Accepted Manuscript

Efficient handover authentication with user anonymity and untraceability for Mobile Cloud Computing

Xu Yang, Xinyi Huang, Joseph K. Liu

PII: S0167-739X(15)00308-8
DOI: http://dx.doi.org/10.1016/j.future.2015.09.028
Reference: FUTURE 2858

To appear in: *Future Generation Computer Systems*

Received date: 1 May 2015
Revised date: 12 September 2015
Accepted date: 16 September 2015

Please cite this article as: X. Yang, X. Huang, J.K. Liu, Efficient handover authentication with user anonymity and untraceability for Mobile Cloud Computing, *Future Generation Computer Systems* (2015), http://dx.doi.org/10.1016/j.future.2015.09.028

Efficient Handover Authentication with User Anonymity and Untraceability for Mobile Cloud Computing

Xu Yang[a,b], Xinyi Huang[a,b,*], Joseph K. Liu[c]

[a] *Fujian Provincial Key Laboratory of Network Security and Cryptology, School of Mathematics and Computer Science, Fujian Normal University, Fuzhou, China*
[b] *The State Key Laboratory of Integrated Services Networks, Xidian University, China*
[c] *Faculty of Information Technology, Monash University, Australia*

Abstract

Various wireless communication technologies have been generated and deployed on account of mass requirements. These enable cloud computing with integration with mobility and Mobile Cloud Computing (MCC) becomes the trend of future generation computing paradigm. In this paper, we address a challenging issue of MCC technology - security and privacy of the handover process. We propose a new design of handoff authentication for heterogeneous mobile cloud networks, which provides user anonymity and untraceability. Compared with previous protocols, our proposed mechanism achieves comprehensive features of universality, robust security and efficiency.

Keywords: mobile cloud computing, handover authentication, security, efficiency, user anonymity, untraceability

1. Introduction

With the rapid growing of different wireless technologies, such as LTE, CDMA, WiMAX, and WiFi, cloud computing is no longer limited to wire-connected computing devices. Smart phone or tablet becomes the most frequently used computing device. With the distributed computing structure of cloud, using mobile devices to access the cloud will be the next generation computing paradigm. This is also known as Mobile Cloud Computing (MCC). Within the paradigm of MCC, user devices will require roam across

*Corresponding author. Email: xyhuang81@gmail.com

heterogeneous access technologies in order to enjoy a seamless connectivity. However, since security policies vary greatly among different networks, security contexts need to be resolved anew upon a vertical handover, which results in efficiency slow-down and induces security risks. Supporting seamless roaming and secure handover in MCC is a challenging task since each access network may have different mobility, Quality-of-Service (QoS) and security requirements. Moreover, real-time cloud applications such as video conferenceing and media streaming [1] have stringent performance requirements on end-to-end delay and packet loss. In order to overcome these performance bounds and provide continuous secure services for mobile clients, it is necessary to design an efficient handover protocol.

Authentication is an important module in the handover protocol. As shown in Figure 1 (assumed that there is an integrated WiMAX and WiFi networks), regardless of the technology implemented in MCC, a typical heterogeneous handover authentication scenario could come down to involving four entities: mobile clients (MCs), access points (APs) or base stations (BSs), gateway routers (GWs) and the authentication server (AS) which is located at the cloud service provider. Before entering the network, a MC must register to AS. After granted the permission from AS, MC connects to an AP (or a BS) for accessing the network through GW. A MC moves from one AP (or BS) to a new AP (or BS) within the domain of a single wireless access network, which refers to horizontal handover. Conversely, a MC handovers among heterogeneous wireless access networks, which refers to vertical handover. After MC roams to a new AP (or BS), handover authentication should be performed at the new AP (or BS). The AP (or BS) will authenticate the legitimate MC and reject any access request by illegitimate users. At the same time, they will establish a session key between this authenticated MC and AP (or BS) for the purpose of providing confidentiality and integrity of the communication session.

In this paper, we further illustrate the above procedure by considering an integrated WiMAX and WiFi heterogeneous networks, where a WiMAX network is interconnecting with WiFi network through a WiFi interworking Function (WIF) [2] which is predefined by the WiMAX forum for roaming support. The WIF plays an important role in interfacing WiMAX and WiFi networks, which enables the MC with WiFi network connectivity to access WiMAX network functionality [3]. In Figure 1, entities enforcing access control are authenticators that refer to an Access Service Network-Gateway (ASN-GW) or AP. An ASN-GW controls multiple BSs and takes charge of

forwarding authentication messages between the MC and the AS residing in the Cloud Service Provider (CSP). Considering the security, we assume that secure transmission protocols have been used in all the entities containing AS, ASN-GW, BS, WIF and AP to maintain mutual trusted relations and establish connections.

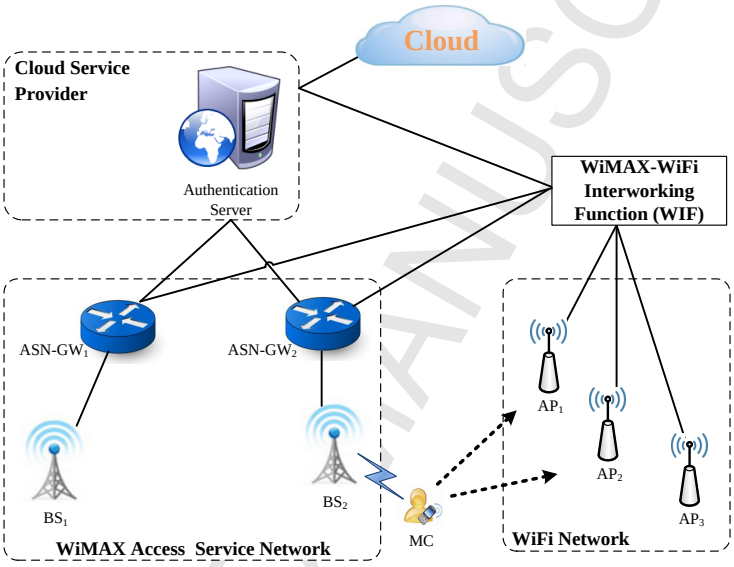

Figure 1: Architecture of a MCC paradigm with an integrated access network for WiMAX and WiFi

There are two major practical issues on designing a handover authentication protocol in MCC:

- First, **security and privacy** are two major concerns for the handover authentication process. For privacy, mobile clients may prefer to keep their identities and location hidden. It is a notable issue in wireless networks since roaming protocols may expose users' identities and locations at the user authentication phase. Identity privacy is relevant to the MC when it sends authentication request (which includes its identity). A robust and privacy-preserving scheme is therefore essential to resist any adversary from getting the identity of the authenticated user. On the other side, location privacy is relevant to the AP or BS when MC has accessed with it, since any attacker can trace MC's movement route. Therefore, user anonymity and untraceability should be paid more attention to in the handover protocol.

- Second, **efficiency** also needs to be intensively considered for handover authentication service. This is of great importance for guaranteeing service continuity and QoS, which means low latency and low packet loss when a MC is handovering to another network [4]. Since either MCs or APs are generally constrained by power and processing capability, an efficient handover authentication protocol should be essential. Furthermore, such a protocol must be able to maintain persistent connectivity between MCs and APs.

1.1. Related Works

There are several authentication protocols have been proposed in some literature for the purpose of achieving a secure and efficient handover authentication in a heterogeneous network [3, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19]. However, most of these existing authentication protocols ultimately turn out to have a few drawbacks, which we divide into following aspects:

- Interact with AS during mutual authentication or need the participation of third parties, such as home AP/BS;
- Cannot provide a privacy protection mechanisms even they may have serious security flaws;
- Incur high authentication costs and low efficiency, which cannot achieve the requirement of seamless handover; and
- Complex design of schemes results in suffering weakness on universality.

Kwon et al. [5] presents a USIM based authentication test-bed implemented for the UMTS-WLAN handover. The performance of full authentication and fast re-authentication in terms of procession time are analyzed and compared. However, there is no detailed description about fast authentication and handover authentication. The performance about fast re-authentication does not meet the requirement of delay-sensitive application. In [6], the authors presented a pre-authentication based scheme for WiFi and WiMAX integrated network. It generates MSKs (master session keys) when a user initially logs in network, and transmits the MSK to the target network where necessary. By executing pre-authentication scheme, the handover process is simplified to become localized authentication and require merely message

flows between the MC and target BSs/APs without involving the AS. In [7], Sun et al. also presented a pre-authentication based secure and efficient handover schemes for WiFi and WiMAX heterogeneous networks. The adoption of key reuse in this scheme decreases the processing time of key re-generation during handover process and even avoids the frequent handovers between two BSs [8]. Nevertheless, the performance analysis shows that both schemes might still undergo lengthy authentication when MSK misses or the MC moves to a target BS/AP that does not receive the key, which results in serious authentication latency. In [9], the authors proposed a one-pass AKA Authentication in 3G-WLAN integrated networks, which reduces the authentication costs by using an International Mobile Subscriber Identity-IP Multimedia Private Identity pair. Unfortunately, security analysis shows that the users are vulnerable to potential spoofing attacks by rogue third party application vendors [20].

Five fast and secure re-authentication protocols for 3GPP subscribers to perform handovers between the WiMAX and the WLAN systems have been proposed in [11], which takes advantage of key reuse and avoids contacting AS in the 3GPP networks during the handovers. Here 'key reuse' means that a key stored in a previously visited network is reused for re-authentication while the user re-visits the network, thus it speeds up the key re-generation process and reduces the authentication cost. Although this scheme can achieve an outstanding performance in terms of the key reuse trait and the re-authentication delay compared with the current 3GPP standard protocols [2] and can provide several security features including forward and backward secrecy, it can only support single-hop communications between a MC and AP/BS and the re-authentication processing time unable to satisfy the requirement of real-time applications. The scheme by [3] presents a fast authentication for WiMAX-WLAN integrated network with the assumption that the AS has robust security features. The authors use the AS to ensure the handover security. By adopting the localized authentication concept and utilizing the approach of pre-authentication, it can avoid suffering a longer delay. However, since the AS is normally located far away from the BS/AP, it may incur accident to degrade the system performance such as a connection loss between the BS/AP and the AS.

Recently, a fast and secure handover authentication scheme based on ticket for WiMAX and WiFi heterogeneous networks has been proposed in [14]. The MC and the target BS/AP can complete the mutual authentication and derive their session key by a credential ticket generated by the previously

visited BS/AP without interacting with AS. By executing such local authentication which significantly reduces the handover authentication delay. Nevertheless, it does not provide a privacy protection and has weakness on universality.

Regarding privacy, unfortunately all the above schemes have provided no privacy protection measures and no universality for various networks. In [15], a universal authentication protocol with strong user anonymity for wireless communication networks was proposed by Yang et al. It is based on group signature and only require three message flaws between the roaming MC and the foreign BS/AP during handover. Though this protocol can assure user anonymity and provide a practical user revocation mechanism, it still fails to provide user untraceability [21] and the protocol may become time-wasting and power-consuming when the number of revoked users is large. Cao et al. [16] proposed an unified ID-based cryptography handover authentication scheme without pairing operation for heterogeneous access networks. The handover authentication is executed between a MC and the target AP without the third party. Although the authors claim that their scheme achieves user anonymity, the identity of the MC may still be exposed to attackers, since the real identity is passed in plaintext when the MC requests handover authentication to the target AP. Therefore, the scheme cannot achieve real user anonymity and untraceability. Very recently, Liu et al. [19] proposed a time-bound anonymous authentication protocol for roaming network. Similar to [15], it is based on group signature with time information embedded into the signature. By doing so, revoked users can be classified into natural revoked (expired user) and obliged revoked. Yet user untraceability is not yet feasible.

1.2. Our Contributions

Taking into account the above analysis, users are unwilling to accept such service which always fails to provide appropriate security and efficiency guarantees. Thus, providing a practical handover authentication with efficiency and user privacy scheme becomes a notable issue in the MCC context. In this paper, taking the advantage of an identity-based elliptic curve algorithm in [22], we propose a new universal efficient handover authentication with user anonymity and untraceability for MCC. Our proposed scheme can be distinguished from previous works and the merits can be summarized in several aspects:

1. **No extra third party.** Except both the MC and the BS/AP, there is no additional participation of any third party during the handover authentication, such as AS or home AP/BS.
2. **Simple in design.** We need only one handover authentication protocol to handle various heterogeneous network scenarios.
3. **Universality.** The protocol is universal in the sense that the same protocol can be used appropriately for different heterogeneous network.
4. **User anonymity and untraceability.** In order to satisfy the requirement of modern society, our protocol supports user anonymity and untraceability.
5. **Robust security and efficiency.** On the basis of a robust security, our protocol enjoys high efficiency in authentication performance compared with existing schemes.

The remaining part of this paper is organized as follows. Section 2 discusses the security requirements and introduces the elliptic curve group. Section 3 presents our scheme and Section 4 analyzes the security and performance of our scheme. We conclude the paper in Section 5.

2. Security Requirements and Preliminaries

2.1. Security Requirements

A secure and user anonymous handover authentication scheme in MCC should satisfy the following requirements:

1. **Mutual authentication:** Both of the roaming MC and the target AP are all authorized by the AS.
2. **Access grant:** MCs should be allowed by AS to authenticate the AP which they visit in order to avoid potential deception and other malicious attacks.
3. **Key establishment:** The MC, the target AP and the AS all share a common secret.
4. **Data integrity:** Data transmitted in the network cannot be tampered, replayed and delayed maliciously. Eavesdropping is also infeasible to get the communicated plaintext.
5. **User anonymity:** Except the AS, the MC is anonymous to anyone including the visited AP.

6. **User untraceability:** Except the AS, no one is able to know the MC's activities.
7. **Forward and backward secrecy:** An adversary cannot use a compromised session key to acquire previous keys that have ever been used or calculate any future ones. The protected sessions are invisible to the adversary.
8. **Attack resistance:** The security of the scheme will not be compromised under various types of attacks (e.g., eavesdropping, replay, spoofing, etc.).

All these requirements are considered in the design of our scheme.

2.2. Elliptic Curve Group

In this section, we briefly introduce the elliptic curve group and the corresponding mathematical hard problems over it.

Let F_q be a prime finite field, E/F_q an elliptic curve defined over F_q, and P an element of a large prime order q in E/F_q. The point on E/F_q together with an extra point Θ called the point at infinity form a group $G = \{(x, y) : x, y \in F_q; (x, y) \in E/F_q\} \cup \{\Theta\}$. G is a cyclic additive group of composite order q. Scalar multiplication over E/F_q can be computed as follows: $tP = P + P + \ldots + P_{\ t\ times}$.

There exist the following problems over the elliptic curve group.

Computational Diffie-Hellman (CDH) Problem: Given aP and bP, where $a, b \in {}_R\mathbb{Z}_q^*$ and P the generator of G, compute the value abP.

Decisional Diffie-Hellman (DDH) Problem: Given aP, bP and cP, where $a, b, c \in {}_R\mathbb{Z}_q^*$ and P the generator of G, confirm whether or not $cP = abP$, that is equal to confirm whether or not $c = ab \bmod q$.

3. Proposed Scheme

In this section, we shall describe the details of our proposed vertical handover authentication scheme. It consists of two phases, namely key predistribution phase and handover authentication phase as shown in Figure 2. Before the description, we will begin with the pre-deployment. The notations used in the scheme are also defined in Table 1.

3.1. Pre-deployment phase

The purpose of this phase is to initialize the system and make a preparation for the future handover and authentication.

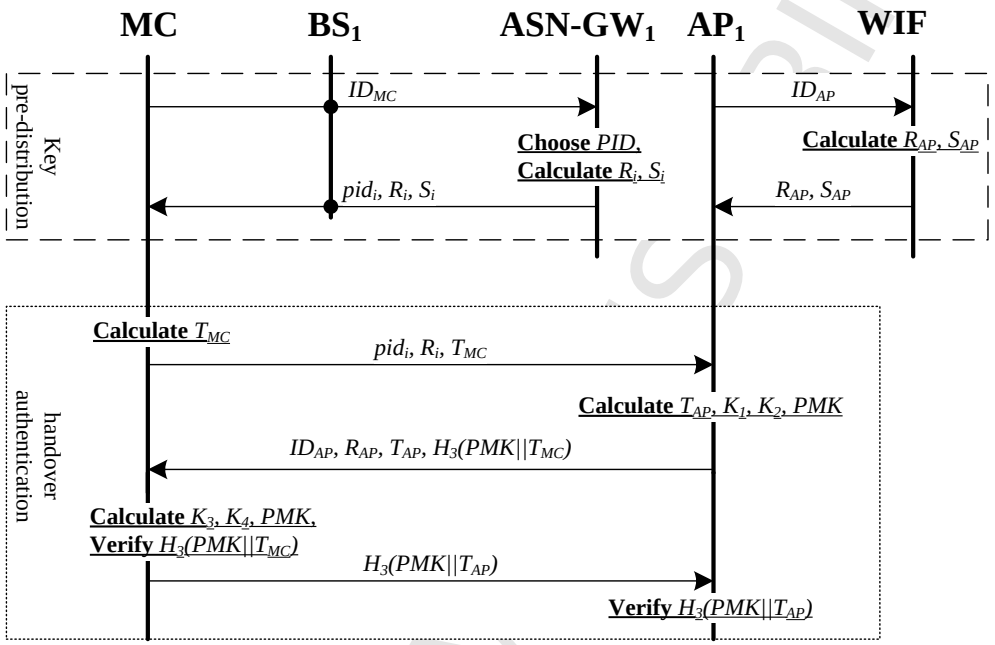

Figure 2: WiMAX to WiFi handover authentication

Table 1: Notations in the scheme

Notation	Description
q	a k-bit prime
F_q	a prime finite field
E/F_q	an elliptic curve E over F_q
G	$G = \{(x, y) : x, y \in E/F_q\} \cup \{\Theta\}$
P	generator for the group G
T_{exp}	expiration time
ID_x	identity of entity x
$H_0()$	a secure hash function $H_0 : G \rightarrow \mathbb{Z}_q^*$
$H_1()$	a secure hash function $H_1 : \{0,1\}^* \times G \rightarrow \mathbb{Z}_q^*$
$H_2()$	a secure hash function $H_2 : \{0,1\}^* \times \{0,1\}^* \times G \times G \rightarrow \{0,1\}^k$
$H_3()$	a secure hash function $H_3 : \{0,1\}^k \times G \rightarrow \{0,1\}^k$
PK_x	public key of entity x
(R_x, S_x)	entity x's private long-term key

System Initialization: We assume the AS will perform the process of system initialization prior to the WiMAX-WiFi interworking networks deployment. The process works as follows.

(1) Choose four secure hash functions H_0, H_1, H_2 and H_3 (the definition of each hash function is given in Table 1).
(2) Choose a k-bit prime q and determine the tuple $\{F_q, E/F_q, G, P\}$.
(3) Choose two random numbers $r_1, r_2 \in \{0,1\}^* \rightarrow \mathbb{Z}_q^*$, compute the public key r_1P, r_2P, and distribute the security context (r_1, r_2P) and (r_2, r_1P) to ASN-GW and WIF, respectively. Besides, compute the secret key $s = H_0(r_1r_2P)$, and distribute sP as the system parameter.
(4) Publish $\{F_q, E/F_q, G, P, r_1P, r_2P, sP, H_0, H_1, H_2, H_3\}$ as system parameters and keep the key $\{r_1, r_2\}$ secret.

3.2. Vertical handover authentication phase

A MC will execute a vertical handover when the MC wants to change its access network provided by different heterogeneous networks (Here we assume that the heterogeneous network is the WiMAX and WiFi interworking networks). Meanwhile, a key pre-distribution process is initialized by the MC at this moment. As shown in Figure 2, before the vertical handover from WiMAX to WiFi (the same to WiFi to WiMAX), there is a key pre-distribution phase. The detailed descriptions of the handover authentication are as follows.

• **key pre-distribution phase:** In this phase, as shown in Figure 2, each AP next to the current BS sends its identifier ID_{AP} to WIF at first before handover authentication. Then WIF chooses a random number $r' \in \mathbb{Z}_q^*$ and computes $s = H_0(r_2r_1P)$, $R_{AP} = r'P$, $h_{AP} = H_1(ID_{AP}\|R_{AP})$, $S_{AP} = r' + h_{AP}s$. Finally WIF sends long-term secret key tuple (R_{AP}, S_{AP}) to the AP using a secure transmission protocol (e.g., wired transport layer security protocol). Similarly, when a MC sends the request message to $ASN\text{-}GW_1$ with its real identity ID_{MC} through BS_1, $ASN\text{-}GW_1$ shall first check the validity. If MC is valid, $ASN\text{-}GW_1$ chooses a family of unlikable pseudo-IDs $PID = pid_1, pid_2, \ldots$. For each pseudo-ID $pid_i \in PID$, $ASN\text{-}GW_1$ chooses a random number $r_i' \in \mathbb{Z}_q^*$ and computes $s = H_0(r_1r_2P)$, $R_i = r_i'P$, $h_i = H_1(pid_i\|R_i)$, $S_i = r_i' + h_is$, and finally securely sends all long-term secret key tuples (pid_i, R_i, S_i) back to MC. By this, MC can constantly change its pseudo-ID to achieve identity privacy and location privacy in handover authentication phase.

Upon receiving the private key S_{AP} or S_i, the AP or MC can validate the key by checking: $S_{AP}P = R_{AP} + H_1(ID_{AP}\|R_{AP})sP$ or $S_iP = R_i + H_1(pid_i\|R_i)sP$.

• **handover authentication phase:** Mutual authentication between the MC and the new AP/BS shall be accomplished in this phase. The Pairwise Master Key (PMK) shared between them can be generated directly upon handover authentication. Here are the messages to be exchanged in our handover authentication protocol.

(1) $\underline{MC \rightarrow AP_1\text{: } pid_i, R_i, T_{MC}}$
After the completion of the previous key pre-distribution, the MC is ready for handoff authentication. Once MC roams to the range of WiFi, it picks an unused pseudo-ID pid_i and the corresponding long term key R_i, S_i. Besides, MC chooses a random value $a \in \mathbb{Z}_q^*$, which is a nonce, computes $T_{MC} = a * P$. Finally, it sends pid_i, R_i and T_{MC} to the new AP AP_1.

(2) $\underline{AP_1 \rightarrow MC\text{: } ID_{AP}, R_{AP}, T_{AP}, H_3(PMK||T_{MC})}$
Upon receiving the message, AP_1 randomly chooses $b \in \mathbb{Z}_q^*$ and computes $T_{AP} = bP$. It then calculates MC's public key PK_{MC}, the shared secrets K_1 and K_2, and the session key PMK as shown below. After that, a confirmation value $H_3(PMK\|T_{MC})$ is generated by AP_1 and AP_1 then sends ID_{AP}, R_{AP}, T_{AP}, and $H_3(PMK\|T_{MC})$ to MC for an agreement.

$$PK_{MC} = R_i + H_1(pid_i\|R_i)sP$$

$$K_1 = S_{AP}T_{MC} + bPK_{MC},\ K_2 = bT_{MC}$$

$$PMK = H_2(pid_i\|ID_{AP}\|K_1\|K_2)$$

(3) $\underline{MC \rightarrow AP_1\text{: } H_3(PMK||T_{AP})}$
After receipt of the message from AP_1, the MC first computes AP_1's public key PK_{AP}, the shared secrets K_3 and K_4, and uses these two shared secrets to generate the session key PMK as shown below. Then MC verifies the correctness of $H_3(PMK\|T_{MC})$ and proceeds to the next step if the verification is successful. At this step, AP_1 is successfully authenticated by MC. Similarly, for the purpose of being authenticated by the AP, MC also sends $H_3(PMK\|T_{AP})$ to AP_1 for verification.

$$PK_{AP} = R_{AP} + H_1(ID_{AP}\|R_{AP})sP$$

$$K_3 = S_i T_{AP} + aPK_{AP},\ K_4 = aT_{AP}$$
$$PMK = H_2(pid_i \| ID_{AP} \| K_3 \| K_4)$$

Finally, AP_1 receives and checks $H_3(PMK||T_{MC})$. MC is successfully authenticated by AP_1 if the confirmation value $H_3(PMK\|T_{AP})$ is correct. This completes the mutual handoff authentication. And the PMK is the session key shared between MC and AP_1 for securing the subsequent communications.

4. Security Analysis and Performance Evaluation

4.1. Security Analysis

We analyze the security of our proposed scheme with respect to the security requirements given in Section 2.

Mutual authentication and key establishment: Due to the existence of trust agreements between AS, ASN-GW, BS, WIF and AP in the WiMAX and WiFi heterogeneous networks, we only discuss the mutual authentication between MC and AP in the proposed scheme. Mutual authentication between the MC and AP_1 is accomplished based on identities and CDH problem. The MC and AP_1 check the hash values from the other side whether they agree the shared secrets, which is shown as follows.

$$\begin{aligned}
K_1 &= S_{AP} T_{MC} + bPK_{MC} \\
&= S_{AP} aP + b(R_i + H_1(pid_i \| R_i) sP) \\
&= S_{AP} aP + S_i bP \\
&= S_i bP + a(S_{AP} P) \\
&= S_i T_{AP} + aPK_{AP} \\
&= K_3 \\
K_2 &= bT_{MC} = baP = aT_{AP} = K_4
\end{aligned}$$

Thus the shared session key PMK for the MC and AP_1 can be computed as follows.

$$\begin{aligned}
PMK &= H_2(pid_i \| ID_{AP} \| K_1 \| K_2) \\
&= H_2(pid_i \| ID_{AP} \| K_3 \| K_4)
\end{aligned}$$

Consequently, only the legitimate MC or AP_1 can generate the valid hash values to achieve the mutual authentication, and establish the agreed session key PMK.

Access grant: After a successful key pre-distribution, the ASN-GW and the WIF grant access for the future handoff of MC and AP by issuing them with long-term secret keys. A MC (or AP) can complete a handover authentication if and only if the long-term secret keys are correctly generated by the ASN-GW (or WIF). An adversary who does not have the knowledge of MC and AP's long-term secret keys cannot make legitimate authentication code request.

Data integrity: Based on the above key agreement, long-term secret keys are constructed to establish a mutual trust between MC and AP. Sessions can be protected by the long-term secret keys until mutual authentication completes. After the mutual authentication, MC and AP can negotiate a shared session key PMK. Consequently, under the aegis of the long-term secret key and session key PMK, data transmitted in the network cannot be maliciously utilized by the adversary.

User anonymity and untraceability: In our scheme, each MC receives a family of pseudo-IDs and the corresponding long-term secret keys from ASN-GW before the handover authentication takes place. These pseudo-IDs, instead of the MC's real identity, are used in handover authentication phase for the purpose of privacy preservation. Thus, only ASN-GW has the knowledge of the relationship between a pseudo-ID and the real identity. Besides, since there is no linkage between pseudo-IDs, anyone except the MC and ASN-GW, including APs is unable to identify the MC or link two sessions initiated by the same MC.

Forward and backward secrecy: Forward and backward secrecy means that even if a long-term secret key is compromised at any point in time, it will not affect the security of the preceding and subsequent session keys. In our scheme, we execute a Diffie-Hellman key exchange in an authenticated way. The temporal Diffie-Hellman parameters used to construct a session key are randomly chosen by the MC and the AP independently, and they are irrelevant to long-term secret keys. Therefore, with compromised long-term secret keys or session keys, an adversary cannot recover historical sessions or decrypt the latter ones, i.e., our proposed protocol can achieve forward and backward secrecy.

Attack resistance: Our scheme can resist various types of attacks. For eavesdropping, though the data transmitted in the newly established connections in the wireless environment can be captured by attackers, the attackers cannot acquire the content of packets because the content of packets are protected by encryption with PMK. On man-in-the-middle attacks, as the

key agreement in our scheme is based on CDH, both the MC and AP send the packets through checking the Diffie-Hellman public components and generate session keys via the long-term secret keys, which makes our protocol achieving mutual authentication and securing against the attacker to cheat by eavesdropping the messages in the middle to forge or replay the messages. Replay attack is also infeasible in our scheme because random values are added in each exchange message, and these messages are verified via the long-term secret keys by the MC and AP. Spoofing and impersonating an authorized MC or AP for receiving data information are prevented as well since only the legitimate users can derive valid long-term secret keys issued by the ASN-GW or WIF.

4.2. Performance Evaluation

In this section, we analyze the performance of our scheme from several aspects, including functionality and performance, by comparing it with other schemes which are the most relevant to ours [11, 3, 14, 16, 15]. As shown in Table 2, the comparison of functionality and performance contains the number of parties, universality, user anonymity, untraceability, communication overhead, and computation overhead.

Table 2: Performance comparison among different handover protocols.

Protocols	No. P	Univ.	Ano./Unt.	Commun.	Comput.
Shidhani [11]	5	No	No/No	$10\alpha + 4\beta + 4\gamma$	(10,6,8,14,0)
Huang [3]	3	No	No/No	$5\alpha + 2\beta$	(8,0,4,6,0)
Fu [14]	3	No	No/No	$4\alpha + 2\beta$	(8,2,4,8,0)
Cao [16]	2	Yes	No/No	3α	(0,8,2,1,2)
Yang [15]	2	Yes	Yes/No	3α	(0,0,6,3,2)
Our scheme	2	Yes	Yes/Yes	3α	(0,8,0,0,2)

No. P : Number of parties.
Univ. : Universality.
Ano./Unt. : User anonymity/Untraceability.
Commun. : Communication overhead.
Comput. : Computation overhead.

The communication overhead represents the handoff time in the authentication and key distribution procedure. Here we assume that the communication cost between the MC and BS/AP is α, the cost between the BS/AP and ASN-GW/WIF is β, and the cost between the BS/AP and AAA server

is γ, respectively. The computation overhead represents the processing delays of the cryptography operations at each entity. We only consider the cost of operations listed as $(T_M, T_H, T_S, T_D, T_E)$, where we denote the time for a MAC operation as T_M, the time for a hash operation as T_H, the time for a symmetric encryption /decryption operation or a signature operation as T_S, the time for a key derivation function as T_D, and the time for one elliptic curve scalar multiplication (ECSM) operation as T_E.

From Table 2, we can see that our scheme achieves all functionality and performance requirements and is more efficient than others. Particularly, we have an obvious advantage in computation overhead compared with the existing schemes, since our scheme only need two ECSM operations to complete a handover authentication without any encryption or decryption operation (it is note that the complexity of highly efficient operations such as hash evaluation is often omitted). Overall, our scheme achieves outstanding performance than other proposed schemes.

5. Conclusions

In this paper, we have proposed a novel protocol to achieve efficient handover authentication for Mobile Cloud Computing paradigm. This novel protocol provides such advantages which can be summarized as universality, robust security and efficiency. The security and performance analysis shows that the proposed scheme achieves user anonymity and untraceability with excellent performance. With these advantages, we believe the new proposal provides a sound solution to handoff in MCC.

Acknowledgement

This work is supported by National Natural Science Foundation of China (61472083, 61402110, U1405255), Fok Ying Tung Education Foundation (141065), Ph.D. Programs Foundation of Ministry of Education of China (20123503120001), Program for New Century Excellent Talents in Fujian University (JA14067), Distinguished Young Scholars Fund of Department of Education, Fujian Province, China (JA13062), ISN Research Fund (ISN15-03), and the Scientific Research Foundation for the Returned Overseas Chinese Scholars.

References

[1] J. K. Liu, M. H. Au, W. Susilo, K. Liang, R. Lu, B. Srinivasan, Secure sharing and searching for real-time video data in mobile cloud, IEEE Network 29 (2015) 46–50.

[2] W. F. N. W. Group, et al., Wimax forum network architecture–stage 3: Detailed protocols and procedures–release 1, version 1.2, in: WiMAX Forum, January.

[3] K.-L. Huang, K.-H. Chi, J.-T. Wang, C.-C. Tseng, A fast authentication scheme for wimax–wlan vertical handover, Wireless personal communications 71 (2013) 555–575.

[4] J. W. Floroiu, R. Ruppelt, D. Sisalem, J. Voglimacci, Seamless handover in terrestrial radio access networks: a case study, Communications Magazine, IEEE 41 (2003) 110–116.

[5] H. Kwon, K.-y. Cheon, K. Roh, A. Park, Usim based authentication test-bed for umts-wlan handover, in: Proceedings of IEEE Infocom.

[6] H. Liming, K. X. Miao, A pre-authentication architecture in wifi&wimax integrated system, in: Communications and Networking in China, 2009. ChinaCOM 2009. Fourth International Conference on, IEEE, pp. 1–5.

[7] H.-M. Sun, S.-M. Chen, Y.-H. Chen, H.-J. Chung, I.-H. Lin, Secure and efficient handover schemes for heterogeneous networks, in: Asia-Pacific Services Computing Conference, 2008. APSCC'08. IEEE, pp. 205–210.

[8] Y. Zhang, N. Ansari, H. Tsunoda, Wireless telemedicine services over integrated ieee 802.11/wlan and ieee 802.16/wimax networks, Wireless Communications, IEEE 17 (2010) 30–36.

[9] C. Ntantogian, C. Xenakis, One-pass eap-aka authentication in 3g-wlan integrated networks, Wireless personal communications 48 (2009) 569–584.

[10] J. Y. Kim, S. U. Shin, et al., Authentication mechanism for fast handoff in cdma2000-wibro interworking, Science in China Series F: Information Sciences 53 (2010) 137–146.

[11] A. A. Al Shidhani, V. C. Leung, Fast and secure reauthentications for 3gpp subscribers during wimax-wlan handovers, Dependable and Secure Computing, IEEE Transactions on 8 (2011) 699–713.

[12] Q. Han, Y. Zhang, X. Chen, H. Li, J. Quan, Efficient and robust identity-based handoff authentication in wireless networks, in: Proc. 6th Int. Conf. Network and System Security, Springer, 2012, pp. 180–191.

[13] Y. Zhang, X. Chen, H. Li, J. Cao, Identity-based construction for secure and efficient handoff authentication schemes in wireless networks, Security and Communication Networks 5 (2012) 1121–1130.

[14] A. Fu, G. Zhang, Z. Zhu, Y. Zhang, Fast and secure handover authentication scheme based on ticket for wimax and wifi heterogeneous networks, Wireless Personal Communications 79 (2014) 1277–1299.

[15] G. Yang, Q. Huang, D. S. Wong, X. Deng, Universal authentication protocols for anonymous wireless communications, Wireless Communications, IEEE Transactions on 9 (2010) 168–174.

[16] J. Cao, M. Ma, H. Li, An uniform handover authentication between e-utran and non-3gpp access networks, Wireless Communications, IEEE Transactions on 11 (2012) 3644–3650.

[17] Y. Zhai, X. Mao, Y. Wang, J. Yuan, Y. Ren, A dht-based fast handover management scheme for mobile identifier/locator separation networks, Science China Information Sciences 56 (2013) 1–15.

[18] Y. Cao, C. Xu, J. Guan, H. Zhang, Qos-driven sctp-based multimedia delivery over heterogeneous wireless networks, Science China Information Sciences 57 (2014) 1–10.

[19] J. K. Liu, C. Chu, S. S. M. Chow, X. Huang, M. H. Au, J. Zhou, Time-bound anonymous authentication for roaming networks, Information Forensics and Security, IEEE Transactions on 10 (2015) 178–189.

[20] M. J. Sharma, V. C. Leung, Improved ip multimedia subsystem authentication mechanism for 3g-wlan networks, International Journal of Security and Networks 6 (2011) 90–100.

[21] D. He, J. Bu, S. Chan, C. Chen, M. Yin, Privacy-preserving universal authentication protocol for wireless communications, Wireless Communications, IEEE Transactions on 10 (2011) 431–436.

[22] X. Cao, W. Kou, X. Du, A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges, Information Sciences 180 (2010) 2895–2903.

*Biographies (Text)

Xu Yang received his B.S. degree from the Department of electrical and information engineering, Hubei University of Automotive Technology, China, in 2013. He is currently a Graduate at the Fujian Provincial Key Laboratory of Network Security and Cryptology, School of Mathematics and Computer Science, Fujian Normal University, China. His research interests include cryptography and information security.

Xinyi Huang received his Ph.D. degree from the School of Computer Science and Software Engineering, University of Wollongong, Australia, in 2009. He is currently a Professor at the Fujian Provincial Key Laboratory of Network Security and Cryptology, School of Mathematics and Computer Science, Fujian Normal University, China. His research interests include cryptography and information security. He has published over 90 research papers in refereed international conferences and journals, such as PKC, IEEE Transactions on Computers, IEEE Transactions on Parallel and Distributed Systems, IEEE Transactions on Information Security and Forensics, and IEEE Journal on Selected Areas in Communications. His work has been cited more than 1600 times at Google Scholar (H-Index: 23). He is in the Editorial Board of IEEE Transactions on Dependable and Secure Computing and International Journal of Information Security. He has served as the program/general chair or program committee member in over 60 international conferences.

Joseph K. Liu received the Ph.D. degree in information engineering from the Chinese University of Hong Kong in July 2004, specializing in cyber security, protocols for securing wireless networks, privacy, authentication, and provable security. He is now a senior lecturer at Monash University, Australia, and an adjunct associate professor at Shenzhen University, China. Prior to that he was a research scientist in the Infocomm Security Department at the Institute for Infocomm Research, Singapore from 2007-2015. His current technical focus is particularly cyber security in the cloud computing paradigm, smart city, lightweight security, and privacy enhanced technology. He has published more than 80 refereed journal and conference papers and received the Best Paper Award from ESORICS 2014. He has served as the program chair of ProvSec 2007, 2014, Pairing 2015, and on the program committees of more than 35 international conferences.

*Biographies (Photograph)

Xu Yang

Xinyi Huang

Joseph K. Liu

HIGHLIGHTS

- We address a challenging issue of Mobile Cloud Computing technology.
- We propose a new handoff authentication scheme with security and privacy.
- Our proposed mechanism achieves universality, robust security and efficiency.
- Security and performance analysis shows the excellent performance of our scheme.