

An Anonymous Roaming Protocol Based on Group Signature without Communication with Home Server

Chih-Hung Wang¹ and Wan-Yu Tsai²

Department of Computer Science and Information Engineering
National Chiayi University, ChiaYi, Taiwan, ROC
wangch@mail.ncyu.edu.tw¹, wytsai96@mail.csie.ncyu.edu.tw²

Abstract. Wireless communication was used in our life for no limits of geography and space mainly due to the convenient capability of roaming. Roaming means a user, belonging to the home agent, wants to travel to another region and request the visited server for services. The visited server generally verifies a user through the home server in the previous literature. In this paper, by using the group signature technique, a novel authentication protocol was proposed in which the visited server can verify users without connecting to users' home server. As the non-repudiation and untraceability can be achieved by the group signature, the proposed protocol also can provide user anonymity. Further, the proposed protocol can resist replay attacks and DoS attacks by the property of hash chains.

Keywords: group signature, roaming protocol, anonymity, wireless communication.

1 Introduction

Wireless LAN (WLAN for short) [1] provides the roaming service for the users. Typically, WLAN uses the modest authentication to check users' identities and chooses SIM (Subscriber Identity Module) based roaming [1][7] to manage the memberships. There are three roles in roaming structure: roaming user, home server (*HS*) and visited server (*VS*). Each user needs to register at the *HS* in the setup stage (see Fig. 1(a)). The roaming user registered at the home server can be verified as a valid user and use similar services when he roams to the foreign area controlled by another server (see Fig. 1(b)). In GSM (Global System for Mobile Communications) roaming, the visited server needs to transmit the billing information and the records of requested services to the home server of users [3].

In general, before providing services to the roaming users, *VS* needs to verify the identities of them by connecting to *HS*. Many previous papers have proposed this kind of model as shown in Fig. 2(a). However, the communication cost is quite expensive in the wireless environment. We proposed a roaming protocol in which *VS* can verify the roaming users without connecting to their *HS*'s (see Fig. 2(b)). The technique we employ is a group signature, since it has many nice properties such as anonymity,

untraceability and unlinkability. The proposed roaming protocol also satisfies all security requirements of roaming system proposed by the previous works.

The basic idea of the proposed roaming protocol is to employ the group signature to achieve user anonymity. The group here means the registered users belonging to a specific home server. Each user can generate the group signature and present it to the visited server in roaming. The visited server can only know the identity of the group the user belongs to, but cannot learn the genuine identity of the user, thus the proposed protocol achieves anonymity of the user. In order to prevent the malicious user from taking misbehavior, the home server can, if necessary, use his own secret key to reveal the actual identity of user to achieve conditional traceability.

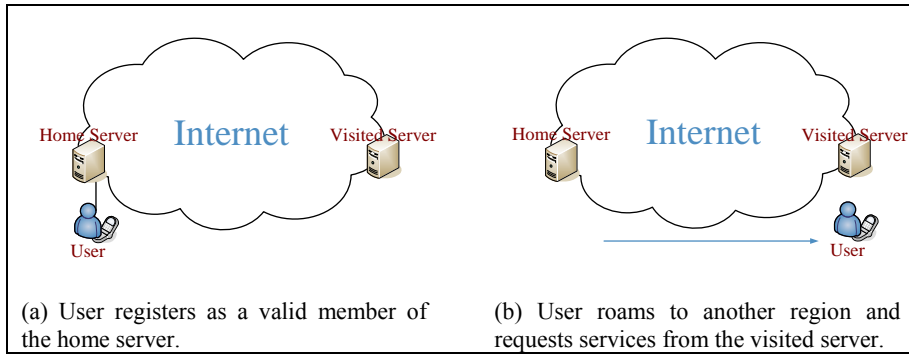


Fig. 1. The diagram of roaming system

The goal of this paper is to reduce the communication time in verifying the roaming user. The delay of the roaming system consists of not only data encapsulation and decapsulation but also the transmission time in communication. If the distance between *HS* and *VS* is too far, the user must spend much time to wait the packet transmissions at routers or switches. The proposed protocol takes time on the computation of user's device, but reduces the transmission time on the communication between *VS* and *HS*. Hence, the critical contribution of the proposed protocol is to reduce both the communication time and security threats between *HS* and *VS*.

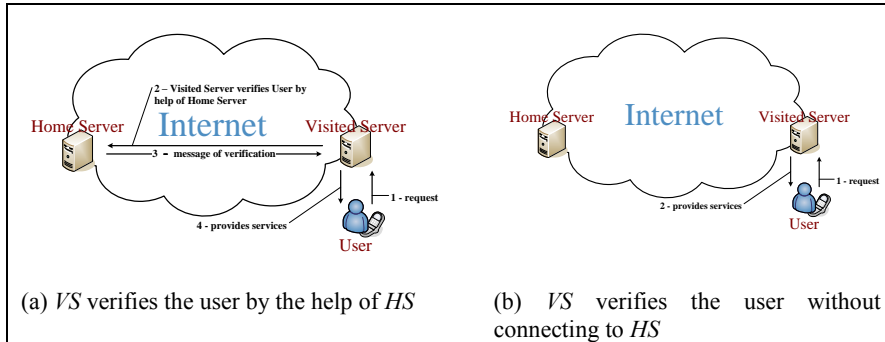


Fig. 2. The comparison of previous protocol and our proposed protocol

The remains of this paper are organized as follows: the related work is shown in Section 2 to describe the previous literature of roaming protocol and the applications of group signature; Section 3 describes the proposed roaming scheme which can skillfully reduce the communication cost. The security of the proposed scheme is shown in Section 4 and finally, we conclude this paper by giving the directions for future researches in Section 5.

2 Related Work

The group signature means a type of signature in which (only) the members can sign the messages on behalf of the group; the verifiers can verify the validity of the signature but cannot learn who made it. The group signature has some core properties including non-repudiation, unforgeability, anonymity, untraceability, unlinkability and revocability. In 2004, Miyaji and Umeda [11] designed a group signature to achieve the property of unlinkability that means two different group signatures that the same user generates cannot be identified and linked together by anyone except for the group manager. If a member leaves the group, his identity information will be deleted through the revocation protocol by the group manager.

The scheme of [11] also can achieve the property of unlinkability. That means that no one except for group manager (*GM*) can identify two difference group signatures signed by the same user. Moreover, Miyaji and Umeda's scheme is based on the zero-knowledge proof named *SPK* (a signature based on a zero-knowledge proof of knowledge). The proof statement " $SPK\{(\alpha_1, \dots, \alpha_n) : Predicates\}$ " [6] is for the signer to prove that he is a valid member to *GM*. The secret information $\alpha_1, \dots, \alpha_n$ are generated by the signer and are known only to the signer. The signed contents are computed by using $\alpha_1, \dots, \alpha_n$ and satisfying *Predicates*.

Fujii et al. [8] proposed a protocol for subscription services to achieve anonymity by using group signature. The subscriber (member P_i) has to register at services manager (*SM*), and then he can request service at distributor (*ICD*). The scenario of subscription service is similar to the roaming system; that means we can regard the subscribers as the roaming user, *SM* as the home server, and the distributors as the visited servers. In the proposed protocol, *ICD* does not need to connect to *SM* to verify P_i . However, the group signature in [8] is linkable thus it cannot achieve full anonymity. When P_i requests a service, he sends his identification ID_i to *ICD* through internet that causes everyone can trace the activities of the subscriber.

Wan et al. [14] in 2008 proposed a roaming protocol by using two-layer hierarchical ID-based cryptosystem [4][9] to achieve that *VS* can verify the roaming user without connecting to user's *HS*. Nevertheless, the roaming protocol in [14] needs an on-line Trust Third Party (*TTP*) to manage and distribute the (domain) secret keys for all servers.

3 The Group Signature-based Anonymous Roaming Protocol

First, we review the security requirements of roaming protocol. Second, we describe the five phases: setup phase, registration phase, authentication and billing phase, revocation phase and tracing phase in our proposed roaming protocol in details. The first phase is for the home server to setup basic information. The second phase is for the user to register at his home server and obtain some secret information in order to roam to another server who offers services. The third phase is for the visited server to verify the user. The visited server will perform billing after it confirms that the user is legitimate. The fourth phase is for the member who is leaving the home server or revoked by the home server. The fifth phase is for the home server to trace the user about his history records.

3.1 Security Requirements

Some security requirements of roaming protocol are listed as follows.

User anonymity: No one can identify the roaming user expect for user's *HS*.

Untraceability: No one can trace user's records expect for user's *HS*. For protecting user's privacy, the identity and related secret information of the user cannot be revealed.

Confidentiality: Only authorized parties (*HS* or *VS*) can obtain user's communication history.

Integrity: No one expect for the authorized party, user, *HS* and *VS*, can modify the message content.

Authentication: The user can request services from *VS* only if *VS* confirms the legitimacy of the user.

Resisting DoS attack: When suffering from DoS attacks, the authentication messages shared between the two parties (user and server) may be inconsistent. That causes a legitimate user to fail in requesting services from the server.

Resisting replay attack: An active adversary cannot succeed in verification by replaying the past authentication messages generated by some legitimate users.

Forward secrecy: The roaming protocol has to ensure that the previous history and secret information of the user cannot be disclosed even though the long-term keys or current session keys are compromised.

3.2 The proposed protocol

The proposed protocol is based on the group signature from [11] and the hash chain technology. The detail procedures are described below.

Phase I : Setup Phase

In the following steps, *HS* generates his secret key and public key and then announces his public key and identity to everyone.

- Choose two random primes p and q , where the size of q is k -bits and $q | (p-1)$, and then set P to be $p \times q$.

- Choose another prime Q , where $P \mid (Q-1)$.
- Randomly choose $g_1, g_2, g_3, g_4 \in G_P$, and $h \in G_Q$.
- Choose a random secret key $x_{HS} \in Z_q$ to compute $y_1 = g_1^{x_{HS}} \bmod P$ and $y_2 = g_3^{x_{HS}} \bmod P$.
- Publish the public key $Y = \{q, P, Q, g_1, g_2, g_3, g_4, h, y_1, y_2, ID_{HS}\}$, where ID_{HS} denotes home server's identity.

Phase II : Registration Phase

In this phase, the user U_i registers as a member to the home sever. U_i chooses a secret key x_i to compute $z_i = g_2^{x_i} \bmod P$, $z_j = h^{x_i} \bmod Q$ and $\sigma_i = SPK\{(\alpha) : z_i = g_2^\alpha \bmod P \wedge z_j = h^\alpha \bmod Q\} = (c, s)$, and then sends them to HS (see Fig. 3). U_i constructs σ_i by choosing random exponents r and computes $c = H(g_2 \parallel h \parallel z_i \parallel z_j \parallel t_1 \parallel t_2 \parallel m)$ and $s = r - cx \bmod q$, where $t_1 = g^r \bmod P$, $t_2 = h^r \bmod Q$. HS checks the validity of σ_i by the equation $c = H(S \parallel V \parallel m)$ with $S = g \parallel h \parallel z_i \parallel z_j$ and $V = g^s z_i^c \parallel h^s z_j^c$. If the verification passes, HS randomly selects w_i to compute $A_i = z_i g_1^{-w_i} \bmod P$ and $b_i = w_i - A_i^{x_{HS}} \bmod q$. HS adds (ID_i, A_i, b_i) in the member list, and sends ID_{HS} and (A_i, b_i) to U_i . U_i then checks whether the equation $A_i y_1^{A_i} g_1^{b_i} \bmod P = z_i$ holds. If yes, U_i stores up the tuple (z_i, A_i, b_i, ID_{HS}) in his device.

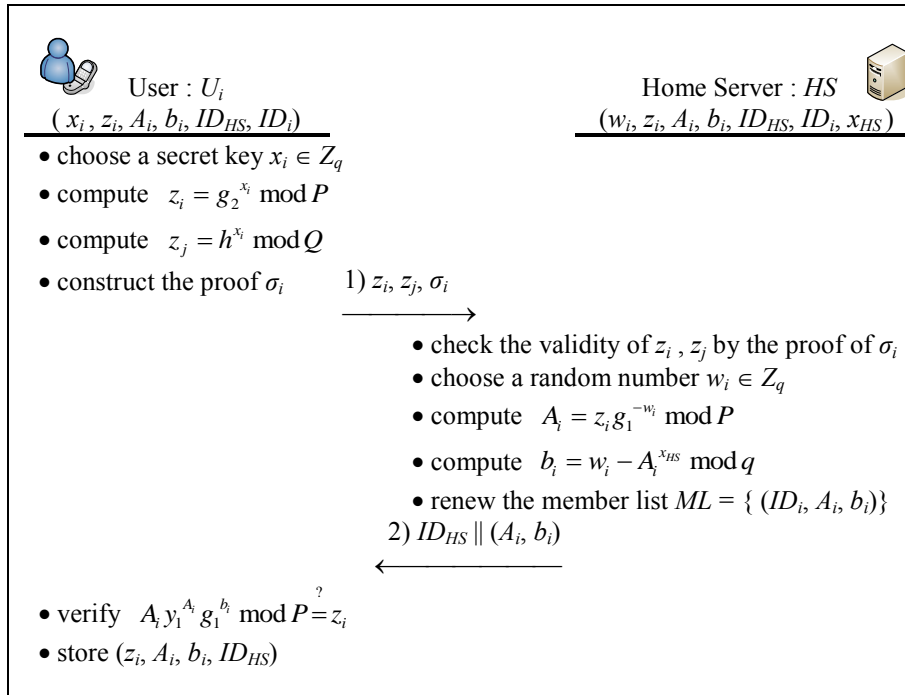


Fig. 3. Registration phase of the proposed roaming protocol

Phase III-A: Authentication and Billing Phase (The user roams to the visited server for the first time or $v = 1$)

When U_i roams to the visited server VS , VS cannot check the validity of U_i . In the previous literature, VS needs to connect to HS . The proposed scheme gives a different approach; that means VS can verify the validity of U_i without connecting to HS . At the beginning of this phase, U_i has to confirm the newest g_4 of HS with the aid of VS because HS may update g_4 in the revocation phase (see **Phase IV**).

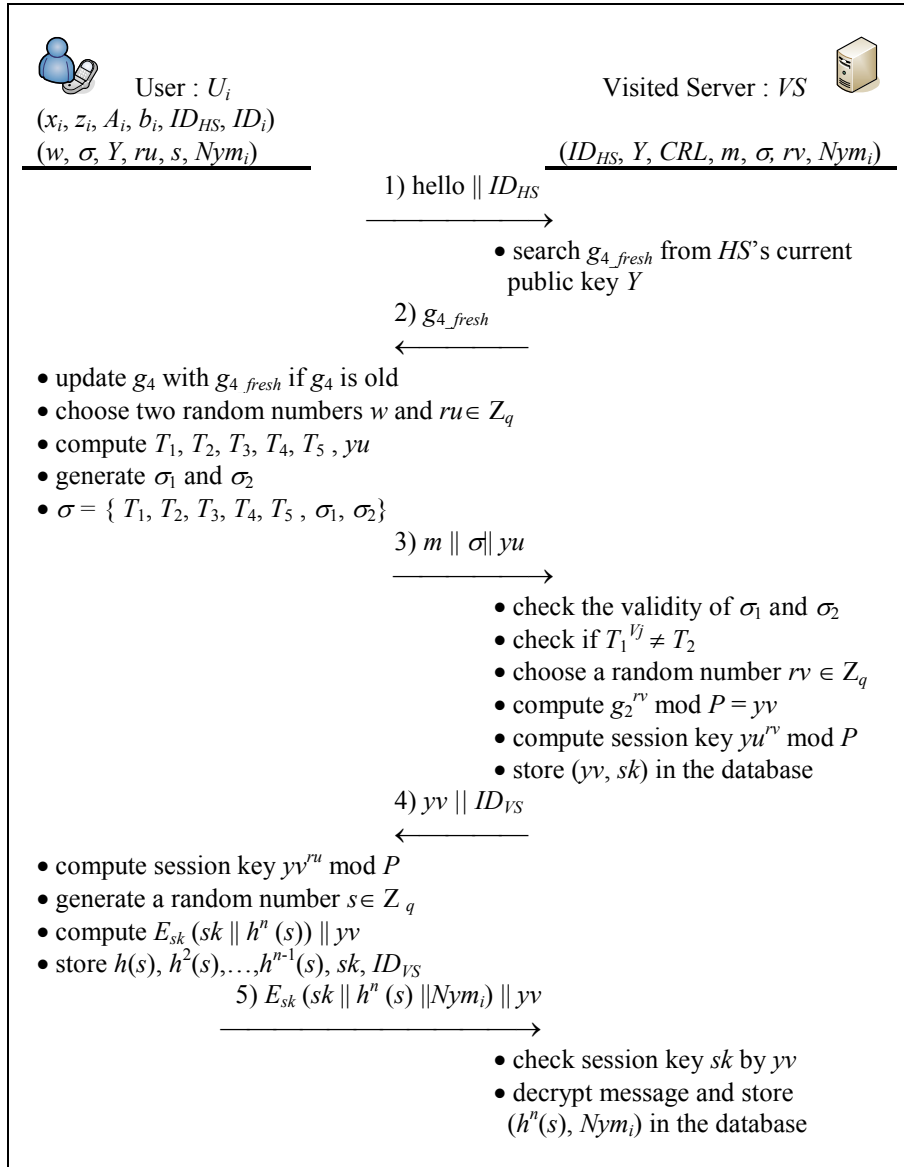


Fig. 4. Authentication and billing phase of roaming protocol

VS obtains g_4 from HS 's current public key $Y = \{q, P, Q, g_1, g_2, g_3, g_4, h, y_1, y_2, ID_{HS}\}$ and then sends g_{4_fresh} to the user. If the user finds that his g_4 is not the newest one, he must update g_4 with g_{4_fresh} . Next, VS checks the validity of U_i . U_i generates two random numbers w and ru to compute T_1, T_2, T_3, T_4, T_5 and yu by the following equations: $T_1 = h^{g_3^w} \bmod Q$, $T_2 = T_1^{g_4^{b_i}} \bmod Q$, $T_3 = g_3^{b_i} g_4^w \bmod P$, $T_4 = A_i g_3^w \bmod P$, $T_5 = y_2^w \bmod P$. U_i generates σ_1 and σ_2 by

$$\sigma_1 = SPK\{(\alpha_1, \alpha_2): T_1 = h^{g_3^{\alpha_2}} \bmod Q \wedge T_2 = T_1^{g_4^{\alpha_1}} \bmod Q \wedge T_3 = g_3^{\alpha_1} g_4^{\alpha_2} \bmod P\}(m) \\ = (c_1, s_{11}, \dots, s_{1k}, s_{21}, \dots, s_{2k}) \in \{0, 1\}^k \times \mathbb{Z}_q^{2k}, \text{ and}$$

$$\sigma_2 = SPK\{(\alpha_3, \alpha_4, \alpha_5, \alpha_6): \alpha_3 \in \mathbb{Z}_P \wedge T_3 = g_3^{\alpha_3} g_4^{\alpha_6} \bmod P \wedge T_4 = y_1^{-\alpha_3} g_1^{-\alpha_4} g_2^{\alpha_5} g_3^{\alpha_6} \bmod P \\ \wedge T_5 = y_2^{\alpha_6} \bmod P \wedge h^{T_4} = T_1^{\alpha_3} \bmod Q\}(m) = (c_2, s_3, s_4, s_5, s_6) \in \{0, 1\}^k \times \mathbb{Z}_q^3 \times \mathbb{Z}_P.$$

U_i constructs σ_1 by choosing random integers $\omega_{1j}, \omega_{2j} \in_R \mathbb{Z}_q$ for $1 \leq j \leq k$, and computing $t_{1j} = h^{g_3^{\omega_{2j}}} \bmod Q$, $t_{2j} = T_1^{g_4^{\omega_{1j}}} \bmod Q$, $t_{3j} = g_3^{\omega_{1j}} g_4^{\omega_{2j}} \bmod P$, $c_1 = H(g_3 \parallel g_4 \parallel h \parallel T_1 \parallel T_2 \parallel T_3 \parallel t_{11} \parallel \dots \parallel t_{1k} \parallel t_{21} \parallel \dots \parallel t_{2k} \parallel t_{31} \parallel \dots \parallel t_{3k} \parallel m)$, $s_{1j} = \omega_{1j} - c_1[j]b_i \bmod q$ and $s_{2j} = \omega_{2j} - c_1[j]w \bmod q$, for $1 \leq j \leq k$, where $c_1[j]$ is the j th bit of string c_1 . Then U_i chooses random integers $\omega_3 \in_R \mathbb{Z}_P$ and $\omega_4, \omega_5, \omega_6 \in_R \mathbb{Z}_q$ as $\alpha_3, \alpha_4, \alpha_5, \alpha_6$ to construct σ_2 by $t_4 = g_3^{\omega_4} g_4^{\omega_6} \bmod P$, $t_5 = y_1^{-\omega_3} g_1^{-\omega_4} g_2^{\omega_5} g_3^{\omega_6} \bmod P$, $t_6 = y_2^{\omega_6} \bmod P$, $t_7 = T_1^{\omega_3} \bmod Q$, $c_2 = H(g_1 \parallel g_2 \parallel g_3 \parallel g_4 \parallel h \parallel y_1 \parallel y_2 \parallel T_1 \parallel T_3 \parallel T_4 \parallel T_5 \parallel t_4 \parallel t_5 \parallel t_6 \parallel t_7 \parallel m)$, $s_3 = \omega_3 - c_2 A_i \bmod P$, $s_4 = \omega_4 - c_2 b_i \bmod q$, $s_5 = \omega_5 - c_2 x_i \bmod q$ and $s_6 = \omega_6 - c_2 w \bmod P$. U_i outputs a group signature $\sigma = \{T_1, T_2, T_3, T_4, T_5, \sigma_1, \sigma_2\}$. Next, U_i computes $yu = g_2^m \bmod P$ and then sends yu, m (including the requested services) and σ to VS . VS checks the validity of σ_1 and σ_2 and uses the revocation list published by $HS (ID_{HS})$ to check whether $T_1^{V_j}$ equals T_2 or not. If VS finds a certain V_j satisfies the equation, which means U_i has been revoked, then VS rejects the authentication; otherwise, VS generates rv to compute yv and session key $sk = yv^m \bmod P$ by Diffie-Hellman key exchange protocol. U_i also can compute $sk = yv^m \bmod P$ by using yv from VS , and then, Finally, U_i uses sk to encrypt the hash chain $h^n(s)$ and a pseudonym Nym_i and sends the encrypted message to VS . U_i stores sk, ID_{VS}, Nym_i and corresponding hash chains $\{h(s), h^2(s), \dots, h^{n-1}(s)\}$ into the device. When VS receives the message $E_{sk}(sk \parallel h^n(s) \parallel yv)$ from U_i , he decrypts the message to obtain the value of hash chain and Nym_i by using session key sk computed from yv . VS finally stores the values of hash chains and Nym_i in the database.

Phase III-B: Fast re-authentication phase (The user roams to the visited server after the first time ($v > 1$)).

After VS checks the validity of U_i by using group signature generated by U_i in Phase III-A, VS can get the hash chain $h^n(s)$ of U_i . When U_i roams to VS at the

second time, U_i uses the hash chain $h^{n-1}(s)$ in the protocol to show his validity (see Fig. 5). No one except U_i knows s to compute $h^{n-1}(s)$. Other people who obtain

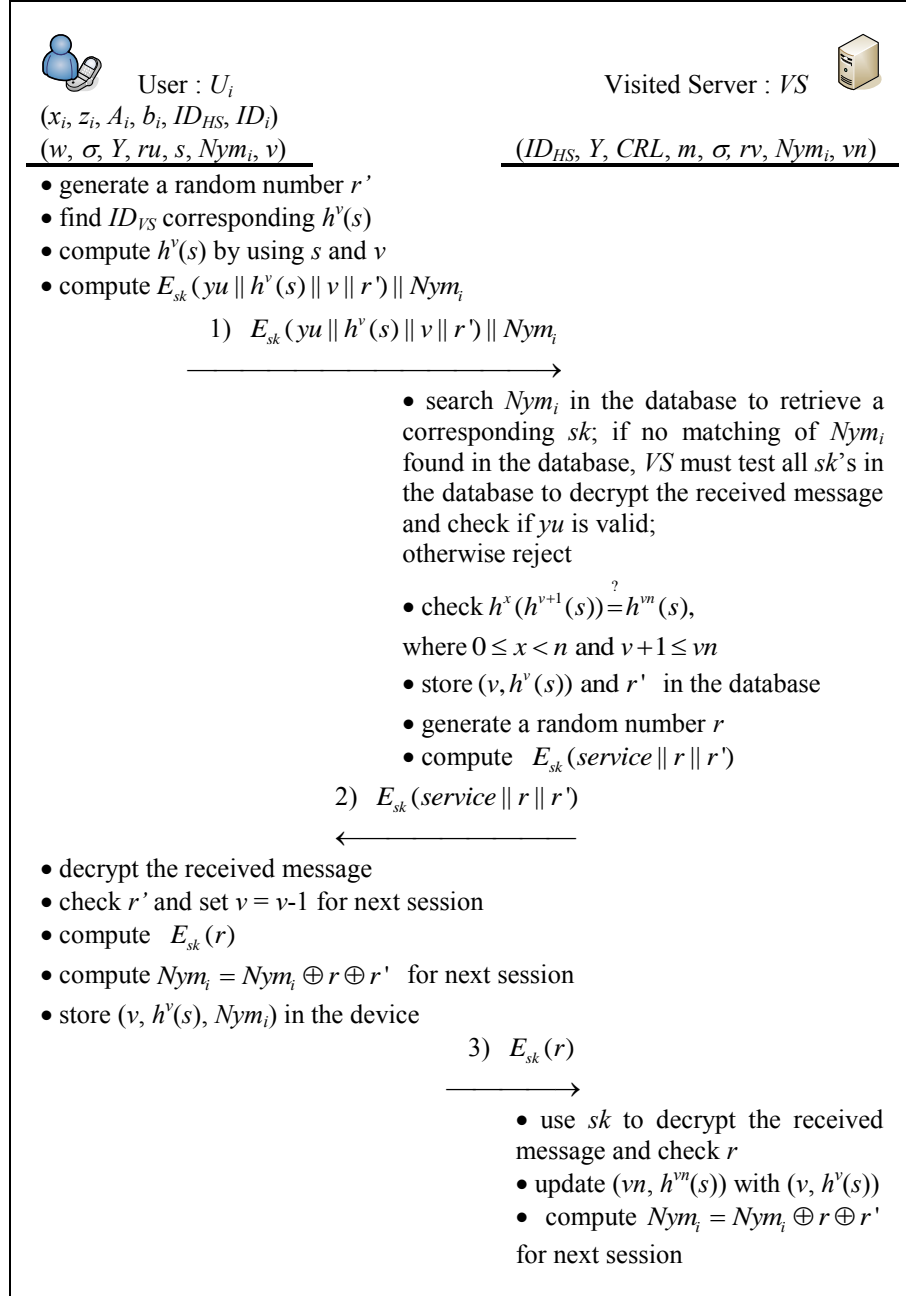


Fig. 5. Fast re-authentication phase

$h^n(s)$ cannot compute $h^{n-1}(s)$ due to the hash function's one-way property. VS and U_i authenticate each others by the following steps.

In the first step, U_i generates a random number r' , uses ID_{VS} to find corresponding $h^v(s)$ and Nym_i , and encrypts $yu || h^v(s) || v || r'$ by using session key sk . Then, U_i sends $E_{sk}(yu || h^v(s) || v || r') || Nym_i$ to VS . In the second step, VS search Nym_i in the database to retrieve a corresponding sk to decrypt received message and check whether $h^x(h^{v+1}(s)) = h^m(s)$ where $x=vn-(v+1)$ and $(vn, h^{vn}(s))$ is a hash chain value stored by VS in the previous session. If no matching of Nym_i found in the database, VS must test all sk 's in the database to decrypt the received message and check if yu is valid. If the above verification fails, VS rejects the roaming user. For avoiding DoS attack which causes the values of hash chains between U_i and VS to be inconsistent, VS has to check if $h^x(h^{v+1}(s)) = h^m(s)$, where $x=vn-(v+1)>0$. Then VS generates a random number r for mutual authentication and sends $E_{sk}(service || r || r')$ to U_i .

In the third step, U_i decrypts $E_{sk}(service || r || r')$ by using session key sk and then he can get r . U_i sets v to be $v-1$ to update the hash chain values for next session. Finally, U_i computes $E_{sk}(r)$ and sends it to VS , and then computes and updates $(v, h^v(s), Nym_i)$ in the device, where $Nym_i = Nym_i \oplus r \oplus r'$. Upon receiving the message delivered from U_i , VS finds corresponding matching of Nym_i in the database and decrypts $E_{sk}(r)$ to check the validity of r . If the verification passes, VS updates $(vn, h^{vn}(s))$ with $(v, h^v(s))$, Nym_i with $Nym_i = Nym_i \oplus r \oplus r'$ for next authentication.

Phase IV: Revocation Phase between Home Server (HS) and Visited Servers (VS)

If a user U_j , belonging to HS , is compromised by an adversary or wants to leave, HS needs to update the revocation member list RML to revoke U_j 's membership. HS performs the following two steps.

- Choose a new revocation base $g_4 \in G_P$ and update Y .
- Update and publish the revocation list $CRL = \{V_j = g_4^{b_j} \text{ mod } P | b_j \in RML\}$ to all servers.

Phase V: Tracing Phase at Home Server

To guarantee the anonymity of U_i , no one except for HS can trace the member U_i . If VS wants to reveal user's identity, he must send T_4 and T_5 to HS . HS then uses his secret key x_{HS} to compute $A_i = T_4 / T_5^{(1/x_{HS})}$ and apply it to find the corresponding identification of U_i .

4 Discussion and Analysis

The security analysis of the proposed protocol is described below.

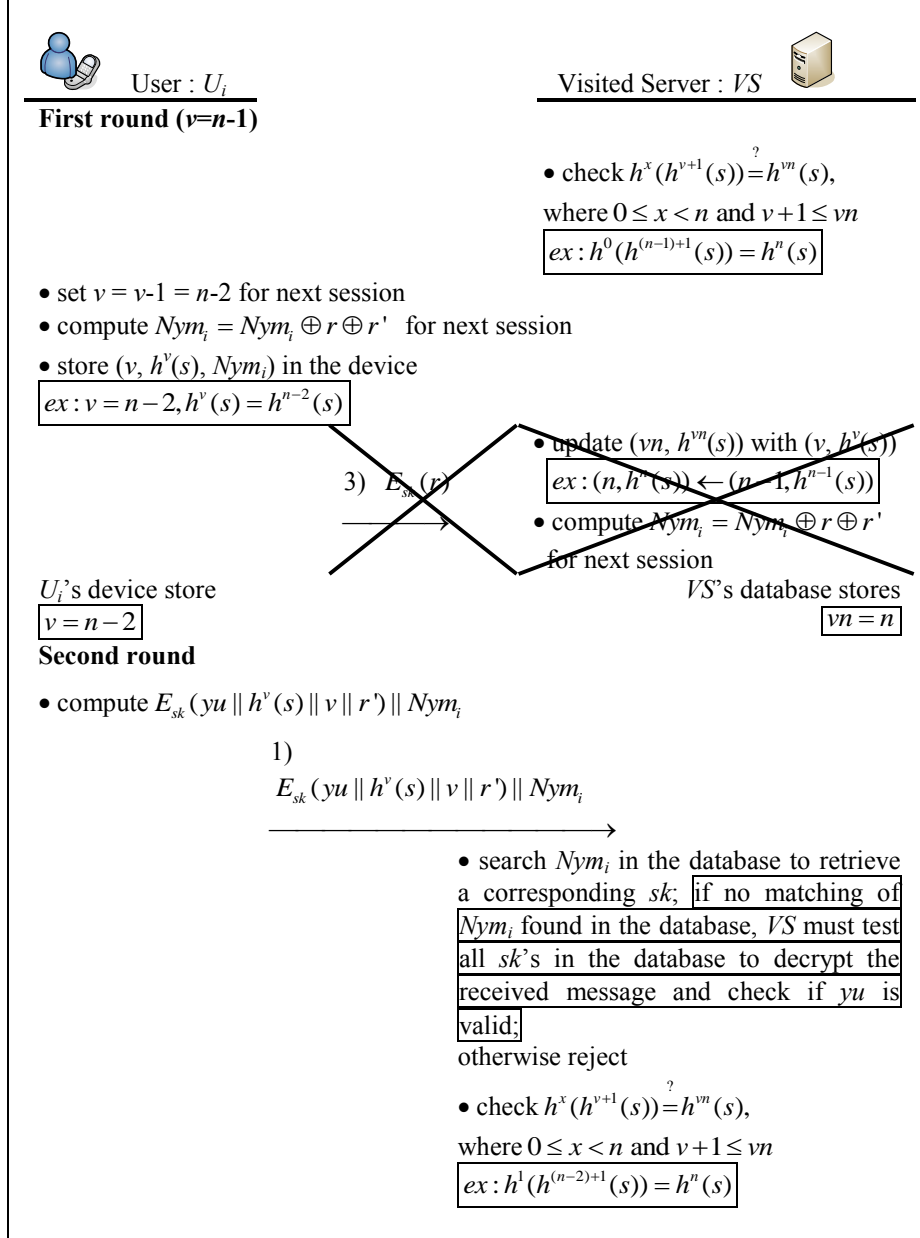


Fig. 6. Demonstration of avoiding DoS attack

Anonymity of user: VS cannot know the information of (A_i, b_i) since U_i is only registered at his HS . Moreover, to solve T_1, T_2, T_3, T_4, T_5 is infeasible under the security assumption of Decision Diffie-Hellman Problem (DDHP). Thus the anonymity of the user in the proposed protocol can be ensured.

Untraceability: No one except for *HS* can trace user. In the proposed scheme, *VS* cannot identify that two signatures, (T_4, T_5) and (T_4', T_5') , is signed by the same user; that is based on the assumption of the strong multiple discrete logarithm problem (MDLP) [11].

Revocability: *VS* can use the public information V_j to check if $T_1^{V_j} = T_2$. If yes, *VS* confirms that the user U_j has been revoked by *HS*. Then, *VS* will reject the authentication request from U_j .

Resisting DoS (Denial of Service) attack: The proposed protocol is secure against the DoS attacks in the communications between users and servers. Fig. 6 shows that *VS* can successfully verify U_i by using hash chain values even if the protocol suffers from DoS attack. If *VS* does not receive the message $E_{sk}(r)$ from U_i (may be dropped by the attacker), the protocol is aborted and *VS* cannot update vn and $h^m(s)$. However, *VS* still can verify the user in next round by checking if $vn > v+1$ and for $x=vn-(v+1)$, if the equation $h^x(h'(s)) = h^m(s)$ holds.

Resisting replay attack: Even if an adversary gets the message generated by the user, the adversary cannot forge the user U_i to generate a group signature in next session. Moreover, the adversary can get the value of n th hash chain, but he still cannot compute the value of $(n-1)$ th hash chain because of the property of one-way hash function.

Table 1 The comparison between the proposed protocol and Wan et al.'s protocol

Roaming protocol	Our proposed protocol	Wan et al. [14]
Security requirements		
Non-repudiation	O	O
Unforgeability	O	O
Unlinkability	O	O
Anonymity of user	O	O
Untraceability	O	O
Revocability	O	O
Resisting DoS attack	O	X
Resisting replay attack	O	O
Forward secrecy	O	O
Hierarchical structure and Trust Third Party (TTP)	X	O
Connecting to HS	X	X

Forward secrecy: Even if the long-term key or current session key is compromised or stolen, the roaming protocol can ensure that the previous data of *VS* and U_i is still secure. The session key of this roaming protocol is based on the Discrete Logarithm Problem (DLP) and Computational Diffie-Hellman Problem (CDHP). Thus, the roaming protocol can achieve forward secrecy.

Unlinkability: If someone gets two signatures $\{T_1, T_2, T_3, T_4, T_5, \sigma_1, \sigma_2\}$ and $\{T_1', T_2', T_3', T_4', T_5', \sigma_1', \sigma_2'\}$ by eavesdropping on Internet, he cannot determine if

these signatures generated by the same user. The problem is based on the decision Diffie-Hellman assumption.

Table 1 shows a comparison between our proposed protocol and Wan et al.'s protocol [14]. Although Wan et al. [14] claimed that their roaming protocol can resist DoS attack, we found that their protocol only checks $h(h^i(s)) = h^{i+1}(s)$ to verify the valid of user. That means they did not consider that the DoS attack occurs in the previous step. Thus we conclude that Wan et al.'s protocol cannot fully resist the DoS attack. For efficiency analysis, Table 2 compares some previous works and the proposed protocol in terms of communication model and used cryptography techniques. The communications between TTP and servers, TTP and the user, and user's *HS* and *VS* may take more costs than the communication between *VS* and the user because the local communication cost is less than the inter-domain communication cost. However, the computations of public key cryptography and pairing operations are higher than the computations of symmetric-key encryption and hash function.

Table 2 The comparison of communication model and cryptography techniques

Roaming protocol Communication model and encryption methods	Jiang et al. [10]	Yang et al. [15]	Wan et al. [14]	Our protocol
Comm. between TTP and all servers	no	no	yes	no
Comm. between TTP and user	yes	no	yes	no
Comm. between user's <i>HS</i> and <i>VS</i>	yes	yes	no	no
Comm. between <i>VS</i> and user	yes	yes	yes	yes
Cryptography techniques	S+H	S+H+D	S+H+D+P	S+H+D

S: symmetric-key encryption
H: one-way hash function
D: public-key cryptography
P: pairing operation

5 Conclusions

We proposed a new roaming protocol to achieve most of the security requirements of roaming protocol. The proposed protocol can resist the replay and DoS attacks and protect the privacy of roaming users. The communication cost can be reduced by using a group signature scheme, which can be particularly suitable for the long distance communication between *VS* and *HS*. However, the proposed protocol has higher computational cost. We are planning to improve the efficiency in the future.

References

1. Ala-Laurila, J., Mikkonen, J., Rinnemaa, J.: Wireless LAN access network architecture for mobile operators. In: IEEE, Communications Magazine, vol. 39, Issue: 11, pp.82—89. (Nov. 2001)
2. Bicakci, K., Baykal, N.: Infinite length hash chains and their applications. In: 11th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 2002 (WETICE 2002), pp.57--61. (2002)
3. Bellavista, P., Corradi, A., Vecchi, S.: Application domain accounting for roaming services. In: 9th IEEE Workshop on Future Trends of Distributed Computing Systems (FTDCS 2003), pp.359--366. (28-30 May 2003)
4. Boneh, D., Franklin, M.: Identity-Based Encryption from the Weil Pairing. In: Advances in Cryptology—Crypto'01, Lecture Notes in Computer Science, vol. 2139, pp. 213--229. Springer, Heidelberg (2001)
5. Brickell, E., Li, J.: Enhanced Privacy ID: A Direct Anonymous Attestation Scheme with Enhanced Revocation Capabilities. In: Proceedings of the 2007 ACM workshop on Privacy in electronic society, Anonymous communications, pp.21--30. (2007)
6. Camenisch, J.: Group signature schemes and payment systems based on the discrete logarithm problem. PhD thesis, vol.2 of ETH-Series in information Security and Cryptography, ISMN 3-89649-286-1, Hartung-Gorre Verlag, Konstanz (1998)
7. Dahlberg, T., Mallat, N., Ondrus, J., Zmijewska, A.: Past, present and future of mobile payments research: A literature review. In: Electronic Commerce Research and Applications archive, Vol. 7, Issue 2, pp. 165-181. (2008)
8. Fujii, A., Ohtake, G., Hanaoka, G., Ogawa, K.: Anonymous Authentication Scheme for Subscription Services. In: Lecture Notes in Computer Science-Knowledge-Based, Intelligent Information and Engineering Systems, vol. 4694, pp.975--985. (2007)
9. Horwitz, J., Lynn, B.: Toward hierarchical id-based encryption, In: Proceedings of EUROCRYPT'02, LNCS, vol. 2332, pp.466--481. (2002)
10. Jiang, Y., Lin, C., Shen, X., Shi, M.: Mutual Authentication and Key Exchange Protocols for Roaming Services in Wireless Mobile Networks. In: IEEE Transactions on Wireless Communications, Vol. 5, Issue 9, pp.2569--2577. (2006)
11. Miyaji, A., Umeda, K.: A Fully-Functional Group Signature Scheme over Only Known-Order Group. In: LECTURE NOTES IN COMPUTER SCIENCE, Applied Cryptography and Network Security, Digital Signature, vol. 3089, pp.164--179. (2004)
12. Scourias, J.: An Overview of the Global System for Mobile Communications. Technical Report, University of Waterloo (1995)
13. Trevathan, J., Read, W.: Secure Online English Auctions. In: LNCS, E-Business and Telecommunication Networks, Communications in Computer and Information Science (CCIS9), pp.119--133. (2008)
14. Wan, Z., Ren, K., Preneel, B.: A Secure Privacy-Preserving Roaming Protocol Based on Hierarchical Identity-Based Encryption for Mobile Networks. In: Proceedings of the first ACM conference on Wireless network security, Device identification and privacy, pp.62--67. (2008)
15. Yang, G., Wong, D.S., Deng, X.: Anonymous and Authenticated Key Exchange for Roaming Networks. In: IEEE Transactions on Wireless Communications, Vol.6, Issue 9, pp.3461--3472. (2007)
16. Yang, Y., Ooi, B.C.: A Privacy Preserving Rental System. In: Lecture Notes in Computer Science (LNCS) Information Security, vol.3650, pp.59--73. (2005)