Proficient Secrecy Roaming Conserving Security in Wireless Mobile Networks

T.K.Raajeshwari¹ Ms. N. Gugha Priya²
¹PG Scholar ²Assistant Professor
²Department of Computer Science and Engineering ²Department of Information Technology
¹,²Kalaignar Karunanidhi Institute of Technology, Coimbatore, India

Abstract— Increasing number of mobile users is being allowed to use wireless mobile network services where the roaming service provides the constant services to a network without breaking the connection. Ensuring security in roaming service is a great challenge. In the absence of home server the inter-domain security should be established which makes it feasible for mobile users to move into the foreign domains. An authentication mechanism is required between the mobile users and the foreign server which supports the highly secured communication in wireless networks. In addition maintaining the privacy of the mobile user is an important requirement such as the information about behavior of the user who needs the roaming service. The participations of home attendants have engrossed significant interest to its stimulus on the communication proficiency. Formal protocols incur high communication and computation cost. The proposed protocol that has a novel three-round architecture which uses a pseudo-identity based signcryption scheme to perform efficient revocation with short revocation list and the authentication efficiency is higher than that of existing protocols. To provide the better computation efficiency and lightweight storage efficiency this scheme does not require the highest computational cost on the roaming user. A detailed analysis and overhead evaluation on a number of performance metrics such as a computation cost and time is given to validate the performance of the proposed protocols.

Keywords: user privacy, anonymous authentication, secure roaming services, signcryption, wireless mobile networks.

I. INTRODUCTION

With the advancement of wireless technologies the user mobility is highly attractive trait in the development of computer networks and telecommunication systems. In some situation the mobile users who initially subscribed to their home networks can travel to other networks with different need of access services. This scenario is called roaming is a prominent service which refers to the ability for the user to make and receive calls, to send and receive messages and to access other services when travelling beyond their home network by means of using the foreign network. The roaming service helps an individual to be kept connected to the network without being limited by the geographical coverage of their own home network. A typical roaming service involves three parties such as a roaming user, a foreign or visited server and a home server where the roaming user is a subscribed user of the home server. In addition the authentication mechanism is needed for the protected roaming service. This mechanism is to identify the legal roaming user who requests the service in the foreign domain. In the meantime the foreign server also must authenticate the user who is originally requested for the service. The location privacy of the user should be protected because no one including the foreign server is able to access the past history of the user. A privacy preserving authentication scheme should satisfy the following properties [5]:

1) Server authentication: the user assured about the identity of a foreign server.
2) Subscription validation: a foreign server assured the identity of the roaming user of the home server.
3) Key establishment: the user and the foreign server establish the random session key which does not known to the home server.
4) User anonymity: besides the user and its home server, no one including the foreign server can tell the identity of the user.
5) User untraceability: besides the user and its home server, no one including the foreign server could be able to access the past protocol runs of the same user.

Among these properties, the subscription validation is the one, which is most difficult to obtain. When user revocation is maintained in the authentication protocol, it is more difficult to achieve user untraceability since the information is given to the foreign server to recognize the revoked user. On the other hand the information to the foreign server should not be able to access the users past history. To overcome this problem the revocation should be unlinkable and anonymous. Furthermore, the secured protocol for roaming service should be proven in Canetti-Krawczyk model which is used to analyze the key agreement between the home server and the foreign server. The keys which are used in the agreement should be protected from the adversary.

Fig. 1: The three-party roaming scenario

Paper organization. In the forth coming session we review the related works on secure roaming. Security and weakness of the mobile authentication is provided in Sec. II. In Sec. III the proposed system model is explained. In Sec. IV the experimental results of the system modules are discussed. Finally the Sec V concludes the proposed protocol.
II. SECURITY AND WEAKNESS OF THE MOBILE AUTHENTICATION

The traditional wireless mobile networks of AAA provide the authentication, authorization and accounting services to the mobile users. The roaming protocol[1] could be classified into two types: three-party roaming protocol which involves a home server, a foreign server and a roaming user and two-party roaming protocol which does not involve the home server. The fig.1 shows the three-party roaming protocol structure. This protocol required at least four rounds of message flow between the three parties since minimum two rounds are needed for a foreign server to obtain the initial authentication information about the roaming user from the home server. In addition an authentication process in the three party roaming protocols is inclined by the state of home server which can be a bottleneck that leads to the high computational time and a single point of failure. There is no security provided for the initial communication connection establishment between the foreign server and the home server. This may lead to the resource depletion attack on the foreign server by an adversary. In the two-party roaming protocol the home server does not participate in the communication. Yang et al [7] considered two levels of user anonymity in roaming service.

Yang et al[7] proposed two protocols; the first is the three-party roaming protocol which satisfies all the five properties mentioned above but does not support the strong user anonymity. The second protocol is two-party roaming protocol with strong user anonymity which is based on the bilinear pairing operation. This protocol incurs high computational cost to generate the group signature. And also it does not provide the backward unlinkability. He et al.[1] proposed a roaming protocol based on the group signature with backward unlinkability. This protocol also involves high roaming authentication cost at the roaming user. To provide efficiency, lightweight protocol based on the symmetric key encryption algorithm and hash function is used. In this protocol the home server is involved which does not provide the backward unlinkability. The second lightweight protocol[7] based on the bilinear pairing operation also depends on the assistance of home server. He et al.[9] proposed another protocol based on pseudo-identity using bilinear pairing with cryptographic operation which does not secure the private and session key of the roaming user from the eavesdropper.

As reviewed all the existing roaming protocols mentioned above shows that the two party roaming protocols proposed earlier does not provide the reasonable anonymous authentication. In this paper the proficient secrecy roaming protocol which overcomes all the above weakness and provide greater security in the roaming service and simulates the calls rate obviously lesser than that of existing protocols. The performance of the communication cost and computational cost will be optimized.

III. PROPOSED SYSTEM

In this section, we propose a signcryption-based roaming system, which mainly consists of two phases, i.e., an initial process phase and an anonymous roaming system phase. The overview of the proposed architecture is shown in the Fig 2.

![Fig. 2: The proposed architecture](image)

<table>
<thead>
<tr>
<th>Roaming Protocols</th>
<th>No. of Rounds</th>
<th>Home Server</th>
<th>Anonymity</th>
<th>Computational cost</th>
<th>CK Model</th>
<th>Backward Unlikability</th>
</tr>
</thead>
<tbody>
<tr>
<td>H.J. Protocol 11</td>
<td>3</td>
<td>offline</td>
<td>Weak</td>
<td>Low Cost</td>
<td>Secure</td>
<td>Provided</td>
</tr>
<tr>
<td>G.Y. Protocol 1</td>
<td>3</td>
<td>offline</td>
<td>Strong</td>
<td>Low Cost</td>
<td>Secure</td>
<td>Not Provided</td>
</tr>
<tr>
<td>G.Y. Protocol 2</td>
<td>3</td>
<td>offline</td>
<td>Strong</td>
<td>2T_{par}</td>
<td>Secure</td>
<td>Not Provided</td>
</tr>
<tr>
<td>G.Y. Protocol 8</td>
<td>4</td>
<td>online</td>
<td>Strong</td>
<td>-</td>
<td>Not Secure</td>
<td>Provided</td>
</tr>
<tr>
<td>D.H. Protocol 11</td>
<td>3</td>
<td>offline</td>
<td>Strong</td>
<td>High Cost</td>
<td>Not Secure</td>
<td>Provided</td>
</tr>
<tr>
<td>D.H. Protocol 12</td>
<td>2</td>
<td>offline</td>
<td>Strong</td>
<td>Not Provided</td>
<td>Not Secure</td>
<td>Provided</td>
</tr>
<tr>
<td>C.C. Protocol 10</td>
<td>4</td>
<td>online</td>
<td>Strong</td>
<td>-</td>
<td>Not Secure</td>
<td>Not Provided</td>
</tr>
<tr>
<td>H.Z. Protocol 12</td>
<td>4</td>
<td>online</td>
<td>Strong</td>
<td>-</td>
<td>Not Secure</td>
<td>Provided</td>
</tr>
<tr>
<td>Q.H. Protocol 12</td>
<td>3</td>
<td>offline</td>
<td>Not Provided</td>
<td>Low Cost</td>
<td>Not Secure</td>
<td>Not Provided</td>
</tr>
</tbody>
</table>

Table 1: Comparison of the number of roaming protocols
A. Overview

HS first performs the initial process phase which is composed of an HS setup step, a roaming agreement step and a registration of RU step for preparation of roaming service.

In the HS setup step, HS generates its own public parameters and secret values. Upon completing the HS setup step, the roaming agreement step and the registration of RU step are conducted to issue secret values of FSs and RUs. The anonymous roaming system phase consists of a roaming protocol step and a revocation step. Finally, the calls rate at the roaming user is simulated in the foreign server where the user can get the services as of in HS.

B. HS Setup

In the home server setup phase the following process is presented. Choose a master secret key \( s \) \( \leftarrow \mathbb{Z} \) *p and compute a public key \( Q_{pub} = sQ \in G2 \) and a roaming key \( RK_{FSi} = H1(IDHS) + sQ \in G2 \). (RKHS is the HS’s secret Value).

The public parameters are Param:\n\n\{G1,G2,GT,\epsilon,P,Q,Q_{pub},\psi,H1,H2,H3,H4,H5,H5,\text{key}\}.

C. Roaming Agreement

When the HS completes its setup process, it establishes a roaming agreement to generate the roaming keys of each FS.

- All FSs send their identity IDFSi to the HS.
- The HS computes a roaming key
\[ RK_{FS_i} = \frac{1}{H1(IDFS_i)} \cdot Q \in G2 \text{ for } FS_i. \]
- The HS sends \( RK_{FS_i} \) to FSi through a secure channel.

D. Registration of RU

- RUi in the HS domain sends its own IDi to the HS via a secure channel.
- The HS generates a random value Seedi and a revocation value \( rvi \) that is used as a key of \( H5, \text{key} \), and produces keyed hash chain values. The length of the chain is \( K \).
- The HS computes private keys for RUi, that are associated with the pseudo-identities,
\[ s_{i,j} = H1(PID_{i,j}) + sQ \in G2(1 \leq j \leq K) \]
- The HS sends \( PID^* i \) and \( s^* i \) generated in previous steps to RUi via a secure channel. Roaming Protocol FSi computes \( r1 = e(T1, RK_{FS_i}) \). It then performs decryption \( MRU_i = C1 \oplus H4(r1) \) and computes \( h = H2(MRU_i) \), \( r1 \). Subsequently, FSi verifies the received messages using the following formula.
\[ r1 = e(S1,H1(PID_{i,j}Q + Q_{pub})g+h. \]

1. Proof

LHS
\[ = e(T1, RK_{FS_i}) \]
\[ = e(x1(H1(IDFS_i)P + sP), 1 / H1(IDFS_i) + sQ) \]
\[ = e(x1(H1(IDFS_i) + sP), 1 / H1(IDFS_i) + sQ) \]
\[ = e(P,Q)x1 = gx1 \]

RHS
\[ = e(S1,H1(PID_{i,j}Q + Q_{pub})g+h) \]
\[ = e((x1+h)\psi(s_{i,j}), H1(PID_{i,j}Q + Q_{pub})g+h) \]
\[ = e((x1+h)\psi(H1(PID_{i,j})+sQ), (H1(PID_{i,j}) + s)Q)g-h \]
\[ = e(x1+hH1(PID_{i,j})+sP, (H1(PID_{i,j}) + s)Q)g-h \]
\[ = e(P,Q)(x1+h)g-h = g(x1+h)g-h = gx1 \]

E. Revocation

In our revocation process, two algorithms are used. Algorithm updates the revocation list by using a new revocation list sent by the HS. Algorithm 2 performs the revocation checking process when RUi sends requests or roaming services to FSs. The detailed steps are as follows.

- The HS checks the current time interval index \( t_j \) to prevent the revoked RU from accessing all FSs after \( t_j \). Next, it computes \( RevInfo_{tj} = H t_j , rvi \) (Seedi) and sends a revocation list \( RL_{tj} \) containing the revocation information \( RevInfo_{tj} , rvi \) and \( t_j \) to all FSs.
- After receiving RL\( t_j \), all FSs update \( RevInfo_{tj} \) \( t_j \) \( \in \) RL\( t_j \).

\[ RevInfo_{tj} = H5,rvi (RevInfo_{tj},t_j) \]

F. Simulating calls rate

In this module the calls rate of the roaming user is simulated as it is provided in their home networks. The user’s service cost is displayed in the foreign networks where the user can use the services as same as they get in their home networks.

![Image](Fig_3.png)

Fig. 3: Comparison cost of authentication at RU
IV. EXPERIMENTAL RESULT

On comparing our protocol with three other protocol. The proposed anonymous roaming protocol which is based on PBC and OpenSSL (the open source toolkit for SSL/TSL) to check the feasibility for use in an actual end user mobile device. The run-time of an authentication algorithm on a mobile device should be less than 500ms. To evaluate the performance of our library, running of each function is performed through the test of library. The average running time of this test is far less than the 500ms.

V. CONCLUSION

Thus various protocols for providing security in the roaming services have been reviewed. The existing systems in which the three-party roaming protocols require the participation of home server whereas the two-party roaming protocol has low security. However the proposed work is focused on an anonymous roaming protocol using signcryption. It includes an efficient anonymity authentication process and a fast revocation process.

REFERENCES