Robust ID based mutual authentication and key agreement scheme preserving user anonymity in mobile networks

Yanrong Lu[1,2], Lixiang Li [1,2], Haipeng Peng[1,2] and Yixian Yang[1,2]
[1] Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China
[e-mail: lixiang@bupt.edu.cn]
National Engineering Laboratory for Disaster Backup and Recovery, Beijing University of Posts and Telecommunications, Beijing 100876, China
*Corresponding author: Lixiang Li

Received October 15, 2015; revised December 22, 2015; accepted January 21, 2016; published March 31, 2016

Abstract

With the swift growth of wireless technologies, an increasing number of users rely on the mobile services which can exchange information in mobile networks. Security is of key issue when a user tries to access those services in this network environment. Many authentication schemes have been presented with the purpose of authenticating entities and wishing to communicate securely. Recently, Chou et al. and Farash-Attari presented two ID authentication schemes. They both claimed that their scheme could withstand various attacks. However, we find that the two authentication schemes are vulnerable to trace attack while having a problem of clock synchronization. Additionally, we show that Farash-Attari's scheme is still susceptible to key-compromise impersonation attack. Therefore, we present an enhanced scheme to remedy the security weaknesses which are troubled in these schemes. We also demonstrate the completeness of the enhanced scheme through the Burrow-Abadi-Needham (BAN) logic. Security analysis shows that our scheme prevents the drawbacks found in the two authentication schemes while supporting better secure attributes. In addition, our scheme owns low computation overheads compared with other related schemes. As a result, our enhanced scheme seems to be more practical and suitable for resource-constrained mobile devices in mobile networks.

Keywords: Authentication, anonymous, two-factor, client-server networks

The authors would like to thank all the anonymous reviewers for their helpful advice. This paper is supported by the National Natural Science Foundation of China (Grant Nos. 61573067, 61472045), the Beijing Natural Science Foundation (Grant No. 4142016), BUPT Excellent Ph.D. Students Foundation (Grant No. CX2015310) and the Asia Foresight Program under NSFC Grant (Grant No. 61411146001).

http://dx.doi.org/10.3837/tiis.2016.03.018 **ISSN : 1976-7277**

1. Introduction

The mobile devices have become an important part of our learning, working and living with the rapid development of wireless communication technology. People often use mobile devices to enjoy network services anytime and anywhere, which provide a lot of convenience in our life. Unfortunately, the majority of these communication environments are insecure, thus leading to the sensitive information might be intercepted by any unauthorized entity. As a result, security has become a big problem when a remote user attempts to access the services over any open networks. Authentication and key agreement is the representative approach to verify the legitimacy of a remote user and establish a session key between the communication parties.

From Lamport [1] proposed the first remote mutual authentication scheme over an unreliable channel, a large number of authentication schemes for different applications, have been presented, analyzed and some broken [2-6]. Shamir [7] first introduced the notion of ID based public-key cryptosystem, which might lighten the certificate overhead compared with the other public-key systems. Later, Boneh-Franklin [8] presented the formal security analysis of the ID based encryption scheme employing pairings. Since then numerous ID based key agreement schemes combining pairings have been presented [9-11]. However, the above schemes are not efficient applying for resource-constrained mobile devices due to the relative computation cost of pairing is approximately 20 times higher than that of the scalar multiplication [12].

With the tremendous development of the network technologies, recently ID based authentication and key agreement schemes using elliptic curve cryptosystem (ECC) have been broadly deployed in the wireless networks for mobile devices. As compared with traditional cryptosystem, ECC offers equivalent security with smaller key size [13-14]. In 2009, Yang-Chang [15] proposed an efficient and practical ID based two-party mutual authentication scheme employing ECC. They both consider ID-based and ECC properties simultaneously. However, both Yoon-Yoo [16] and Islam-Biswas [17] discovered that Yang-Chang's two-party scheme had some security flaws such as suffered from impersonation, replay attacks and did not provide the session key forward secrecy. To resolve these problems, Yoon-Yoo [16] and Islam-Biswas[17] respectively proposed their effective enhancements with higher security. In Yoon-Yoo's scheme, user's identity was hashed and mapped to a point on elliptic curve. Nevertheless, He et al. [18] identified thatYoon-Yoo's scheme [16] failed to achieve forward secrecy and then presented an improvement scheme to erase the drawbacks of Yoon-Yoo's scheme. Subsequently, Chou et al. [19] pointed out that both Yang-Chang's and Yoon-Yoo's schemes lacked the public key for users. Moreover, Chou et al. also showed that there were no legible key confirmation in He et al.'s scheme [18]. In order to eliminate the security pitfalls, Chou et al. presented an efficient ID and ECC based two-party scheme for mobile users. In Chou et al.'s scheme, the process of the user's private key generation is an efficient and the user could check the correctness for his own private key. Recently, Farash-Attari [20] demonstrated that Chou et al.'s two-party scheme could not resist impersonation and key-compromise impersonation attacks. Then, Farash-Attari also presented an effective enhancement over Chou et al.'s scheme with more security.

ID based three-party scheme was proposed by Yang-Chang[21], which enhanced security and efficiency of Chen et al.'s [22] scheme. However, Tan [23] showed that Yang-Chang's

scheme was insecure against impersonation and parallel attacks. To conquer the problems, Tan proposed an improved scheme and claimed that their scheme satisfied many security attributes. However, He et al. [24] pointed out that the server had to maintain the users' certificates in both Yang-Chang's scheme [21] and Tan's scheme [23]. Then, He et al. proposed an enhanced ID based three-party remote mutual authentication scheme to eliminate these flaws. He et al.'s scheme adopted general cryptographic hash function without considering map to point function. Unfortunately, Chou et al. [19] showed that He et al.'s scheme still existed the problem that there were no verification on user's private key and the establishment of the user's private key was time consuming. Subsequently, Chou et al. also proposed an ID based three-party authentication scheme as an extension based on their two-party scheme. Recently, Farash-Attari [20] showed that Chou et al.'s three-party scheme was susceptible to impersonation attack. To eliminate the security drawbacks in Chou et al.'s scheme, Farash-Attari proposed a modified two-party scheme.

In this paper, we present a cryptanalysis of Chou et al.'s and Farash-Attari's schemes. We indicate that the two schemes are vulnerable to trace attack and do have the problem of clock synchronization. In addition, we show that Farash-Attari's scheme is still susceptible to key-compromise impersonation attack. Therefore, we present an enhanced scheme based on Farash-Attari's scheme to remedy the security weaknesses. We also demonstrate the completeness of the enhanced scheme through the Burrow-Abadi-Needham (BAN) logic. Security analysis shows that our scheme prevents the drawbacks found in the two authentication schemes while supporting better secure attributes. In addition, our scheme owns low computation overheads compared with other related schemes. As a result, our enhanced scheme seems to be more practical and suitable for resource-constrained mobile devices in mobile networks.

The remainder of this paper is organized as follows. The review and cryptanalysis of Chou et al.'s and Farash-Attari's schemes are shown in Section 2 and Section 3, respectively. We present our proposed scheme and its analysis in Sections 4 and Section 5, respectively. Section 6 shows the performance and functionality comparisons between the enhanced scheme and other related ones. Section 7 is a brief conclusion.

2. Review and analysis of Chou et al.'s scheme

In this section, we will briefly review Chou et al.'s two-party and three-party authentication schemes [19]. Moreover, we show that Chou et al.'s scheme is susceptible to the trace attack and has the problem of clock synchronization. We list notations used throughout this paper for convenience in **Table 1**.

2.1 Two-party scheme

There are mainly two phases in Chou et al.'s two-party scheme: registration and authentication phases.

2.1.1 Registration

Before registration, S publishes $\{E_p(a,b), K_s, h_1, h_2\}$, where $K_s = k_s \oplus P$.

1) S sends his identity ID_u to S;

2) S computes $k_u = k_s + h_1(ID_u)h_1(ID_u \oplus k_s)$, $Q_{ID_u} = h_1(ID_u \oplus k_s)P$, and delivers $\{k_u, Q_{ID_u}\}$ to U.

Table 1. Notations

Notations	Description
U, S	User and Server
ID_a	Identity of an entity A
$h_1(\cdot)$	Hash function $h_1(\cdot):\{0,1\}^* \to Z_n^*$
$h_2(\cdot)$	Hash function $h_1(\cdot):\{0,1\}^* \to Z_p^*$,where p is a large prime
k_s, K_s	Private key and public key selected by S
k_u, Q_{ID_u}	Private key and public key selected U
$\oplus$, $\|\|$	Exclusive-or operation and Concatenation operation
$E_p(a,b)$	A non-super singular elliptic curve over a finite field
P	A point value on the elliptic curve

3) U checks $k_u P \stackrel{?}{=} K_s + h_1(ID_u)Q_{ID_u}$. If so, U puts k_u as his private key and publishes his public key Q_{ID_u}.

2.1.2 Authentication

1) U selects a random number r_u and computes $R_u = r_u P$, $V = k_u R_u$, $h_u = h_2(ID_u \| R_u \| V \| T_u)$. Then, U sends $\{ID_u, R_u, h_u, T_u\}$ to S.

2) When receiving message, S verifies the freshness of T_u and checks whether $(k_s + h_1(ID_u)h_1(ID_u \oplus k_s))$, $R_u \stackrel{?}{=} V'$. If they are equal, S selects a random number r_s and computes $R_s = r_s P$, $sk = r_s R_u$, $h_s = h_2(ID_u \| R_u \| R_s \| V' \| T_s \| sk)$. Finally, S sends $\{R_s, h_s, T_s\}$ to U.

3) After receiving the message, U checks the freshness of T_s and checks whether $h_2(ID_u \| R_u \| R_s \| V' \| T_s \| r_u R_s) \stackrel{?}{=} h_s$. If they are correct, U computes $h_2(ID_u \| V' \| sk' + 1)$ and sends it to S.

4) S computes $h_2(ID_u \| V' \| sk + 1)$ and verifies it with the received message. If it holds, U and S successfully agree on the common session key sk.

2.2 Three-party scheme

There are also mainly two phases in Chou et al.'s three-party scheme: registration, and authentication and key agreement. The registration phase is the same as the two-party scheme,

that is, both A and B obtain their private/ public key k_a / Q_{ID_a} and k_a / Q_{ID_a}, respectively, where $k_a = k_s + h_1(ID_a)h_1(ID_a \oplus k_s)$, $Q_{ID_a} = h_1(ID_a \oplus k_s)P$, $k_b = k_s + h_1(ID_b)h_1(ID_b \oplus k_s)$, and $Q_{ID_b} = h_1(ID_b \oplus k_s)P$.

2.2.1 Authentication and key agreement

1) $A \rightarrow B$

A selects his identity ID_a and sends $\{ID_a, request\}$ to B.

2) $A \rightarrow S$

A chooses a random number r_a, computes $R_a = r_a P$, $V_a = k_a R_a$ and $h_a = h_2(ID_a \| ID_b \| R_a \| V_a \| t_a)$, where T_a denotes the current timestamp. Then, A sends $\{ID_a, ID_b, R_a, h_a, t_a\}$ to S.

3) $B \rightarrow A$

Upon receiving the message from A, B immediately sends $\{ID_a, response\}$ to A.

4) $B \rightarrow S$

When receiving the message from A, B chooses a random number r_b and computes $R_b = r_b P$, $V_b = k_b R_b$, $h_b = h_2(ID_b \| ID_a \| R_b \| V_b \| t_b)$, where t_b denotes the current timestamp. Then, B sends $\{ID_b, ID_a, R_b, h_b, t_b\}$ to S.

5) $S \rightarrow A$

Upon receiving the message from A, S first checks the freshness of t_a, computes $V_a^{'} = (k_s + h_1(ID_a)h_1(ID_a \oplus k_s))R_a$ and checks whether $h_2(ID_a \| ID_b \| R_a \| V_a^{'} \| t_a) \stackrel{?}{=} h_a$. If they are true, S computes $h_{sa} = h_2(ID_a \| ID_b \| V_a^{'} \| R_b \| t_s)$ and sends $\{R_b, h_{sa}, t_s\}$ to A.

6) $S \rightarrow B$

Upon receiving the message from B, S first checks the freshness of t_b, computes $V_b^{'} = (k_s + h_1(ID_b)h_1(ID_b \oplus k_s))R_b$ and checks whether $h_2(ID_a \| ID_b \| R_a \| V_b^{'} \| t_b) \stackrel{?}{=} h_b$. If they are true, S computes $h_{sb} = h_2(ID_a \| ID_b \| V_b^{'} \| R_b \| t_s)$ and sends $\{R_a, h_{sb}, t_s\}$ to B.

7) $S \rightarrow A$

Upon receiving the message from S, A checks whether $h_2(ID_a \| ID_b \| V_a \| R_b \| t_s) \stackrel{?}{=} h_{sa}$. If holds, A calculates the common session key $sk = r_a R_b$. Similarly, B executes the same operations as A. Finally, A and B negotiate the session key sk with the help of S.

2.3 Analysis of Chou et al.'s scheme

2.3.1 Trace attack

User anonymity is of significance issue in the wireless environment since it can protect user's privacy. In the two authentication phases, the identity ID_u is transmitted as a plain-text without any protection in an open channel, which gives an adversary to track his current location and recognize what type of services the user enjoys. This results seriously invades individual's privacy and potentially increases a bit more risk exposure. Farash-Attari presented their enhanced scheme according to Chou et al.'s scheme but the trace attack is still not immune to their scheme. For this reason, the trace attack is also inevitable in Farash-Attari's scheme.

2.3.2 Clock synchronization problem

The timestamp is employed to withstand the replay attack in the two authentication phases. Notice there is no mention of the transmitted delay can be limited in a certain interval of time. In this case, if the adversary resends the older authentication messages, then S will still authenticate the adversary each time. This inevitably leads to the problem of clock synchronization especially applying the time interval for wide area networks. Even when initially set accurately, real clocks will differ after some amount of time due to clock drift, caused by clocks counting time at slightly different rates.

Farash-Attari's scheme goes after the same authentication mechanism as of Chou et al.'s scheme. Therefore, clock synchronization problem also exists in Farash-Attari 's scheme.

3. Review and analysis of Farash-Attari's scheme

In this section, we will briefly review Farash-Attari's two-party authentication scheme. Moreover, we show that Farash-Attari's scheme is also inability to protect against the track attack and avoid the clock synchronization problem. Besides, Farash-Attari's scheme is still susceptible to key-compromise impersonation attack.

3.1 Two-party scheme

Farash-Attari's scheme [20] also contains two phase: registration, authentication and key agreement, where registration phase is the same as Chou et al.'s scheme, we omit it. Now, we mainly describe the authentication and key agreement phase.

3.1.1 Authentication and key agreement

1) U selects a random number r_u, computes $R_u = r_u P$, $K_1 = r_u k_u K_s$, $h_u = h_2(ID_u \| R_u \| K_1 \| t_u)$, where t_u denotes the current timestamp. Then, U sends $\{ID_u, R_u, t_u, h_u\}$ to S.

2) Upon receiving the message, S checks the freshness of t_u. If it is valid, S computes $K_1 = k_s(k_s + h_1(ID_u)h_1(ID_u \rangle k_s))R_u$ and checks $h_2(ID_u \| R_u \| K_1 \| t_u) \stackrel{?}{=} h_u$. If it holds, S selects a random number r_s and computes

$R_s = r_s P$, $K_2 = r_s R_u$, $h_s = h_2(0 \| ID_u \| R_u \| R_s \| K_1 \| K_2 \| t_s)$. Then, S sends $\{R_s, h_s, t_s\}$ to U, where t_s is the timestamp of S.

3) After receiving the message, U verifies if t_s is valid. If true, U computes $K_2^{'} = r_u R_s$ and verifies $h_2(0 \| ID_u \| R_u \| R_s \| K_2 \| K_1 \| t_s) \stackrel{?}{=} h_s$ .Then, U computes $h_2(1 \| ID_u \| R_u \| R_s \| K_2 \| K_1 \| t_s)$ and sends it to S.

4) S checks whether $h_2(1 \| ID_u \| R_u \| R_s \| K_2 \| K_1 \| t_s)$ is equal to the received value. If it is equal, S establishes the session key $sk = h(ID_u \| R_u \| R_S \| K_1 \| K_2 \| t_u \| t_s)$ with U.

3.2 Analysis of Farash-Attari 's scheme

Farash-Attari's scheme is also prone to suffer from trace and replay attacks. Previous subsections analyze the reason, here we won't cover those again. Following we present another attack referring to Farash-Attari's scheme.

3.2.1 Key-compromise impersonation attack

When the private key of S is compromised is that an adversary is able to impersonate not only as S but also to S as U. Suppose the adversary gets k_s and tries to impersonate as U to access the services provided by S.

1) The adversary eavesdrops the login request message $\{ID_u, R_u, t_u, h_u\}$ from U to S. Then, he generates a random number $r_u^{'}$ and computes $R_u^{'} = r_u^{'} P$, $K_1^{'} = r_u^{'} k_s (K_s + h_1(ID_u) Q_{ID_u})$, $h_u^{'} = h_2(ID_u \| R_u^{'} \| K_1^{'} \| t_u^{'})$. Subsequently, he sends the forged message $\{ID_u, R_u^{'}, t_u^{'}, h_u^{'}\}$ to S, where $t_u^{'}$ is the current timestamp.

2) When receiving the message, S first checks the freshness of $t_u^{'}$. If it is valid, he then continues to check $h_2(ID_u \| R_u^{'} \| K_1 \| t_u^{'}) \stackrel{?}{=} h_u$, where $K_1 = k_s(k_s + h_1(ID_u) h_1(ID_u \oplus k_s)) R_u$. Obviously, the equation is true. Therefore, S authenticates the adversary who impersonates as a legal user. After that, S selects a random number r_s and calculates $R_s = r_s P$, $K_2^{'} = r_s R_u^{'}$, and $h_s = h_2(0 \| ID_u \| R_u^{'} \| R_s \| K_1 \| K_2^{'} \| K_2^{'} \| t_s)$. Finally, S transsmits the respond message $\{R_s, h_s, t_s\}$ to U, where t_s is the current timestamp.

3) After receiving the message, the adversary also verifies the validness of t_s. If holds, he figures up $K_2^{'} = r_u^{'} R_s$ and checks whether $h_2(0 \| ID_u \| R_u \| R_s \| K_1^{'} \| K_2^{'} \| t_s) \stackrel{?}{=} h_s$ is true. If holds, he calculates $h_2(1 \| ID_u \| R_u^{'} \| R_s \| K_2 \| K_1^{'} \| t_s)$ and then delivers it to S.

4) Upon receiving the message, S verifies if $h_2(1 \| ID_u \| R_u^{'} \| R_s \| K_2^{'} \| K_1^{'} \| t_s)$ is equal to the received value. If true, S consults with the adversary to ensure the session key

$sk = h(ID_u \| R_u^{'} \| R_s \| K_1^{'} \| K_2^{'} \| t_2^{'} \| t_s)$. That is, the adversary successfully impersonates as a legal user to cheat S but S believing the adversary is just the corresponding user.

4.The enhanced scheme

In this section, we present a simple enhancement on Chou et al.'s and Farash-Attari's two-party schemes, which inherits the advantages of original schemes and is immune to the security pitfalls stated in previous sections. Three-party scheme can be easily constructed by extending two-party scheme.In our scheme, the user and the server will authenticat each other and establish a session key, which is used to encrypt the subsequently information . Therefore, our scheme can be applied in many electronic transactions environments, such as online banking, on-line shopping, Pay-TV and electronic voting.

4.1 Registration

Similarly, S publishes $\{E(a,b), K_s, h_1, h_2\}$, where $K_s = k_s P$ before registration.

1) U chooses his identity ID_u and submits it to S via a secure channel.

2) S generates a random number r_s and computes $k_u = r_s h_1(ID_u \oplus k_s)$, $Q_{ID_u} = h_1(ID_u \oplus k_s)$ as U's private and public keys. Subsequently, S stores r_{s_1} into its secret database and returns $\{r_{s_1}, k_u, Q_{ID_u}\}$ to U through a secret channel.

3) After receiving the message, U examines $k_u P = r_{s_1} Q_{ID_u} P$. If the equation holds, U keeps k_u secretly and releases Q_{ID_u}.

4.2 Authentication and key agreement

1) U randomly chooses a number r_u and computes $P_1 = r_{s_1} P \oplus ID_u$, $K = h_2(ID_u \| r_{s_1})$, $P_2 = K \oplus r_u P$, $P_3 = h_2(K \| r_u P \| k_u P)$. Then, U sends $\{P_1, P_2, P_3\}$ to S.

2) Upon receiving the login message, S firstly derives ID_u by computing $P_1 \oplus r_{s_1} P$ and then he makes use of ID_u to get $r_u P$ by computing $h_2(ID_u \| r_{s_1}) \oplus P_2$. After that, S checks whether $h_2(K \| r_u P \| r_{s_1} Q_{ID_u}) \stackrel{?}{=} P_3$. If it holds, S chooses a random number r_{s_2} and computes $SK = r_{s_2} r_u P$, $Q_1 = K \oplus r_{s_2} P$, $Q_2 = h_2(K \| r_u P \| SK)$. Then, S sends $\{Q_1, Q_2\}$ to U.

3) After receiving the authentication message, U reveals $r_{s_2} P$ by computing $K \oplus Q_1$ and computes $SK = r_u r_{s_2} P$. Subsequently, U verifies $h_2(K \| r_u P \| SK) \stackrel{?}{=} Q_2$. If the equation is correct, U continues to compute $P_4 = h_2(K \| r_s P \| SK)$ and sends it to S.

4) When receiving the message, S checks whether $h_2(K \| r_s P \| SK) \stackrel{?}{=} P_4$. If it is true, S successfully negotiates the session key with U. Therefore, they can encrypt the

communicated messages through the established session key. **Fig. 1** shows the phases of registration and authentication of our scheme.

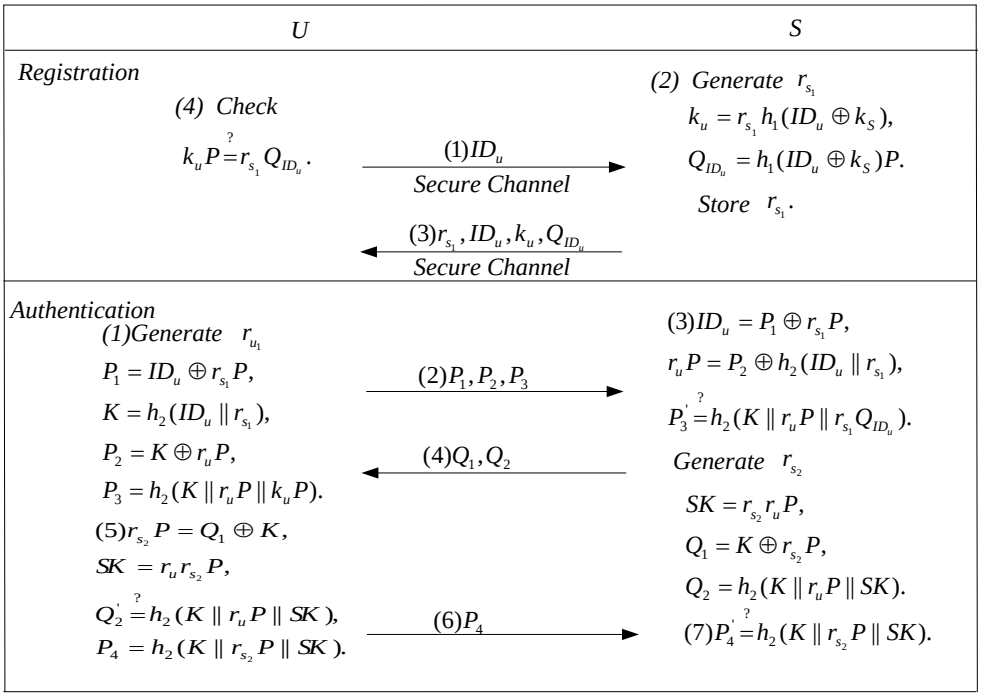

Fig. 1. Registration and authentication phase of the enhanced scheme

5. Analysis of the enhanced scheme

This section presents a cryptanalysis of the enhanced scheme and shows that it not only is secure against trace and key-compromise impersonation attacks but also provides the session key perfect forward secrecy and mutual authentication and other related security properties. In addition, Burrows-Abadi-Needham (BAN) logic mechanism [25] is adopted to prove that U and S achieve mutual authentication and correctly generate a session key within authentication process. Suppose an adversary has fully monitored the authentication and key agreement phase and then he can insert, modify and delete any messages transmitted between the user and the corresponding server [1].

5.1 Withstanding the trace attack

In the authentication and key agreement phase, the user's identity ID_u is hidden in all the transmitted messages $P_1 = r_{s_1} P \oplus ID_u$, $P_2 = h_2(ID_u \| r_{s_1}) \oplus r_u P$,

$P_3 = h_2(h_2(ID_u \| r_{s_1}) \| r_u P \| k_u P)$, $P_4 = h_2(h_2(ID_u \| r_{s_1}) \| r_s P \| SK)$, $Q_1 = h_2(ID_u \| r_{s_1}) \oplus r_{s_2} P$,

and $Q_2 = h_2(h_2(ID_u \| r_{s_1}) \| r_u P \| SK)$, where r_{s_1} is a shared random number between the user and the server, r_u and r_s are the random numbers generated by the user and the server, respectively. Acctually, a toilless method for an adversary is to know the shared random number r_{s_1} and then derive the real identity by intercepting P_1. As a result, it is computationally infeasible for an

adversary to derive the real identity from $r_{s_1}P$ due to the property of Elliptic Curve Discrete Logarithmic Problems [26]. Therefore, the adversary has no opportunity to obtain the user's identity and thus he has no opportunity to plot the trace attack.

5.2 Withstanding the key-compromise impersonation attack

Even if an adversary has obtained the private key of one of the entities, he cannot successfully plot an impersonation attack. We assume U's private key k_u is leaked, which is concealed in the value of P_3. If the adversary attempts to impersonate as a legal sever, he should know U's identity ID_u and r_uP, but both of them are protected by a random number r_{s_1} which is only known by U and S. On the other hand, suppose the private key k_s of S is lost, the adversary is still not able to launch an impersonation attack without the knowledge of ID_u. In a word, the key-compromise impersonation attack dose not work in the enhanced scheme.

5.3 Avoiding the clock synchronization problem

In the enhanced scheme, we adopt random numbers instead of timestamp. If an adversary tries to resending the old login message to pretend as U, S will detect the attack from U since random numbers r_{s_1} and r_uP are different for each session. Therefore, the replay attack is impractical to the enhanced scheme.

5.4 Providing the session key perfect forward secrecy

Even though an adversary has known the secret key of all the entities and the previous session key, he cannot compute the next session key. Since the session key is decided by two distinct random numbers generated by U and S and the new session key is different from the old one. Therefore, the session key perfect forward secrecy is easily achieved.

5.5 Achieving the mutual authentication

In the enhanced scheme, U authenticates S through the verification $Q_2 = h_2(ID_u \| SK \| r_uP)$ because any unauthorized sever is not possible to derive the user's real identity and then work out the correct value r_uP. S authenticates U by computing $P_3 = h_2(ID_u \| r_uP \| r_{s_1}Q_{ID_u})$ and $P_4 = h_2(ID_u \| r_{s_2}P \| SK)$. Only the legal user knows r_{s_1} and thus derives $r_{s_2}P$ from Q_2. S will immediately perceive the attack if any one attempts to modify the parameters. Therefore, the enhanced scheme satisfies mutual authentication.

5.6 Withstanding the impersonation attack

Suppose an adversary eavesdrops the login request message to impersonate as a legal user to cheat S. However, it is impossible to pass through S without the knowledge of U's identity ID_u and the shared random number r_{s_1}. Both two values are only known by U and S. The same reason is appropriate for the adversary tries to impersonate as a legal sever to deceive U. Therefore, the enhanced scheme is immune to the impersonation attack.

5.7 Verifying the enhanced scheme with BAN logic

Some notations **(Table 2)** and logical postulates of BAN logic that we will used in our scheme are introduced as follows.

1) BAN logical postulates

a. Message-meaning rule: $\frac{A \mid\equiv A \overset{K}{\leftrightarrow} B, A \triangleleft \{X\}_K}{A \mid\equiv B \mid\sim M}$: if A believes that K is shared by A and B and sees X encrypted with K, then A believes that B once said X.

b. Nonce-verification rule: $\frac{A \mid\equiv \# X, A \mid\equiv B \mid\sim X}{A \mid\equiv B \mid\equiv X}$: if A believes that X could have been uttered only recently and that B once said X, then A believes that B believes X.

c. Belief rule: $\frac{A \mid\equiv X, A \mid\equiv Y}{A \mid\equiv (X,Y)}$: if A believes X and Y, then A believes (X,Y)

d. Fresh conjuncatenation rule: $\frac{A \mid\equiv \#(X)}{A \mid\equiv \#(X,Y)}$: if A believes freshness of X, A then believes freshness of (X,Y).

e. Jurisdiction rule: $\frac{A \mid\equiv B \Rightarrow X, A \mid\equiv B \mid\equiv X}{A \mid\equiv X}$: if A believes that B has jurisdiction over X and A trusts B on the truth of X, then A believes X.

Table 2. BAN logic notations

Notations	Description
$A \mid\equiv X$	A believes a statement X
$U \overset{K}{\leftrightarrow} S$	Share a key K between user and sever
$\# X$	X is fresh
$A \triangleleft X$	A sees X
$A \mid\sim X$	A said X
$(X,Y)_K$	X and Y are hashed with the key K
$< X,Y >_K$	X is xored with the key K

2)Idealized scheme

$$U : \{r_u P\}_{U \overset{K}{\leftrightarrow} S}, \{k_u P, r_u P\}_{U \overset{K}{\leftrightarrow} S}, \{SK, r_{s_2} P\}_{U \overset{K}{\leftrightarrow} S}, < ID_U >_{r_s}$$

$$S : \{r_{s_2} P\}_{U \overset{K}{\leftrightarrow} S}, \{SK, r_u P\}_{U \overset{K}{\leftrightarrow} S}$$

3) Establish security goals

$$g_1 : S \mid\equiv U \mid\equiv U \overset{SK}{\leftrightarrow} S$$

$$g_2 : S \mid\equiv U \overset{SK}{\leftrightarrow} S$$

$g_3 : U \mid\equiv S \mid\equiv U \overset{SK}{\leftrightarrow} S$

$g_4 : U \mid\equiv U \overset{SK}{\leftrightarrow} S$

4) Initiative premises

$p_1 : U \equiv \#r_u$

$p_2 : U \mid\equiv \#r_{S_1}$

$p_3 : S \mid\equiv \#r_{S_1}$

$p_4 : S \mid\equiv \#r_{S_2}$

$p_5 : S \mid\equiv U \overset{K}{\leftrightarrow} S$

$p_6 : U \mid\equiv U \overset{K}{\leftrightarrow} S$

$p_7 : S \mid\equiv U \Rightarrow (U \overset{SK}{\leftrightarrow} S)$

$p_8 : U \mid\equiv S \Rightarrow (U \overset{SK}{\leftrightarrow} S)$

5) Analysis scheme

a_1: By p_5 and $S \triangleleft \{U \overset{SK}{\leftrightarrow} S, r_{S_2} P\}_{U \overset{K}{\leftrightarrow} S}$, according to the message-meaning rule, we obtain:

$S \mid\equiv U \mid\sim (U \overset{SK}{\leftrightarrow} S, r_{s_2} P)$.

a_2: By p_4 and a_1, according to the fresh conjuncatenation rule and nonce-verification rule,

we obtain: $S \mid\equiv U \mid\equiv (U \overset{SK}{\leftrightarrow} S, r_{s_2} P)$

g_1: By a_2, according to the belief rule, we obtain: $S \mid\equiv U \mid\equiv U \overset{SK}{\leftrightarrow} S$

g_2: By p_7 and g_1, according to the jurisdiction rule, we obtain: $S \mid\equiv U \overset{SK}{\leftrightarrow} S$

a_3: By p_6 and $U \triangleleft \{U \overset{SK}{\leftrightarrow} S, r_u P\}_{U \overset{K}{\leftrightarrow} S}$, according to the message-meaning rule, we obtain:

$U \mid\equiv S \mid\sim \{U \overset{SK}{\leftrightarrow} S, r_u P\}$.

a_4: By p_1 and a_3, according to the fresh conjuncatenation rule and nonce-verification rule,

we obtain: $U \mid\equiv S \mid\equiv (U \overset{SK}{\leftrightarrow} S, r_u P)$

g_3: By a_4, according to the belief rule, we obtain: $U \mid\equiv S \mid\equiv U \overset{SK}{\leftrightarrow} S$

g_4: By p_8 and g_3, according to the jurisdiction rule, we obtain: $U \mid\equiv U \overset{SK}{\leftrightarrow} S$.

6. Performance and functionality comparison

In this section, we will compare the performance and functionality of the enhanced scheme with other related authentication schemes using ECC [15-20]. Let T_{PM} , T_{PA}, T_H be the time for performing an elliptic curve point multiplication, an elliptic curve point addition and a hash function. We neglect XOR operation considering it needs very few computations. To estimate accurately for the running time, we use the jPBC library 2.0.0 [27] to perform the cryptographic primitives for thousand executions and take the arithmetic mean based on Windows 10 operating system, Pentium 3:20 GHz CPU, and 4.0GB RAM. The execution time for performing an elliptic curve point multiplication is approximately 10.5129 ms, an elliptic curve point addition is approximately 0.4338 ms and a hash function is approximately 0.0359 ms. **Table 3** shows the performance comparison. From Table 3, we see that the user side requires $3T_{PM} + 4T_H$ and the server side consumes as much as the user side. The results show that our schem has similar or better efficiency in comparison with other related ID based authentication schemes. In addition, we have only made a summing up of those security attributes which have been appeared by the authors of the related schemes. In our scheme, we adopt nonce based mechanism instead of timestamp, consider the scenario of compromised the private key and protect the user's identity based on the hard problem of Elliptic Curve Discrete Logarithmic. Therefore, our scheme can withstand track attack, key-compromise impersonation attack and avoid clock synchromication attack. As a consequence, in comparison to all other related schemes, our scheme supports much more security features and has thus proved to be more secure.

7.Conclusion

In this paper, we have shown that both Chou et al.'s scheme and Farash-Attari's scheme are insecure the trace attack and do have the problem of clock synchronization. In addition, we also demonstrated that Farash-Attari's scheme cannot resist the key-compromise impersonation attack. We then proposed an enhanced ID based mutual authentication scheme

with privacy protection to tackle these problems. According to the performance and functionality analyses compared with other related schemes, we show that the enhanced scheme is more secure and efficient for mobile networks.

Table 3. Performance cost

	Ours	**Farash-Attari[20]**	**Chou et al.[19]**	**He et al. [18]**	**Islam-Biswas [17]**	**Yoon-Yoo** [16]	**Yang-Chang** [15]
Key agreement phase	$6T_{PM}+8T_H \approx 63.36ms$	$6T_{PM}+10T_H \approx 63.43ms$	$6T_{PM}+8T_H \approx 63.36ms$	$6T_{PM}+9T_H \approx 63.40ms$	$7T_{PM}+4T_{PA}+6T_H \approx 75.54ms$	$7T_{PM}+4T_{PA}+12T_H \approx 75.76ms$	$8T_{PM}+5T_{PA}+8T_H \approx 86.56ms$
N_1	Yes	Yes	Yes	Yes	Yes	Yes	Yes
N_2	Yes	Yes	Yes	Yes	Yes	Yes	No
N_3	Yes	No	No	No	Yes	No	No
N_4	Yes	No	No	Yes	-	-	-
N_5	Yes	Yes	No	No	Yes	Yes	No
N_6	Yes	No	No	No	Yes	No	No

N_1:Providing mutual authentication; N_2:Providing the session key perfect forward secrecy; N_3: Withstanding trace attack;N_4: Withstanding key-cpmpromise impersonation attack; N_5: Withstanding impersonation attack; N_6: Avoiding clock synchromization attack.

References

[1] L. Lamport, "Password authentication with insecure communication," *Communications of the. ACM*, vol. 24, no.11, pp. 770-772, 1981. Article (CrossRef Link).

[2] Y. Chen, S.C. Chuang, L.Y. Yeh, J.L. Huang, "A practical authentication protocol with anonymity for wireless access networks," *Wireless Communications and Mobile Computing*, vol. 11, pp. 1366-1375, 2011. Article (CrossRef Link).

[3] R. Tso, "Security analysis and improvements of a communication-efficient three-party password authenticated key exchange protocol," *The Journal of Supercomputing*, vol. 66, pp. 863-874, 2013. Article (CrossRef Link).

[4] Y.P. Liao, C.M. Hsiao, "A novel multi-server remote user authentication scheme using self-certified public keys for mobile clients," *Future Generation Computer Systems*, vol. 29, no. 3, pp. 886-900, 2013. Article (CrossRef Link)

[5] W.B. Hsieh, J.S. Leu, "Anonymous authentication protocol based on elliptic curve Diffie–Hellman for wireless access networks," *Wireless Communications and Mobile Computing*, vol. 14, no. 10, pp. 995-1006, 2014. Article (CrossRef Link)

[6] H. Lu, L. Jie, "Privacy-preserving authentication schemes for vehicular ad hoc networks: a survey," *Wireless Communications and Mobile Computing*, 2014. Article (CrossRef Link)

[7] A. Shamir, "Identity-based cryptosystems and signature schemes," *Advances in Cryptology-CRYPTO'84*, Springer, New York, pp. 47-53, 1985. Article (CrossRef Link)

[8] D. Boneh, M. Franklin, "Identity-based encryption from the Weil pairing," *SIAM Journal on Computing*, vol. 32, no.3, pp. 586-615, 2003. Article (CrossRef Link)

[9] K. Shim, "Cryptanalysis of two ID-based authenticated key agreement protocols from pairings," *Cryptology ePrint Archive Report*, 357, 2005. Article (CrossRef Link)

[10] H.M. Sun, B.T. Hsieh, "Security analysis of Shim's authenticated key agreement protocols from pairings," *Cryptology ePrint Archive Report*, 113, 2003. Article (CrossRef Link)

[11] M. Hölbl, T. Welzer, B. Brumen, "An improved two-party identity-based authenticated key agreement protocol using pairings," *Journal of Computer and System Sciences*, vol. 78, pp. 142-150, 2012. Article (CrossRef Link)

[12] X.F. Cao, W.D. Kou, Y.U. Yu, R. Sun, "Identity-based authentication key agreement protocols without bilinear pairings," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 91, no. 12 , pp. 3833-3836, 2008. Article (CrossRef Link)

[13] V.S. Miller, "Use of elliptic curves in cryptography," *Advances in Cryptology-Crypto'85 Proceedings*, Springer Berlin, Heidelberg, 417, 1986. Article (CrossRef Link)

[14] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of computation*, vol. 48, pp. 417-426, 1987. Article (CrossRef Link)

[15] J.H. Yang, C.C. Chang, "An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem," *Computers & security*, vol.28, no. 3, pp. 138-143, 2009. Article (CrossRef Link)

[16] E.Yoon, K.Yoo, "Robust ID-based remote mutual authentication with key agreement protocol for mobile devices on ECC," in *Proc. of 2009 international conference on computational science and engineering*, pp. 633-640, 2009. Article (CrossRef Link)

[17] S.H. Islam, G.P. Biswas, "A more efficient and secure ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem," *Journal of Systems and Software*, vol.84, no.11, pp. 1892-1898, 2011. Article (CrossRef Link)

[18] D.B. He, J.H. Chen, J. Hu, "An ID-based client authentication with key agreement protocol for mobile client-server environment on ECC with provable security," *Information Fusion*, vol.13, no.3, pp. 223-230, 2011. Article (CrossRef Link)

[19] C.H. Chou, K.Y. Tsai, C.F. Lu, "Two ID-based authenticated schemes with key agreement for mobile environments," *The Journal of Supercomputing*, vol.66, no.(2): 973–988, 2013. Article (CrossRef Link)

[20] M.S. Farash, M.A. Attari, "A secure and efficient identity-based authenticated key exchange protocol for mobile client–server networks," *The Journal of Supercomputing*, vol. 69, pp. 395-411, 2014. Article (CrossRef Link)

[21] J.H. Yang, C.C. Chang, "An efficient three-party authenticated key exchange protocol using elliptic curve cryptography for mobile-commerce environments," *Journal of Systems and Software*, vol. 82, no. 9, pp. 1497-1502, 2009. Article (CrossRef Link)

[22] T.H. Chen, W.B. Lee, H.B. Chen, "A round-and computation-efficient three-party authenticated key exchange protocol," *Journal of Systems and Software*, vol.81, no. 9, pp. 1581-1590, 2008. Article (CrossRef Link)

[23] Z.W. Tan, "An enhanced three-party authentication key exchange protocol for mobile commerce environments," *Journal of Communications*, vol. 5, no. 5, pp. 436-443, 2010. Article (CrossRef Link)

[24] D.B. He, Y.T. Chen, and J.H. Chen, "An ID-based three-party authenticated key exchange protocol using elliptic curve cryptography for mobile-commerce environments," *Arabian Journal for Science and Engineering*, vol.38, no. 8, pp. 2055-2061, 2013. Article (CrossRef Link)

[25] M. Burrow, M. Abadi, R.M. Needham, "A logic of authentication," *ACM Transactions on Computer Systems*, vol. 8: 18-36, 1990. Article (CrossRef Link)

[26] K.E. Lauter, and K.E. Stange, "The elliptic curve discrete logarithm problem and equivalent hard problems for elliptic divisibility sequences," *Selected Areas in Cryptography*, Springer Berlin Heidelberg, 309-327, 2009. Article (CrossRef Link)

[27] Java Pairing Based Cryptography Library (jPBC). Article (CrossRef Link)

Yanrong Lu received the M.S. degree in cryptography from Xidian University of China, Xi'an, China, in 2012. she is currently a Ph.D. student in Beijing University of Posts and Telecommunications, Beijing, China. Her research interests is focused on information security and cryptography, in particular, cryptographic protocols. E-mail:luyanrong1985@163.com

Lixiang Li received the M.S. degree in circuit and system from Yanshan University, Qinhuangdao, China, in 2003, and the Ph.D. degree in signal and information processing from Beijing University of Posts and Telecommunications, Beijing, China, in 2006. She is currently a professor at the School of Computer Science, Beijing University of Posts and Telecommunications, China. Her research interests include swarm intelligence, information security and network security. Prof. L. Li is the co-author of 70 scientific papers and 10 Chinese patents. E-mail:li_lixiang2006@163.com

Haipeng Peng received the M.S. degree in system engineering from Shenyang University of Technology, Shenyang, China, in 2006, and the Ph.D. degree in signal and information processing from Beijing University of Posts and Telecommunications, Beijing, China, in 2010. He is currently an associate professor at the School of Computer Science, Beijing University of Posts and Telecommunications, China. His research interests include information security, network security, complex networks and control of dynamical systems. Dr. H. Peng is the coauthor of 50 scientific papers and over 10 Chinese patents. E-mail:penghaipeng@bupt.edu.cn

Yixian Yang received the M.S. degree in applied mathematics in 1986 and the Ph.D. degree in electronics and communication systems in 1988 from Beijing University of Posts and Telecommunications, Beijing, China. He is the Managing Director of information security center, Beijing University of Posts and Telecommunications, Beijing, China. His research interests include network security, information security and coding theory. Dr. Y. Yang is the co-author of 300 scientific articles and 50 patents. E-mail:yxyang@bupt.edu.cn