An Efficient Privacy-Preserving Handover Authentication Scheme for Mobile Wireless Network

Jiaqing Mo[1](✉), Zhongwang Hu[1], and Yuhua Lin[2]

[1] School of Computer Science and Software, Zhaoqing University,
Zhaoqing 526061, China
mojiaqing@126.com

[2] Education Technology and Computer Center, Zhaoqing University,
Zhaoqing 526061, China

Abstract. An efficient and secure authentication protocol is essential to enable the mobile devices handover seamlessly to a different access point. However, due to the limited computation resource and battery capacity in mobile devices as well as the openness and insecurity of wireless channel, designing an efficient and secure handover scheme for wireless network is a challenging task. Furthermore, most of the existing handover schemes are vulnerable to various kinds of attacks and cannot yield good performance. According to the analysis of the current schemes, we summarize the security goals that should be fulfilled by the handover authentication scheme. In this paper, we present a new handover authentication and key agreement scheme on elliptic curve cryptosystem for mobile wireless networks which does not involve the trusted third party and provides privacy-preserving mutual authentication between mobile devices and the access point. The proposed scheme consists of three phases: system setup, handover preparation, handover authentication. We give the details of each phase. The theoretical analysis indicates that the proposed scheme achieves universal security features. The secrecy of the generated session key and mutual authentication of the proposed scheme are verified by ProVerif. In addition, performance comparison shows that the proposed scheme outperforms the related schemes in terms of computation cost and communication overhead.

Keywords: Handover authentication · Anonymity · Privacy · Efficiency
Mobile wireless networks

1 Introduction

With the development of wireless communication technology (e.g. WiFi, WiMax, LTE) and the popularity of mobile intelligent terminal (e.g., smartphone, tablet PC), the network brings more and more convenience to the people. The requirement of users on network mainly in mobility support and business diversification have become an increasingly high demand, especially the real-time services such as interactive

X. Sun et al. (Eds.): ICCCS 2018, LNCS 11065, pp. 490–505, 2018.
https://doi.org/10.1007/978-3-030-00012-7_45

streaming and voice also bring challenges to the mobile wireless networks (MWN). Compared with the limitation of the traditional wired networks, the MWN arouses the interest in industry and academia for its deploying flexibility, easy installation, low cost and mobility [1, 2]. A typical MWN involves three kinds of entities, i.e. many mobile terminals (MTs), a lot of access points (APs), an authentication server (AS). Each *AP* has limited geographic coverage, when a MT moves out of the current AP's coverage, it needs to handover to the new *AP* to continue the ongoing sessions. As discussed in [3], the total handover time should be limited to 50 ms, and the ideal time of the authentication module should not exceed 20 ms. In order to provide seamlessly continuous access services for the mobile terminals, it is essential to design a secure and efficient handoff authentication protocol to reduce communication latency and improve Quality-of-Service (QoS).

A handover authentication overview is showed in Fig. 1. In the authentication process, a *MT* first submits relevant information to the *AS* for registration, then connects to an *AP* and subscribes services or starts a session with other MT. In the course of the session, if the *MT* moves from the current *AP* (e.g., *AP1*) to another *AP* (e.g., *AP2*)'s coverage, the handover authentication mechanism should be performed between the *MT* and the *AP2*. By this way, the *MT* and the *AP2* can authenticate each other and generate a session key in order to provide integrity and confidentiality for the future communication. Meanwhile, the illegal users are prevented from unauthorized access.

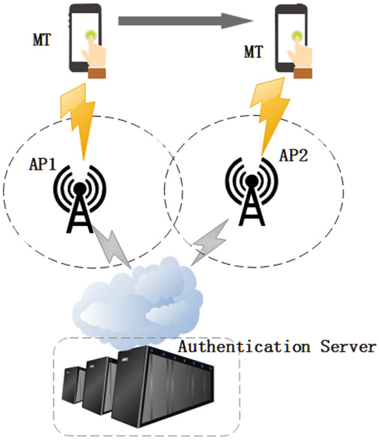

Fig. 1. A typical handover authentication scenario in mobile wireless networks

1.1 Related Works

Since the messages are transmitted between the related parties in a wireless channel instead of a wired connection, this provides an opportunity for an adversary to eavesdrop the transferred messages and temper with them. Thus, security and privacy are serious issues in handover authentication services. In particular, mobile users are extremely concerned about the protection of sensitive information such as their identity and location. Therefore, the handover authentication should achieve the user anonymity and untraceability.

For the purpose of improving efficiency and preserving user privacy, a number of handover authentication schemes using different methods have been proposed for MWN. In these schemes, elliptic curve cryptosystem (ECC), provides the same security level with smaller keys and faster computation compared with the other public key cryptography such as RSA, e.g., a 160-bit ECC based public key can provide security level of 1024-bit RSA based public key. Thus, the authentication schemes based on ECC are more beneficial for mobile devices than other cryptosystems.

To achieve efficiency and handover seamlessly, He et al. [3] proposed a handover authentication scheme named PairHand on bilinear pairing, in which they introduced the concept of short-lived unlinkable pseudonyms and the corresponding private keys to preserve user privacy. Moreover, considering to reduce the communication overhead and alleviate the heavy burden on *AS*, their scheme just requires two handshakes for handover authentication and key agreement between the mobile client and the *AP*. However, He et al. [4] and Yeo et al. [5] pointed out that PairHand is insecure since the private key of mobile client can be recovered by adversary from the signature in the transferred message, and they presented an improved version to fix the security weakness respectively. Later, Tsai et al. [6] and Wang et al. [8] found that the enhanced version of PairHand cannot withstand an attack named algorithm of Pohlig and Hellman [7], and the private key can be recovered from signature by employing linearly combining method, respectively. And they also put forward the countermeasures to eliminate the security risks. However, the security of handover protocols [3, 4, 6, 8, 9] rely on time-consuming bilinear pairings leading to inefficient with regard to computation cost and cannot improve performance of PairHand and its improved version.

It is very important to improve efficiency of the handover authentication for mobile client in which computation capability is inefficient and battery power is limited while maintaining the security in wireless network. For this purpose, some studies have been proposed with pairing-free for handover services [10–14]. Sun et al. [10] described a certificateless authenticated key agreement protocol with pairing-free and claimed it is practical for low-power devices, but the excessive operations of elliptic curve multiplication make it hard to be implemented on mobile devices. Islam and Khan [11] presented an identity-based handover authentication protocol with pairing-free for WMW. In addition, in order to achieve the goal of efficiency, their protocol adopts light-weight hash function instead of time-consuming map-to-point hash function. In 2012, Cao et al. [15] proposed a handover authentication schemes with pairing-free for mobile networks to decrease the system complexity and computation cost. However, Li et al. [16] found that Cao et al.'s protocol failed to achieve true user anonymity and untraceablity, then put forward a privacy-aware identity-based scheme for mobile devices without pairing operation, and argued that their new scheme can provide user anonymity, resistance to replay attack and mutual authentication. Unfortunately, Xie et al. [13] pointed out that Li et al. [16]'s scheme is suffered from impersonation attack in the response of the handover authentication phase and cannot provide mutual authentication. As a remedy, Xie et al. presented an improved handover authentication scheme. However, both Li et al. [16] and Xie et al. [13] suffered from impersonation attack, because in their authentication phase, the request message contains all the parameters to construct verified expression in the *AP* side, and this request message transferred in public channel can be intercepted by the adversary, as a result, the adversary can select some parameters satisfying the form of verified expression and fake a request message and send it to *AP*, thus the *AP* would consider the adversary as a legal user. In the same year, Chaudhry et al. [14] also showed that the scheme in [16] is suffered from access point impersonation attack and proposed an improved scheme. However, there is a mistake in the authentication phase of their scheme, that is when the *AP* computes the parameter Z_j, the *AP* does not know m_j in advance. There are some other recent studies [17–21] proposed the user authentication schemes with privacy preservation using different techniques for mobile devices. Unfortunately, these schemes are found neither satisfy some security requirement nor be practical for mobile environment [22–26].

As the analysis aforementioned, due to their different inherent design weakness, most of the current handover authentication schemes are either insecure to withstand some serious attacks [13, 15, 16], or inefficient to be implemented in MWN [10]. As pointed out in [25], to date, how to develop a privacy-preserving handover authentication scheme which can withstand various known attacks while maintaining efficiency, is still an open problem.

1.2 Our Contribution

Motivated by above observation, we propose a new efficient and robust handover authentication protocol making use of ECC algorithm in MWN context. In short, our protocol has the following features:

- The proposed protocol is more efficient than the other related works with regard to computation cost and communication overhead.
- The proposed protocol not only achieves user anonymity and user untraceablity, but also provides mutual authentication and fast handover authentication with two handshakes between the *MT* and the *AP* in heterogeneous wireless network environment.
- The proposed protocol is proved to be secure with cryptographic protocol verifier ProVerif.

The rest of the paper is organized as follows: In Sect. 2, we give a brief view of preliminary and security goals. Details of our handover authentication protocol for WMN are described in Sect. 3, the security analysis and formal security verification are incorporated in Sect. 4. Next, the performance comparison is introduced in Sect. 5. Finally, conclusions are drawn in Sect. 6.

2 Preliminary and Security Goals

In this section, we provide a brief description of mathematical problems on elliptic curve and the security goals.

2.1 Mathematical Problems

An elliptic curve E/F_p is defined by the equation y^2 mod $p = x^3 + ax + b\ mod\ p$, where p is a big prime number, and a, $b \in F_p$ with $(4a^3 + 27b^2)\ mod\ p \neq 0$. Two important mathematical problems that rely on the elliptic curve are described below.

Elliptic Curve Discrete Logarithm Problem (ECDLP): Given Q, $P \in G$, find an integer $a \in [1, p - 1]$ such that $Q = aP \in G$ is hard.
Computational Diffie-Hellman Problem (CDHP): Given (P, aP, bP) for any a, $b \in [1, p - 1]$, finding $abP \in G$ is hard.

2.2 Security Goals

A secure handover protocol should achieve the following goals:

Anonymity: Except AS, the MT's identity should be unknown to other entities including AP.
Untraceability: No strong global adversaries can track the actions of MTs.
Mutual authentication: Both MT and AP should authenticate each other over insecure channels without disclosing their identities.
Key agreement: The MT and AP should establish a symmetric session key to encrypt the messages in their future conversations. Additionally, the session key should not be compromised to compute previous keys and the future ones. This means the scheme can provide backward and forward secrecy.
Robustness: The protocol should be able to withstand various kinds attacks like impersonation attack, replay attack, man-in-middle attack, etc.
Integrity: The transferred messages via open channels should not be tempered, replayed, altered by adversaries. Also, the eavesdropped messages should prevent the adversaries from getting plaintext.

3 The Proposed Protocol

In this section, we present a new efficient mutual authentication protocol for WMN. Our protocol consists of three phases, i.e., system setup phase, handover preparation phase, handover authentication phase.

3.1 System Setup Phase

The AS selects a security parameter n as an input to generate all the system parameter in the following ways:

(1) Chooses a t-bit prime number p and the field size q where $q = 2p + 1$ and generates an elliptic curve E/F_P which is defined on a finite field F_p with order p, an additive cyclic group G over E/F_P with order q and determines a generator P of G.
(2) Selects the master key $s \in Z_q^*$, and computes $K_{pub} = sP$ as the public key.
(3) Selects five one way hash functions $H_1(), H_2(), H_3(): \{0,1\}^* x\ G \rightarrow \{0,1\}^n$.
(4) Publishes system parameter $\{F_P, E/F_P, p, P, K_{pub}, G, H_1(), H_2(), H_3()\}$ and keeps s secretly.

Afterwards, the *AS* computes the private key and the public key for each *AP*:

(1) Assigns a unique ID_{AP} for each *AP*.
(2) Selects a random number $r_j \in Z_q^*$, computes $R_j = sH_1(ID_{AP}||r_j)$, sets the tuple (r_j, R_j) as the private key of *AP*. '||' is the concatenate operation.
(3) Assume that a pre-shared key has been built between *AP* and *AS* before. The *AS* encrypts the tuple (r_j, R_j) with the pre-shared key and emits them to the *AP*.

Upon receiving the encrypted message, the *AP* decrypts (r_j, R_j) and keeps (r_j, R_j) secret, and computes $K_{AP} = R_jP$ as his public key.

3.2 Handover Preparation Phase

When the *MT* registers to *AS* with his real ID, in order to provide user anonymity and untraceability, the *AS* selects a set of unlink-able pseudo-identifiers $(PID_1, PID_2, \ldots, PID_n)$ for the *MT*. For each pseudo-ID PID_i, *AS* computes a private key and the corresponding public key *AS* follows:

(1) *AS* selects $r_i \in Z_q^*$ at random, and computes $R_i = r_iP$.
(2) *AS* computes $d_i = r_i + sH_1(PID_i||R_i)$.
(3) *AS* sends (PID_i, d_i, R_i) to *MT* via a secure channel.

MT sets (d_i, R_i) *AS* his private key after receipt of the tuple (PID_i, d_i, R_i) from *AS*, and computes his public key $D_i = d_iP = R_i + H_1(PID_i||R_i)K_{pub}$.

3.3 Handover Authentication Phase

Assume the *AP* periodically broadcasts a beacon message with its identity, public key and other regular information to declare service existence. If *MT* moves out of the coverage of current *AP* and receives the beacon message of the new *AP*, he extracts the identity and the public key and performs handover authentication with the new *AP AS* follows:

(1) $MT \rightarrow AP$: $\{PID_i, h_{MT}, R_i, S, D_i\}$

MT selects a random number $a \in Z_q^*$, and computes $T_{MT} = AP$, then MT generates a signature $S = a/(d_i + h_{MT})$ with private key d_i, where $h_{MT} = H_2(T_{MT}||PID_i)$. Finally, MT sends the message $\{PID_i, h_{MT}, R_i, S, D_i\}$ to the target AP.

(2) $AP \rightarrow MT$: $\{ID_{AP}, PT_{AP}, MAC\}$

On receiving the message, AP computes $h_{AP} = H_2(PID_i||R_i)$, $(T_{MT'} = S(R_i + h_{AP}K_{pub} + \mathrm{h}_{MT}P)$, and checks whether the equation $H(T_{MT'}||PID_i)\ ? = h_{MT}$ holds. If it is unsuccessful, AP aborts this session. Otherwise, AP selects a random number $b \in Z_q^*$, computes $T_{AP} = bP, K_{am} = D_i \cdot b \cdot K_{AP}, l_{AP} = H_2(ID_{AP}||r_j), PT_{AP} = T_{MT'} \oplus (l_{AP}||T_{AP})$, and the message authentication code $MAC = H_3(PID_i||K_{am}||T_{MT'}||ID_{AP})$. Finally, AP sends the message $\{ID_{AP}, PT_{AP}, MAC\}$ to MT. '$\oplus$' is the exclusive-or operation (XOR).

(3) After receipt of message from P, MT computes $(l_{AP}||T_{AP}) = PT_{AP} \oplus T_{MT}$, the session key $K_{ma} = d_i \cdot T_{AP} \cdot l_{AP} \cdot K_{pub}$, $MAC' = H_3(PID_i||K_{ma}||T_{MT}||ID_{AP})$. MT further verifies the equation $MAC' = MAC$. If the result is unsuccessful, the MT terminates this session. Otherwise, MT treats the AP AS a legal service provider, and completes the mutual handover authentication. Finally, a secure channel is established with the session key K_{am} $(=K_{ma})$ between MT and AP.

The proposed handover authentication phase is shown in Fig. 2.

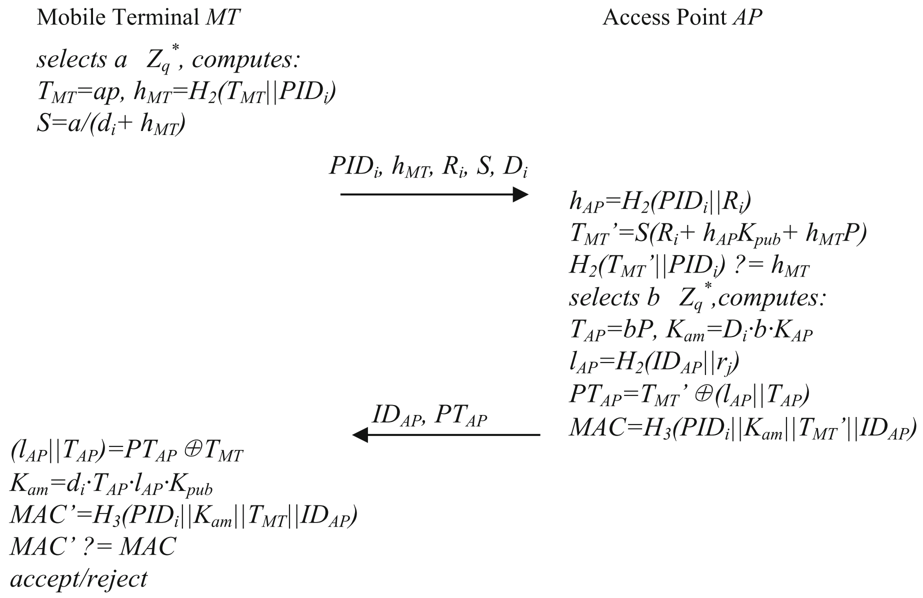
Mobile Terminal MT
Access Point AP
selects a Z_q^*, computes:
T_{MT}=ap, $h_{MT}=H_2(T_{MT}||PID_i)$
$S=a/(d_i+h_{MT})$
$PID_i, h_{MT}, R_i, S, D_i$
$h_{AP}=H_2(PID_i||R_i)$
$T_{MT}'=S(R_i+h_{AP}K_{pub}+h_{MT}P)$
$H_2(T_{MT}'||PID_i)\ ?= h_{MT}$
selects b Z_q^*,computes:
$T_{AP}=bP, K_{am}=D_i{\cdot}b{\cdot}K_{AP}$
$l_{AP}=H_2(ID_{AP}||r_j)$
$PT_{AP}=T_{MT}'\oplus(l_{AP}||T_{AP})$
$MAC=H_3(PID_i||K_{am}||T_{MT}'||ID_{AP})$
ID_{AP}, PT_{AP}
$(l_{AP}||T_{AP})=PT_{AP}\oplus T_{MT}$
$K_{am}=d_i{\cdot}T_{AP}{\cdot}l_{AP}{\cdot}K_{pub}$
$MAC'=H_3(PID_i||K_{am}||T_{MT}||ID_{AP})$
$MAC'\ ?= MAC$
accept/reject

Fig. 2. Handover authentication phase

4 Security Analysis and Formal Security Verification

4.1 Security Analysis

we analyze the security of the proposed protocol with regard to security goals described in Subsect. 2.2.

4.1.1 Mutual Authentication and Key Agreement

In the handover authentication phase, *AP* verifies the legitimacy of *MT* based on the signature *S*, and *MT* verifies the legitimacy of *AP* based on his private key and *AP*'s public information issued by *AS*. If one of these two verifications is unsuccessful, the session would be aborted. Otherwise, the proposed protocol achieves mutual authentication between *MT* and *AP*.

It is easy to see that the session key K_{am} generated by *AP* and K_{ma} generated by *MT* are identical, which is shown *AS* follows:

$$\begin{aligned}K_{am} &= D_i \cdot b \cdot K_{AP}\\ &= d_i \cdot P \cdot b \cdot s \cdot H_2(ID_{AP}||r_j) \cdot P\\ &= d_i \cdot b \cdot P \cdot H_2(ID_{AP}||r_j) \cdot s \cdot P\\ &= d_i \cdot T_{AP} \cdot l_{AP} \cdot K_{pub}\\ &= K_{ma}\end{aligned}$$

4.1.2 Provide User Anonymity and Untraceability

In the proposed scheme, each *MT* will obtain a series of pseudo identifiers PID_i $(1 \leq i \leq n)$ and the corresponding secret key d_i when he registers in *AS*. And at the beginning of the handover authentication phase, *MT* picks an unused PID_i to replace his real identifier in order to preserve privacy. Therefore, only *AS* knows the relationship between pseudo identifier PID_i and the real *ID* of *MT*. Furthermore, the adversary, even the *AP* cannot discern the two sessions whether are initiated by the same *MT* because there is no link between these pseudo identifiers.

4.1.3 Resistance to Attacks

The design of a secure protocol needs to consider the ability to resist various attacks. Our protocol can meet this requirement. For replay attack, if the adversary intercepts the message $\{PID_i, h_{MT}, R_i, S, D_i\}$ and impersonate *MT* to replay this message to *AP*, but the adversary cannot compute a right MAC' to pass *MT*'s verification without the knowledge of *a* and T_{MT}. Moreover, if the adversary intends to impersonate the *AP* and replay $\{ID_{AP}, PT_{AP}, MAC\}$ to *MT*, it is infeasible because the random number *b* is different in each exchanged message. For man-in-the-middle attack, the key agreement of proposed protocol is based on the ECDLP and CDHP, and the session key between *MT* and *AP* is established with partial keys from each party which are long-term private keys so that the proposed protocol can prevent the attacker from eavesdropping the exchanged message to forge or replay the messages in the middle. It is also infeasible for the adversary impersonating the authorized *MT* or *AP* to receive data message owing to the fact that the long term secret key of participant is issued by the *AS*.

4.1.4 Provide Forward and Backward Secrecy

In the proposed protocol, the session key $K_{ma} = d_i \cdot T_{AP} \cdot l_{AP} \cdot K_{pub}$ is computed by *MT* and the session $K_{ma} = D_i \cdot b \cdot K_{AP}$ is computed on *AP* side. The forward secrecy and the backward secrecy is to say that if the private key d_i of *MT* and the private key r_j of *AP* are comprised, the adversary cannot breach the secrecy of the session key whether it is previous or subsequent. It is clear that if the private key d_i of *MT* and the private key r_j of *AP* are comprised, the adversary cannot compute K_{am} or K_{ma} without the knowledge of secret number *a* and *b*. Moreover, the random number *a* and *b* are selected by *MT* and *AP* when *MT* moves out of the coverage of current *AP* and performs the handover authentication mechanism everytime. Thus, the proposed protocol can provide forward and backward secrecy.

4.2 Formal Security Verification via ProVerif

ProVerif is an effective automatic cryptographic protocol verifier based on pi calculus in Dolev-Yao model [27] and implements many cryptographic primitives, such as symmetric encryption and asymmetric encryption, signatures, hash, mac, Diffie-Hellman key agreements. Many protocols have been tested by ProVerif to prove their secrecy, authentication and other correspondence properties [27]. Here, we use ProVerif to provide a formal security verification of the proposed protocol to ensure that our scheme can provide the secrecy and authentication property.

According to the protocol description, we introduce three channels, channel *ch1* is used for the secure (private) communication between *AP* and *AS*, channel *ch2* is used for secure communication between *MT* and *AS*. In particular, channel *ch3* models the public insecure communication between *MT* and *AP*.

```
(*Channels*)
free ch1:channel [private].
free ch2:channel [private].
free ch3:channel.
```

Next, we define two private variables *kma* and *kam*, which represent the session keys generated by *MT* and *AP*, respectively.

```
(*Session key*)
free kam,kma:bitstring [private].
```

The constants and variables are declared *AS* follows:

```
(*constants and varibles*)
const P: bitstring.
const p: bitstring.
const q: bitstring.
free IDi: bitstring.
free ID_AP: bitstring.
free IDj: bitstring.
free Kpub:bitstring.
free PIDi: bitstring.
free PIDx: bitstring.
```

The cryptographic functions are described as follows.

```
(*Constructor*)
fun concat(bitstring,bitstring):bitstring.
fun mult(bitstring,bitstring):bitstring.
fun add(bitstring,bitstring):bitstring.
fun syme(bitstring,bitstring):bitstring.
fun inverse(bitstring):bitstring.
fun xor(bitstring,bitstring):bitstring.
fun H1(bitstring):bitstring.
fun H2(bitstring):bitstring.
fun H3(bitstring):bitstring.
fun fp(bitstring):bitstring.(*former part*)
fun bp(bitstring):bitstring.(*back part*)
```

To model the symmetric decryption, the destructor is introduced.

```
(*destructor and equations*)
reduc forall m:bitstring,key:bitstring;symd(syme(m,key),key)=m.
```

Four events are introduced to verify the mutual authentication between *MT* and *AP*. For example, event *beginAP* represents that *AP* receives the authentication request from *MT*, the event *endAP* occurs says that *AP* sends the response to *MT*. In particular, we can use ProVerif to ensure the authenticity by testing whether the begin event occurs before the end event.

```
(*events*)
event beginAP(bitstring).
event endAP(bitstring).
event beginMT(bitstring).
event endMT(bitstring).
```

We define three distinct process macros *AServer*, *APoint*, *MTerminal* for participant *AS*, *AP*, *MT* in terms of the operations of *AS*, *AP*, *MT* during the proposed protocol execution, respectively. The macro *AServer* is modeled as follows.

```
(*Authentication Server*)
let AServer=
new s: bitstring;
let Kpub = mult(s, P) in
new rj: bitstring;
let Rj = mult(s,H1(concat(IDi,rj))) in
out (ch1,(rj,Rj));
new ri: bitstring;
let Ri = mult(ri,P) in
let di = add(ri,mult(s,H1(concat(PIDi,Ri)))) in
out(ch2,(PIDi,di,Ri)).
```

The macro *APoint* is modeled as follows.

```
(*Access Point*)
let APoint=
in(ch1,(Xrj:bitstring,XRj:bitstring));
   let K_AP=mult(XRj,P) in
event beginAP(IDi);
out(ch3, (XRj,IDj));
in(ch3,(XPIDi:bitstring,
      Xh_MT:bitstring,XRi:bitstring,XS:bitstring,XDi:bitstring));
let h_AP=H2(concat(XPIDi,XRi)) in
let T_MT' = mult(XS,add(XRi,add(mult(h_AP,Kpub),mult(Xh_MT,P)))) in
let  Xh_MT'=H2(concat(T_MT',XPIDi)) in
if (Xh_MT = Xh_MT') then
   new b:bitstring;
   let T_AP=mult(b,P) in
   let kam=mult(XDi,mult(b,K_AP)) in
   let l_AP=H2(concat(ID_AP,Xrj)) in
   let PT_AP=xor(T_MT',concat(l_AP,T_AP))  in
   let MAC_AP=H3(concat(XPIDi,concat(kam,concat(T_MT',ID_AP)))) in
   out(ch3,(ID_AP,PT_AP,MAC_AP));
   event endAP(IDi).
```

The macro *MTerminal* is modeled as follows.

```
(*Mobile Terminal*)
   let MTerminal=
   in(ch2,(XPIDi:bitstring,Xdi:bitstring,XRi:bitstring));
   let Di=mult(Xdi,P) in
   in(ch3,(XRj:bitstring, XIDj:bitstring));
   event beginMT(PIDx);
   new a:bitstring;
   let T_MT=mult(a,P) in
   let h_MT=H2(concat(T_MT,XPIDi)) in
   let S=mult(a,inverse(add(Xdi,h_MT))) in
   out(ch3,(XPIDi,h_MT,XRi,S,Di));
   in(ch3,(XID_AP:bitstring,XPT_AP:bitstring,XMAC_AP:bitstring));
   let lAP_TAP=xor(XPT_AP,T_MT) in
   let l_AP'=fp(lAP_TAP) in
   let T_AP'=bp(lAP_TAP) in
   let kma = mult(Xdi,mult(T_AP',mult(l_AP',Kpub))) in
    let MAC_MT=H3(concat(XPIDi,concat(kma,concat(T_AP',XIDj)))) in
    if (MAC_MT=XMAC_AP) then
      event  endMT(PIDx).
```

The modeled protocol is emulated *AS* running in parallel for these three macros *AS* follows.

```
process((!AServer) | (!APoint) | (!MTerminal))
```

In order to verify the adversary's capabilities in breaching the secrecy of the session key K_{ma} generated by *MT* and K_{ma} generated by *AP* (K_{ma} and K_{ma} are actually equal), we define the queries as follows:

```
query attacker(kam).
query attacker(kma).
```

Furthermore, to verify the mutual authentication between *MT* and *AP*, we model the correspondence assertions as follows:

```
query id:bitstring;inj-event(endAP(id))==>inj-event(beginAP(id)).
query id:bitstring;inj-event(endMT(id))==>inj-event(beginMT(id)).
```

The output of these processes as running in ProVerif v1.98 (latest version) is showed as follows.

1 RESULT inj-event(endMT(id)) ==> inj-event(beginMT(id)) is true.
2 RESULT inj-event(endAP(id_1254)) ==> inj-event(beginAP(id_1254)) is true.
3 RESULT not attacker(kma[]) is true.
4 RESULT not attacker(kam[]) is true.

The experimental result in line 1–2 indicates that the proposed protocol can provide mutual authentication between *MT* and *AP*. Meanwhile, line 3–4 shows that the attacker cannot obtain the session key K_{am} or K_{ma}. In other words, because all these results are true, attacker can neither break the secrecy of the session key generated by each party nor break the authentication property that is verified by correspondence assertions in Dolev_Yao model.

5 Performance Comparison

In this section, we compare the computation cost and communication overhead in handover authentication phase with related protocols [13, 14, 28].

We set q to be the order of the super singular curve, p to be the order of non-super singular curve E over a finite field F_p, and their values are set to 512 bits and 160 bits, respectively. For brevity, let T_m, T_a be the execution time for an elliptic curve multiplication in G, the execution time for an elliptic curve addition in G, respectively. The execution time of other operations, e.g., a one-way hash function operation and a message authentication code operation, are ignored because they are much less than that of T_m or T_a. All of the cryptographic operations are benchmarked on environment *AS* follows: PBC library (version 0.5.14) on 32-bit [29], 3.4 GHz Intel i7 processor, 2 GB main memory, running Ubuntu desktop 14.04. In our experiment, T_m takes approximately 0.017 ms, while T_a takes 0.013 ms. The comparison of computation cost between our scheme and the related protocols is shown Table 1.

Table 1. Computation cost comparison

Scheme	Computation cost of *MT*	Computation cost of *AP*
[13]	$5T_m + 4T_a \approx 0.137$ ms	$6T_m + 4\ T_a \approx 0.154$ ms
[14]	$4\ T_m + 4\ T_a \approx 0.120$ ms	$7\ T_m + T_a \approx 0.171$ ms
[28]	$6\ T_m + 2\ T_a \approx 0.128$ ms	$6\ T_m + 2\ T_a \approx 0.128$ ms
Ours	$5\ T_m + T_a \approx 0.098$ ms	$5\ T_m + T_a \approx 0.098$ ms

To facilitate comparison in communication overhead, we set l_{i}, l_{p}, l_{h}, l_{t}, l_{mac} be the length of client's identifier, a point, an one-way hash value, a timestamp, a message authentication code, respectively. And their corresponding values are defined as 32 bits, 1024 bits, 160 bits, 32 bits, 160 bits, respectively. Table 2 demonstrates the comparison of communication overhead between our scheme and the related protocols.

Table 2. Communication overhead comparison

Scheme	Message components	Communication overhead
[13]	$2l_{\mathrm{i}} + 6l_{\mathrm{p}} + l_{\mathrm{t}} + l_{\mathrm{mac}}$	6400 bits
[14]	$2l_{\mathrm{i}} + 4l_{\mathrm{p}} + l_{\mathrm{t}} + l_{\mathrm{mac}}$	4352 bits
[28]	$2l_{\mathrm{i}} + 4l_{\mathrm{p}} + 2l_{\mathrm{h}}$	4480 bits
Ours	$2l_{\mathrm{i}} + 4l_{\mathrm{p}} + l_{\mathrm{h}}$	4320 bits

From Table 1, we can learn that on both *MT* and *AP*, the consumed time of the proposed scheme is 0.098 ms, which is much less than other related protocols [13, 14, 28]. Thus, the proposed scheme is more efficient than [13, 14, 28] both on *MT* side and *AP* side. Moreover, from Table 2, we can see that the communication overhead of our scheme is 4320 bits, which is slightly lower than that of [14] and decreases greatly *AS* compared with [13, 28]. Therefore, the proposed scheme has the advantage in communication overhead compared with [13, 14, 28]. Overall, the proposed scheme has better performance than [13, 14, 28].

6 Conclusion

In this paper, we summarize the current handover authentication schemes and put forward an efficient anonymous handover authentication protocol with privacy-preserving for mobile wireless network. Owing to the hardness of ECDLP and CDHP assumption, the proposed scheme has merits of efficiency and robust security. We also provide a formal security verification via the automatic cryptographic protocol verifier ProVerif to show that our scheme can preserve the secrecy of the session key and provide mutual authentication property. In particular, our protocol achieves excellent performance as compared with the related up-to-date handover protocols. Based on these merits, we are convinced that the proposed scheme provides a reasonable deployment solution for handover in mobile wireless network.

References

1. Fu, L., et al.: Joint optimization of multicast energy in delay-constrained mobile wireless networks. IEEE/ACM Trans. Netw. **99**, 633–646 (2018)
2. Pedersen, J., i Amat, A.G., Andriyanova, I., Brannstrom, F.: Distributed storage in mobile wireless networks with device-to-device communication. IEEE Trans. Commun. **64**, 4862–4878 (2016)
3. He, D., Chen, C., Chan, S., Bu, J.: Secure and efficient handover authentication based on bilinear pairing functions. IEEE Trans. Wirel. Commun. **11**, 48–53 (2012)
4. He, D., Chen, C., Chan, S., Bu, J.: Analysis and improvement of a secure and efficient handover authentication for wireless networks. IEEE Commun. Lett. **16**, 1270–1273 (2012)
5. Yeo, S.L., Yap, W.S., Liu, J.K., Henricksen, M.: Comments on "analysis and improvement of a secure and efficient handover authentication based on bilinear pairing functions". IEEE Commun. Lett. **17**, 1521–1523 (2013)

6. Tsai, J.L., Lo, N.W., Wu, T.C.: Secure handover authentication protocol based on bilinear pairings. Wirel. Pers. Commun. **73**, 1037–1047 (2013)
7. Pohlig, S.C., Hellman, M.E.: An improved algorithm for computing logarithms over GF(p) and its cryptographic significance. IEEE Trans. Inform. Theory **24**, 106–110 (1978)
8. Wang, W., Hu, L.: A secure and efficient handover authentication protocol for wireless networks. Sensors **14**, 11379–11394 (2014)
9. He, D., Khan, M.K., Kumar, N.: A new handover authentication protocol based on bilinear pairing functions for wireless networks. Int. J. Ad Hoc Ubiquitous Comput. **18**, 67–74 (2015)
10. Sun, H., Wen, Q., Zhang, H., Jin, Z.: A novel pairing-free certificateless authenticated key agreement protocol with provable security. Front. Comput. Sci. **7**, 544–557 (2013)
11. Islam, S.H., Khan, M.K.: Provably secure and pairing-free identity-based handover authentication protocol for wireless mobile networks. Int. J. Commun. Syst. **29**, 2442–2456 (2016)
12. Chang, C.C., Huang, Y.C., Tsai, H.C.: Design and analysis of chameleon hashing based handover authentication scheme for wireless networks. J. Inf. Hiding Multimedia Sig. Process. **5**, 107–116 (2014)
13. Xie, Y., Wu, L., Kumar, N., Shen, J.: Analysis and improvement of a privacy-aware handover authentication scheme for wireless network. Wirel. Pers. Commun. **93**, 523–541 (2017)
14. Chaudhry, S.A., Farash, M.S., Naqvi, H., Islam, S.H., Shon, T.: A robust and efficient privacy aware handover authentication scheme for wireless networks. Wirel. Pers. Commun. Int. J. **93**, 311–335 (2017)
15. Cao, J., Ma, M., Li, H.: An uniform handover authentication between E-UTRAN and non-3GPP access networks. IEEE Trans. Wirel. Commun. **11**, 3644–3650 (2012)
16. Li, G., Jiang, Q., Wei, F., Ma, C.: A new privacy-aware handover authentication scheme for wireless networks. Wirel. Pers. Commun. **80**, 581–589 (2015)
17. Wang, Y.Y., Liu, J.Y., Xiao, F.X., Dan, J.: A more efficient and secure dynamic ID-based remote user authentication scheme. Comput. Commun. **32**, 583–585 (2009)
18. Juang, W.S., Chen, S.T., Liaw, H.T.: Robust and efficient password-authenticated key agreement using smart cards. IEEE Trans. Ind. Electron. **55**, 2551–2556 (2008)
19. Wen, F., Li, X.: An improved dynamic ID-based remote user authentication with key agreement scheme. Comput. Electr. Eng. **38**, 381–387 (2012)
20. Tsai, J.L., Lo, N.W., Wu, T.C.: Novel anonymous authentication scheme using smart cards. IEEE Trans. Indus. Inform. **9**, 2004–2013 (2013)
21. Kim, K.-k., Kim, M.-H.: Retracted: an enhanced anonymous authentication and key exchange scheme using smartcard. In: Kwon, T., Lee, M.-K., Kwon, D. (eds.) ICISC 2012. LNCS, vol. 7839, pp. 487–494. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-37682-5_34
22. Khan, M.K., Kim, S.K., Alghathbar, K.: Cryptanalysis and security enhancement of a 'more efficient & secure dynamic ID-based remote user authentication scheme'. Comput. Commun. **34**, 305–309 (2011)
23. Ma, C.G., Wang, D., Zhao, S.D.: Security flaws in two improved remote user authentication schemes using smart cards. Int. J. Commun. Syst. **27**, 2215–2227 (2015)
24. Huang, X., Chen, X., Li, J., Xiang, Y., Xu, L.: Further observations on smart-card-based password-authenticated key agreement in distributed systems. IEEE Trans. Parallel Distrib. Syst. **25**, 1767–1775 (2014)
25. Wang, D., Wang, N., Wang, P., Qing, S.: Preserving privacy for free: efficient and provably secure two-factor authentication scheme with user anonymity. Inf. Sci. **321**, 162–178 (2015)

26. Ding, W., Ping, W.: Two birds with one stone: two-factor authentication with security beyond conventional bound. IEEE Trans. Dependable Secure Comput. **PP**, 1 (2016)
27. http://prosecco.gforge.inria.fr/personal/bblanche/proverif/
28. Yang, X., Huang, X., Liu, J.K.: Efficient handover authentication with user anonymity and untraceability for mobile cloud computing. Future Gen. Comput. Syst. **62**, 190–195 (2016)
29. https://crypto.stanford.edu/pbc/