol in Section 4 using HLPSL. As seen in the protocol, there are two basic roles *U* and *F* which represent the two participants of the mobile user *U* and foreign server *F*, respectively. The role of the foreign server *F* is shown in **Fig. 5** (we only present the basic role of foreign server *F* as an example and the role of the mobile user is similar to the role of the foreign server).

```
role f(
U,F   :agent,
PKu, PKf     :public_key,
P                  : text,
H            :hash_func,
M            :hash_func,
SND,RCV        :channel(dy))
played_by F def=
local
    N_U:text,
    N_F :text,
    K_1 : text,
    K_2 : text,
    K_3 : text,
    K_UF:message,
    State:nat
const
sec_u_k, sec_f_k :protocol_id
init
   State:=1
 transition
1. State=1/\RCV(exp(P, N_U').{U.exp(P, N_U').F}_(exp(PKf,N_U')))
      =|>
    State':=3
        /\ N_F':=new()
        /\ K_1':=exp(exp(P,N_U'),inv(PKf))
        /\ K_2':=exp(PKu,N_F')
        /\SND(exp(P, N_F'). M(exp(exp(P,N_U'),inv(PKf)).exp(P,N_F')))
        /\ K_3':=exp(exp(P,N_U'),N_F')
        /\ K_UF':=H(U.F.K_1'.K_2'.K_3')
        /\ secret(K_UF', sec_f_k,{U,F})
        /\witness(F,U,m_f,M(exp(exp(P,N_U'),inv(PKf)).exp(P,N_F')))
  2. State=3/\ RCV(M(K_2'.exp(P,N_U)))
      =|>
     State':=5
            /\request(F,U,m_u,M(K_2'.exp(P,N_U)))
end role
```

Fig. 5. Role of Foreign Server F

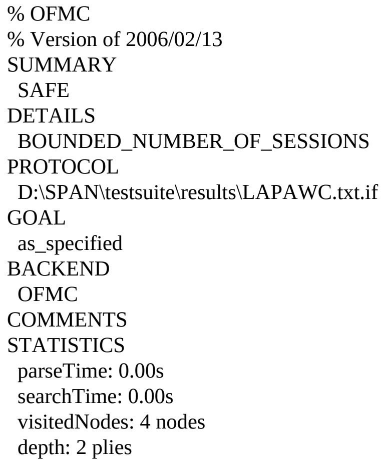
More precisely, when simulating the protocol, *F* waits to receive the messages *aP* and σ from U and then sends *bP* and $Auth_F$ to the *U*. The state *State* of *F* will be changed from 1 to 3 at this moment. After *State* has been changed to 3, $Auth_{U_H}$ is sent to *F* from *U*. We use *channel (dy)* to denote the Dolev-Yao model which considers an active intruder who controls the network but cannot break cryptography. In this model, the intruder can eavesdrop, intercept, insert, tamper and replay the messages to other honest communication parties under any agent name.

We analyze the basic properties of the secure protocol using AVISPA, i.e., the authentication of *U* and *F* and the secrecy of the session key between *U* and *F*. The goals are described in **Fig. 6**. For authentication, our goal is to check that the intended peer, which is present in the current session, has reached a certain state and agreed on a certain session key. For secrecy, our goal is to confirm that the session key should be secret between the communication parities which are declared. If the goals cannot be achieved, it means that the intruder successfully attacks the protocol and gets the session key of this session. We verify two *authentication* and one *secrecy* goals as follows.

```
goal
secrecy_of   sec_u_k, sec_f_k
 authentication_on m_f
authentication_on m_u
end goal
```

Fig. 6. Analysis goals of the model

- ➢ *U* authenticates *F* on $Auth_F$: *F* chooses a random value *b* and generates the MAC value using *b* and its private key. When receiving the message from *F*, U obtains $Auth_F$ which comes with *F*'s identity. Then, *U* can authenticate *F* by verifying the value $Auth_F$.
- ➢ *F* authenticates *U* on $Auth_{U_H}$: Similarly, *U* chooses a random value *a* and generates the MAC value $Auth_{U_H}$ using a and its private key. When receiving the message from *U*, *F* obtains $Auth_{U_H}$ which comes with *U*'s identity. *U* can authenticate F by verifying the value $Auth_{U_H}$.
- ➢ Secrecy of $K_{U_H F}$: The random values *a* and *b* which are used to generate the session key are only known by *U* and *F*, respectively. So only legal user and server can get the sercets K_1,K_2 and K_3 . Thus, any intruder cannot get the session key $K_{U_H F} = H(ID_{U_H} \| ID_F \| K_1 \| K_2 \| K_3)$ between the *U* and *F*.



```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  D:\SPAN\testsuite\results\LAPAWC.txt.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.00s
  visitedNodes: 4 nodes
  depth: 2 plies
```

Fig. 7. Results reported by the OFMC back-end

We use the back-end analysis tool On-the-fly-Model-Checker (OFMC) to deal with the results translated from the HLPSL since OFMC is state-of-the-art both in terms of coverage and performance [15]. At first, OFMC shows that our scheme can resist the replay attack by performing a search for a passive intruder and giving the intruder the knowledge of some "normal" sessions between the honest agents. We then set the depth of the search to be two and the output of the model checking results is shown in **Fig. 7**. From **Fig. 7**, we can conclude that the proposed scheme can achieve the properties of the authentication and secrecy of the session key. Moreover, it can also resist some other malicious attacks such as Man-in-the-Middle attacks under the test of AVISPA using the OFMC back-end with bounded number of sessions.

6.1.2 Other Security Metrics

- **Subscription validation checking**. If the authentication process is successfully, the foreign server F can ascertain that the mobile user U_H is a legal user who has registered in H. The reason is that F computes the session key between U_H and F using the public key of U_H's home server H. If U_H did not register in H, he/she cannot get the delegation key s_{U_H} and he/she cannot compute $K_2 = b\cdot(R_{U_H} + H_1(ID_{U_H} \| R_{U_H})mpk_H) = s_{U_H}\cdot bP$ either. So the subscription validation can be checked by any foreign server.
- **Privacy of the mobile user**. Here we discuss two kinds of anonymity, *weak anonymity* and *strong anonymity*. Weak anonymity denotes that the privacy of the mobile user is protected against the unauthorized person but not the foreign server. Strong anonymity denotes that anyone including the foreign server cannot obtain the privacy of the mobile user. We demonstrate weak anonymity can be achieved in the authentication protocol in Section 4 and strong anonymity can be achieved in the authentication protocol in Section 5.1.

- ➢ Weak anonymity. Suppose the encryption algorithm is secure then the adversary can not reveal the identity of U_H. The identity of U_H is encrypted by the partial private key K_1 where $K_1 = a \cdot s_F P$. So if ID_{U_H} is revealed by the adversary, then it means he/she has computed the $K_1 = a \cdot s_F P$ by aP and $s_F P$. It further means the adversary has solved the ECDH problem. Since the ECDH problem is hard, the identity as well as the roaming line of the mobile user can be protected.
- ➢ Strong anonymity. As shown in Fig.3, we can see when authenticating with F, U_H selects an unused pseudo-ID pid_i so if U_H does not reuse the pseudo-ID, F is unable to identify U_H, i.e., it provides strong anonymity for the mobile user.

- ● **Forward security**. Forward security means even if the private key of the mobile user or the foreign server has been corrupted by the adversary, he/she cannot retrieve the session key which was computed before this point. In the proposed protocol, if the long time private keys of both participates (the mobile user and the foreign server) are corrupted by the adversary he/she can compute K_1 and K_2. However, the adversary cannot compute $K_3 = abP$ since the partial key K_3 is independent in each protocol instance so he/she cannot retrieve the session key before this point.

6.2 Performance

Small computation cost is important for mobile terminals since these devices are always limited to processor speed or battery power. We illustrate the efficiency of the proposed authentication protocol on the computation cost by the comparisons. We choose Yang *et al.*'s protocol [4] and He *et al.*'s protocol [5] as comparison. The reason why we choose these two protocols is that both of them are in the mobile user-foreign server model, where the home server of the mobile user does not participate in the roaming authentication. Note that we do not take the symmetric key processing time, cryptographic hash operation time and MAC operation time into consideration since they are negligible compared with that of ECSM (Elliptic Curve Scalar Multiplication) operation and pairing operation. **Table 2** shows the computation costs of different protocols for roaming networks. The computation costs of ECSM and pairing operations on 200MHz and 1GHz mobile devices are shown in Table 3 [4]. By using the results in Table 3 we can illustrate the detailed computation costs of the related protocols on the mobile user side in **Fig. 8** and **Fig. 9**. From **Fig. 8** and **Fig. 9** we can see, the proposed protocol is not efficient compared with He *et al.*'s protocol [5] in 200MHz mobile device. However, it is more efficient than He *et al.*'s protocol in 1GHz mobile device. Since the processor of the mobile device is more and more fast, our protocol will be more efficient than He *et al.*'s protocol. **Table 4** shows some other performance metrics considered in wireless networks. Here we assume q=160 bits, the elliptic curve points is 160 bits and the hash operation, MAC operation and encryption/decryption operation are 128 bits. The identities of all participants are 4 bytes and the time stamp is 2 bytes. From **Table 4** we can see He *et al.*'s authentication protocol [5] has better performance on communication rounds and communication cost than Yang *et al.*'s protocol [4] and ours. However, the reason is that there is no confirmation message from the user to the server. In such case the server can not determine whether the mobile user has completed the authentication and computed the session key. Meanwhile, the forward security cannot be achieved in [5] which may cause the problem of the key exposure. So based on an overall consideration of efficiency and security, our protocol has good performance compared with the protocols mentioned above.

Table 2. Computation costs of different protocols for roaming network

Cryptography Operation	**Entity**	**Protocol of [4]**	**Protocol of [5]**	**Our protocol**
ECSM	U	8.75m	1m	4m
	F	9m	1m	4m
Pairing	U	3p	1p	0
	F	5p	2p	0
Total of U or F	U	3p+8.75m	1p+1m	4m
	F	5p+9m	2p+1m	4m
Total of U and F	U+F	8p+18.25m	3p+2m	8m

Table 3. Computation costs of ECSM and pairing operations on different mobile devices

Time	**200MHz Processor**		**1GMHz Processor**	
	ECSM	Pairing	ECSM	Pairing
Time(ms)	23	38	2	11

Table 4. Some other performance metrics

Performance Metrics	**Protocol of [4]**	**Protocol of [5]**	**Our protocol**
Communication rounds	3	2	3
Mutual authentication	Yes	Yes	Yes
Forward security	Yes	No	Yes
Communication cost(byte)	⩾256	58	88

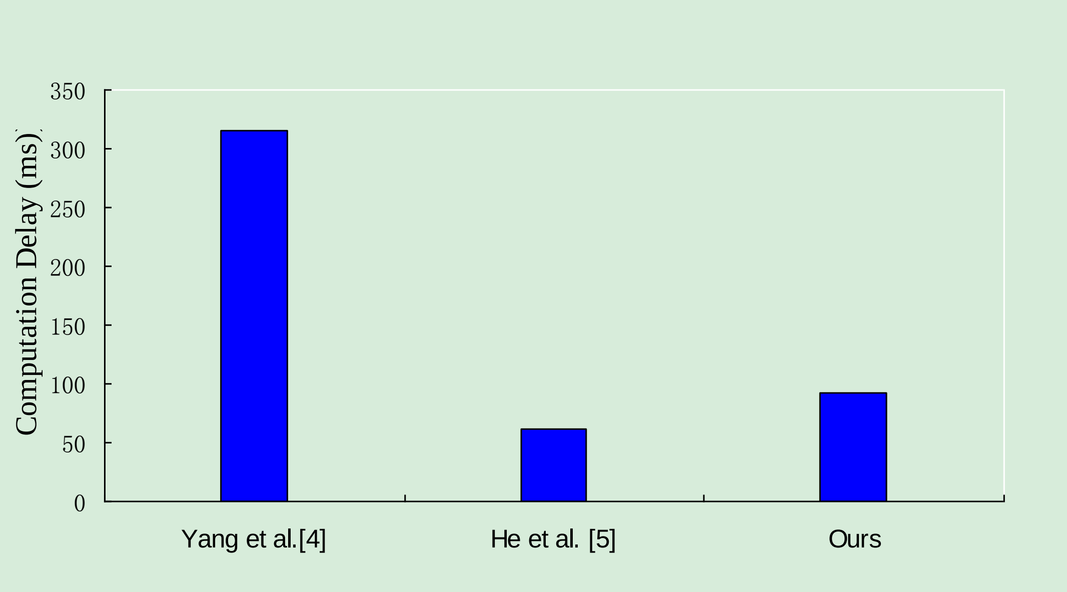


Fig. 8 Computation delay on 200MHz mobile device

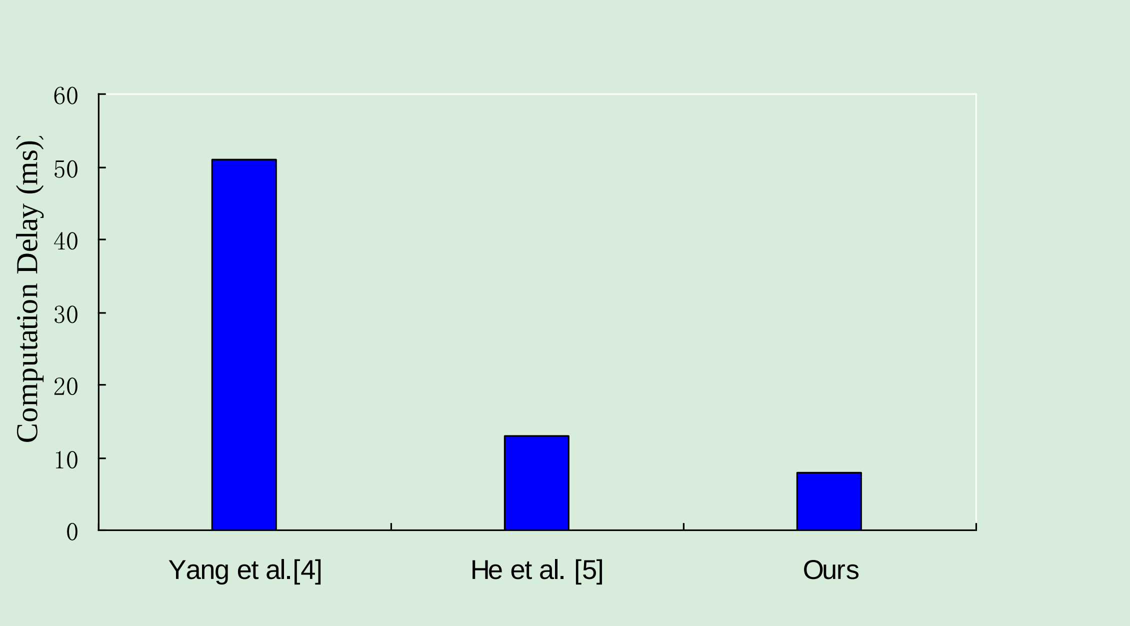


Fig. 9. Computation delay on 1GHz mobile device

7. Conclusion

In this paper we propose a new roaming authentication framework for wireless communication using the ID-based cryptography. The new roaming authentication protocol in the new framework does not need the home server's participation. It has good performance compared with related authentication schemes in wireless networks. Moreover, we also give two extensions of the roaming authentication protocol. On the one side, it provides strong anonymity for the mobile user, on the other side, it gives a user-to-user authentication protocol which expands the application of the new framework. The trick used in this paper can be applied to various kinds of wireless networks such as Cellular Networks, Wireless Mesh Networks and Vehicle Networks. Our further work will be on solving the problems of user revocation and DoS (denial of service) in our framework which are two fundamental problems in wireless communication.

References

[1] W.B. Lee and C.K. Yeh, "A new delegation-based authentication protocol for use in portable communication systems," *IEEE Transaction on Wireless Communications*, vol. 4, no.1, pp. 57-64, January, 2005. Article (CrossRef Link)

[2] M. Zhang and Y. Fang, "Security analysis and enhancements of 3GPP authentication and key agreement protocol," *IEEE Trans. Wireless Commun.*, vol. 4, no. 2, pp. 734–742, 2005. Article (CrossRef Link)

[3] Q. Jing, Y. Zhang, A. Fu and X. Liu, "A privacy preserving handover authentication scheme for EAP-based wireless networks," in *Proc. of IEEE GLOBECOM*, pp. 1-6, December 5-9, 2011. Article (CrossRef Link)

[4] G. Yang, Q. Huang, D. S. Wong and X. Deng, "Universal authentication protocols for anonymous wireless communications," *IEEE Transaction on Wireless Communications*, vol.9, no.1, pp. 168-174, January, 2010. Article (CrossRef Link)

[5] D. He, C. Chen, S. Chan and J. Bu, "Secure and efficient handover authentication based on bilinear pairing functions," *IEEE Transaction on Wireless Communications*, vol. 11, no. 1, pp. 48-53, January, 2012. Article (CrossRef Link)

[6] European Telecommunications Standards Institute (ETSI), GSM 2.09: Security aspects. http://www.etsi.org/deliver/etsi_gts/04/0403/05.02.00_60/gsmts_0403v050200p.pdf

[7] I. Akyildiz, X. Wang and W. Wang, "Wireless mesh networks: a survey," *Computer Networks*, vol.47, no.4, pp. 445-487, March, 2005.Article (CrossRef Link)

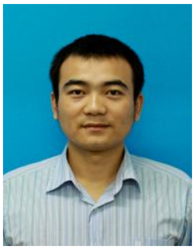
[8] R. Lu, X. Lin, X. Liang and X. Shen, "A dynamic privacy-preserving key management scheme for location-based services in VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol.13, no. 1, March, 2012. Article (CrossRef Link)

[9] Y. Jiang, C. Lin, X. Shen and M. Shi, "Mutual authentication and key exchange protocols for roaming services in wireless mobile networks," *IEEE Transaction on Wireless Communications*, vol.5, no.9, pp. 2569-2576, September, 2006. Article (CrossRef Link)

[10] C. Tang and D.O. Wu, "An efficient mobile authentication scheme for wireless networks," *IEEE Transaction on Wireless Communications*, vol.7, no.4, pp. 1408-1416, April, 2008. Article (CrossRef Link)
[11] C.C. Chang and H.C. Tsai, "An anonymous and self-verified mobile authentication with authenticated key agreement for large-scale wireless networks," *IEEE Transactions on Wireless Communications*, vol. 9, no.11, pp. 3346-3353, November, 2010. Article (CrossRef Link)
[12] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. of CRYPTO*, pp. 47-53, August 19-22, 1984. Article (CrossRef Link)
[13] S.L.Ng and C. Mitchell, "Comments on mutual authentication and key exchange protocols for low power wireless communications," *IEEE Communication Letters*, vol. 8, no.4, pp. 262-263, April, 2004. Article (CrossRef Link)
[14] AVISPA v1.1 User Manual, 2006. http://www.avispa-project.org/
[15] D. Basin, S. Mödersheim and L. Viganò, "An on-the-fly model-checker for security protocol analysis," in *Proc. of Esorics*, pp. 253-270, October 13-15, 2003. Article (CrossRef Link)

Xiaowei Li received his B.S. in Department of Applied Mathematics from Xidian University, China, in 2008. He is currently a Ph.D. candidate in Department of Communication Engineering, Xidian University, China. He has joined in State Key Laboratory of Integrated Services Networks, in Xidian University. He has published several papers in International Journals and conferences including Security and Communication Networks and Globecom. His research interests include provable security, network protocol security and wireless network security.

Yuqing Zhang is a professor and supervisor of Ph.D. candidates of Graduate University of Chinese Academy of Sciences. He received his B.S. and M.S. degree in computer science from Xidian University, China, in 1987 and 1990 respectively. He received his Ph.D. degree in Cryptography from Xidian University in 2000. He is a member of IEEE Communications Society and IEICE Transactions on Communications. He has published lots of papers in International Journals and conferences including IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Wireless Communications, IEEE Communications Letters, Globecom, RAID and so on. His research interests include cryptography, information security and network protocol security.



Xuefeng Liu received his B.Sc in information security from Xidian University, China, 2007. He has joined in 2007 for his M.Sc and Ph.D in Xidian University. His research interests include wireless network security, cloud computing, mobile computing and applied cryptography.

Jin Cao received the B.Sc. degree from Xidian University, China, in 2008. He is currently working toward the Ph.D. degree in Cryptography, Xidian University, China. His interests are in wireless network security and LTE networks.

Qianqian Zhao received her B.Sc in information and computing science from Henan University, China, 2009. She has joined in 2010 for her M.Sc and Ph.D in Xidian University. Her research interests include wireless network security, cloud computing, mobile social networking and applied cryptography.