symmetry

MDPI

Article

A Secure Mobility Network Authentication Scheme Ensuring User Anonymity

Ya-Fen Chang [1], Wei-Liang Tai [2,*] and Min-How Hsu [1]

[1] Department of Computer Science and Information Engineering, National Taichung University of Science and Technology, Taichung 40401, Taiwan; cyf@cs.ccu.edu.tw (Y.-F.C.); rickyhsu1942@gmail.com (M.-H.H.)
[2] Department of Information Communications, Chinese Culture University, Shilin, Taipei 11114, Taiwan
* Correspondence: tai.wei.liang@gmail.com; Tel.: +886-2-28610511 (ext. 37433)

Received: 26 October 2017; Accepted: 4 December 2017; Published: 8 December 2017

Abstract: With the rapid growth of network technologies, users are used to accessing various services with their mobile devices. To ensure security and privacy in mobility networks, proper mechanisms to authenticate the mobile user are essential. In this paper, a mobility network authentication scheme based on elliptic curve cryptography is proposed. In the proposed scheme, a mobile user can be authenticated without revealing who he is for user anonymity, and a session key is also negotiated to protect the following communications. The proposed mobility network authentication scheme is analyzed to show that it can ensure security, user anonymity, and convenience. Moreover, Burrows-Abadi-Needham logic (BAN logic) is used to deduce the completeness of the proposed authentication scheme.

Keywords: authentication; mobility networks; elliptic curve cryptography; man-in-the-middle attack; synchronization problem; BAN logic

1. Introduction

With the rapid growth of network technologies, users are used to accessing various services with their mobile devices. As a result, mobile devices and mobility networks play an important role in people's daily lives. There are three entities in mobility networks; mobile user, home agent and foreign agent. Before being able to access mobile services, a mobile user needs to register with the home agent. After successful registration, the mobile user with a mobile device can access mobile services. These mobile services are provided by the home agent directly or a foreign agent. If the requested mobile service is provided by a foreign agent, the registered mobile user needs the home agent's help to have himself/herself authenticated by the foreign agent. An illustration of mobility networks is shown in Figure 1, where a mobile user with a mobile device can be regarded as a mobile node. Plenty of mobility network applications are proposed and utilized because they provide great convenience.

Although mobility networks bring people great convenience and advantages, security threats exist. First, the transmission medium is a public but insecure channel such that an attacker can easily eavesdrop or intercept the transmitted data. Second, when a mobile user enters a service domain dominated by a new foreign agent, the mobile user has to access services via the new foreign agent. In this condition, two issues raise: (1) how the mobile user determines whether the foreign agent is legal; and (2) how the foreign agent determines whether the mobile user is legal. That is, the mobile user and the foreign agent have to authenticate each other. Unfortunately, in the beginning, no secret is shared between them. Third, because the mobile user is a visitor, the foreign agent serves the mobile user when he continuously stays. The mobile user may continuously stay, but the mobile user may not request mobile services continuously. This denotes that the mobile user and the foreign agent do not always communicate with each other. In such a condition, it is a challenge for the mobile user and the foreign agent to ensure each other's legality after they have already authenticated each other. Forth,

a mobile user may roam. Because the transmission medium is public, anyone can eavesdrop. If an attacker wants to trace a mobile user, he can eavesdrop and use the intercepted messages to obtain required information.

To ensure security of mobility networks, many authentication protocols are proposed [1–10]. In 2004, Zhu and Ma proposed an authentication scheme with anonymity for wireless environments based on the hash function and smart cards [5]. Later, Lee et al. [6] analyzed Zhu and Ma's scheme and found that Zhu and Ma's scheme does not provide mutual authentication and cannot resist forgery attack. In 2006, Lee et al. [7] proposed an enhancement to improve Zhu and Ma's authentication scheme for wireless networks. In 2009, Chang et al. [8] analyzed Lee et al.'s scheme [7] and pointed out that Lee et al.'s scheme still suffers from forgery attack and also proposed an improvement.

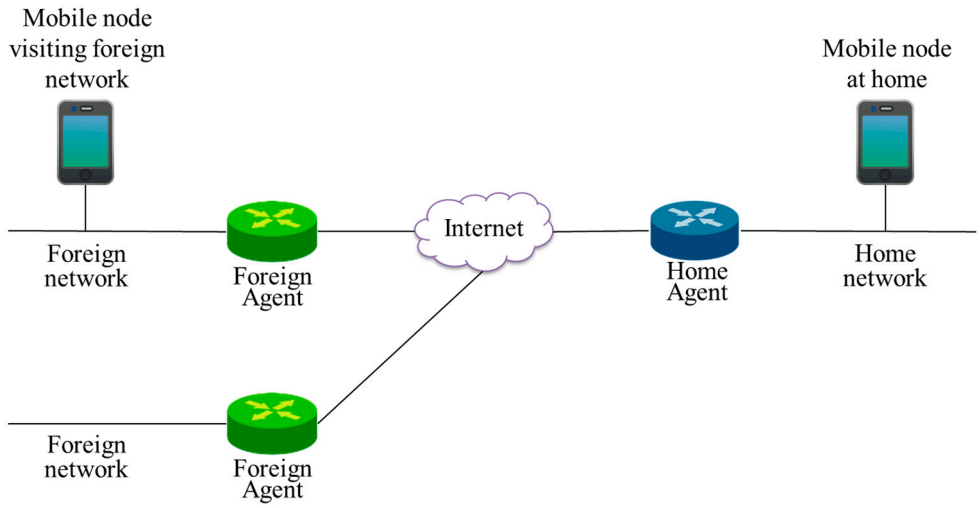

Figure 1. An illustration of mobility networks.

In 2014, Kuo et al. [9] showed that Chang et al.'s scheme cannot ensure anonymity for mobile users and proposed an improvement. Kuo et al. claimed that their scheme could ensure efficiency and security in mobility networks and provide anonymity for mobile users. In 2015, Lu et al. [10] showed that Kuo et al.'s scheme suffers from three drawbacks, vulnerability to insider attack, unfriendly password changes, and no local validation. They also proposed an authentication scheme to remedy these drawbacks. Later, Chang et al. [11] found that Kuo et al.'s scheme [9] is vulnerable to the other two weaknesses in 2016. First, Kuo et al.'s scheme cannot resist man-in-the-middle attacks when a mobile user and a foreign agent negotiate the session key. Via this security flaw, an attacker can impersonate a mobile user and negotiate the session key with the foreign agent. Second, Kuo et al.'s scheme cannot resist the synchronization problem. An attacker only needs to modify the transmitted data in password change phase such that a legal mobile user is unable to be authenticated by the home agent anymore. Lu et al. [10] claimed that their scheme could defend against replay attack and provide mobile user anonymity.

After thoroughly analyzing Lu et al.'s scheme, Chang et al. found that it possesses three drawbacks [12]. First, Lu et al.'s scheme is vulnerable to replay attack in authentication with key agreement phase. An attacker only needs to eavesdrop and resend the intercepted message with a new timestamp to cheat the foreign agent and the home agent. Second, user anonymity is not ensured as claimed because some transmitted parameters are fixed. Third, a random number chosen by the mobile user in registration phase is not stored in his/her smart card. As a result, the mobile user's smart card cannot compute one essential parameter to have himself/herself authenticated by the home agent in authentication with key agreement phase.

In addition to mobility networks, privacy is also an important topic in different types of networks. To ensure privacy and security in different types of networks, related security mechanisms are

proposed [13–18]. After analyzing the previous authentication schemes, the weaknesses that they suffer from and the security mechanisms of other networks, we propose a mobility network authentication scheme by considering the following four properties to ensure security and convenience.

Property 1: user anonymity

User anonymity needs to be ensured to prevent an unauthorized party from tracing a specific user. It denotes that only the authorized parties can know who the user is.

Property 2: resistance to common attacks

The proposed authentication scheme should be able to resist common attacks to ensure security.

Property 3: local password change

A mobile user should be able to change his/her password locally and at will without accessing the home agent to make the authentication scheme more convenient and user-friendly.

Property 4: mutual authentication between any two of a mobile user, a foreign agent and the home agent

In a mobility network authentication scheme, any two of a mobile user, a foreign agent and the home agent have to authenticate each other mutually to make sure that the other communication parties are legal.

The rest of this paper is organized as follows. The proposed scheme is shown in Section 2. The corresponding analysis is given in Section 3. Further discussions including comparisons and authentication proof using Burrows-Abadi-Needham logic (BAN logic) [19] are made in Section 4. Finally, some conclusions are given in Section 5.

2. The Proposed Secure Mobility Network Authentication Scheme Ensuring User Anonymity

In this section, we propose a user anonymity-ensured mobility network authentication scheme for mobility networks based on elliptic curve cryptography. Our scheme is composed of five phases: registration phase, login phase, authentication and establishment of the session key phase, update session key phase, and password change phase. A mobile user has to register with the home agent before accessing mobile services. In the registration phase, a mobile user registers with the home agent, the home agent stores parameters in a smart card, and the home agent issues it to the user. The mobile user and the home agent communicate via a secure channel. And the home agent stores parameters in a smart card securely because the smart card only can be accessed and modified by privilege users or administrators. In the login phase, a mobile user inserts his smart card into his terminal device. This denotes that the mobile user and the smart card can exchange required data via the terminal device. The terminal device possesses computational capacities and has a user interface to show the authentication progress or the response. The terminal device will execute computational operations on behalf of the mobile user. The terminal device should be personal or protected with proper security mechanisms such as firewalls. For simplicity, the communications between the mobile user and the smart card will be omitted, and the operations executed by either the user or the terminal device will be denoted by the user. In both the authentication and establishment of the session key phase and the update session key phase, data is transmitted via public channels. Notations used in our mobility network authentication scheme are listed in Table 1. The details are as follows.

Table 1. Notations used in our mobility network authentication scheme.

Symbol	Definition
MU	A mobile user
FA	A foreign agent
HA	The home agent
ID_A	The identifier of an entity A
$h(\cdot)$	A collision free one-way hash function
p_{MU}	The password chosen by MU
PW_{MU}	The secret of MU that is computed by ID_{MU} and p_{MU}
R_A	A random nonce chosen by an entity A
p	A prime greater than 2^{160}
n	A prime greater 2^{160}
P	A point on the elliptic curve $E_p(a, b)$ of order n, where $a, b \in Z_p$, $E_p(a, b)$: $y^2 = x^3 + ax + b$ and $4a^3 + 27b^2 \neq 0$
$P.x$	The x coordinate of the point P
$p_{HA\text{-}MU}$	The secret key of HA for MU
$p_{FA\text{-}HA}$	The secret key shared between HA and FA
$\|\|$	Concatenation operator
$\oplus$	Exclusive-or operator

2.1. Registration Phase

In this phase, if MU wants to access the roaming service, he/she must register with HA at first. Registration phase is depicted in Figure 2, and the details are as follows:

Step 1: MU selects his/her password p_{MU} and identifier ID_{MU}.
Step 2: MU sends ID_{MU} and p_{MU} to HA via a secure channel.
Step 3: After HA receives $\{ID_{MU}, p_{MU}\}$ from MU, HA checks if ID_{MU} does not exist. If it does hold, HA generates a random nonce R_{MU} and the secret key $p_{HA\text{-}MU}$ for MU.
Step 4: HA computes $PW_{MU} = h(ID_{MU} \,||\, p_{MU})$, $U = h(p_{HA\text{-}MU} \,||\, R_{MU})$, $W = PW_{MU} \oplus R_{MU}$, $V = R_{MU} \oplus p_{HA\text{-}MU}$ and $L = h(ID_{MU} \,||\, R_{MU} \,||\, PW_{MU})$.
Step 5: HA stores $\{ID_{HA}, L, W, V, h(\cdot)\}$ into a smart card and issues it to MU via a secure channel.
Step 6: HA stores $\{U, R_{MU}, p_{HA\text{-}MU}\}$ into HA's database for MU.

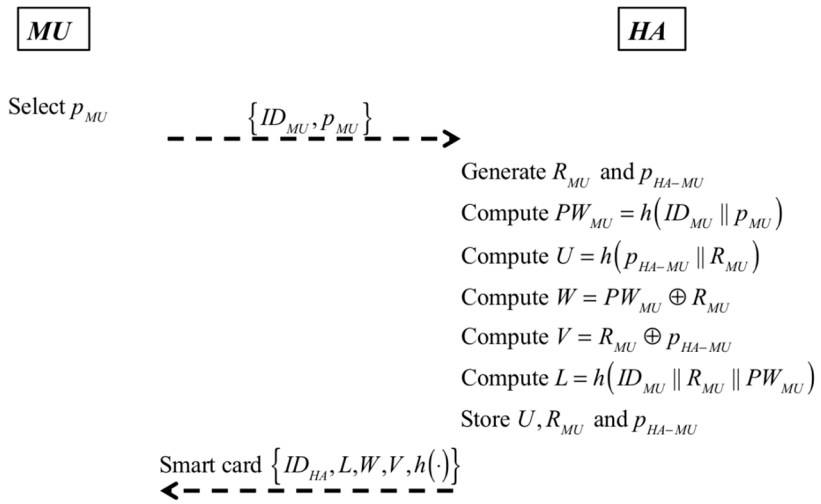

Figure 2. Registration phase in our scheme.

2.2. Login Phase

After registering with *HA*, *MU* can login with the smart card issued in registration phase to access the roaming service. Login phase is depicted in Figure 3, and the details are as follows:

Step 1: *MU* inserts his/her smart card into his/her terminal device and enters ID_{MU} and p_{MU}.

Step 2: The smart card computes $PW_{MU} = h(ID_{MU} \,||\, p_{MU})$, $R_{MU} = W \oplus PW_{MU}$, and $L' = h(ID_{MU} \,||\, R_{MU} \,||\, PW_{MU})$.

Step 3: The smart card checks if L' is equal to L. If it does not hold, the smart card aborts the process and accumulates the number of times for L' is not equal to L. If the entered ID_{MU} and p_{MU} make L' and L differ from each other three consecutive times, the smart card will be locked automatically. Note that the counter will be reset to zero when the entered ID_{MU} and p_{MU} have L' equal L.

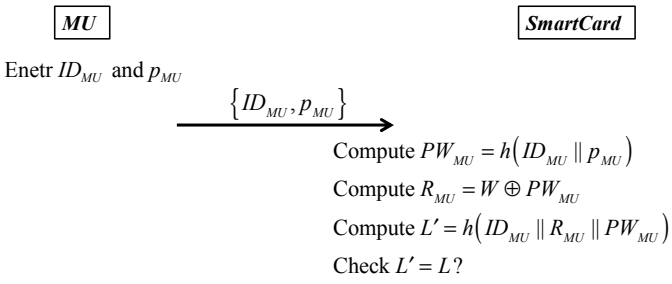

Figure 3. Login phase in our scheme.

2.3. Authentication and Establishment of the Session Key Phase

After the login phase, the authentication and establishment of the session key phase is executed. In this phase, *MU* can be authenticated anonymously and negotiate a session key with *FA* while roaming. In the proposed scheme, *HA* and *FA* share a secret key $p_{FA\text{-}HA}$ in advance, where different *FA*'s possess different $p_{FA\text{-}HA}$'s. The authentication and establishment of the session key phase is depicted in Figure 4, and the details are as follows:

Step 1: The smart card generates a new random nonce $R_{MU_{new}}$ and selects a random number b_0.

Step 2: The smart card computes b_0P, $R_{MU} = PW_{MU} \oplus W$, $p_{HA\text{-}MU} = R_{MU} \oplus V$, $S_1 = h(p_{HA\text{-}MU} \,||\, R_{MU})$, $S_2 = R_{MU} \oplus R_{MU_{new}}$, and $S_3 = h(R_{MU} \oplus h(p_{HA\text{-}MU} \,||\, R_{MU_{new}}) \,||\, b_0P.x)$.

Step 3: *MU* sends $\{ID_{HA}, S_1, S_2, S_3, b_0P\}$ to *FA* and stores $\{b_0, R_{MU_{new}}\}$.

Step 4: After *FA* receives $\{ID_{HA}, S_1, S_2, S_3, b_0P\}$, *FA* selects a new random number a_0 and computes a_0P and $S_{FA_1} = h(a_0P.x \,||\, b_0P.x \,||\, p_{FA\text{-}HA})$.

Step 5: *FA* stores the information $\{ID_{HA}, b_0P, a_0, a_0P\}$ and sends $\{ID_{FA}, S_1, S_2, S_3, a_0P, b_0P, S_{FA_1}\}$ to *HA*.

Step 6: When *HA* receives $\{ID_{FA}, S_1, S_2, S_3, a_0P, b_0P, S_{FA_1}\}$, *HA* uses S_1 to get the corresponding data $\{R_{MU}, p_{HA\text{-}MU}\}$ from its database because the matched $\{R_{MU}, p_{HA\text{-}MU}\}$ makes $S_1 = h(p_{HA\text{-}MU} \,||\, R_{MU})$. Then *HA* computes $R_{MU_{new}} = S_2 \oplus R_{MU}$, $S'_3 = h(R_{MU} \oplus h(p_{HA\text{-}MU} \,||\, R_{MU_{new}}) \,||\, b_0P.x)$, and $S'_{FA_1} = h(a_0P.x \,||\, b_0P.x \,||\, p_{FA\text{-}HA})$.

Step 7: *HA* checks if $S'_3 = S_3$ and $S'_{FA_1} = S_{FA_1}$. If they both hold, *HA* selects a new random number c_0 and computes c_0P and $S_4 = h(c_0b_0P.x \,||\, a_0P.x \,||\, ID_{FA} \,||\, ID_{HA} \,||\, R_{MU} \,||\, R_{MU_{new}})$; otherwise, *HA* aborts this authentication request and terminates this phase. After that, *HA* updates U and R_{MU} stored in its database to $h(p_{HA\text{-}MU} \,||\, R_{MU_{new}})$ and $R_{MU_{new}}$, respectively. Note that the original $U = S_1$ and the original R_{MU} are also stored in *HA*'s database to resist the synchronization problem. That is, the original U instead of the updated one will be searched to find the corresponding data {the original R_{MU}, $p_{HA\text{-}MU}$} when only *HA*'s data is updated.

Step 8: *HA* computes $S_{FA_2} = h(c_0a_0P.x \,||\, b_0P.x \,||\, p_{FA\text{-}HA})$ and sends $\{ID_{HA}, c_0P, S_4, S_{FA_2}\}$ to *FA*.

Step 9: After receiving $\{ID_{HA}, c_0P, S_4, S_{FA_2}\}$ from *HA*, *FA* checks if ID_{HA} exists in its database. If it does exist, *FA* computes $S'_{FA_2} = h(a_0c_0P.x \,||\, b_0P.x \,||\, p_{FA\text{-}HA})$ and checks if $S'_{FA_2} = S_{FA_2}$. If it does hold, *FA* computes $K_{MF_0} = h(a_0b_0P.x)$ and $C_{MF_0} = h(h(K_{MF_0} \,||\, b_0P.x))$; otherwise, *FA* terminates this phase directly.

Step 10: *FA* sends $\{ID_{FA}, S_4, a_0P, c_0P, C_{MF_0}\}$ to *MU*.

Step 11: When *MU* receives $\{ID_{FA}, S_4, a_0P, c_0P, C_{MF_0}\}$, *MU* computes $S'_4 = h(b_0c_0P.x \,||\, a_0P.x \,||\, ID_{FA} \,||\, ID_{HA} \,||\, R_{MU} \,||\, R_{MU_{new}})$ and checks whether S_4 is equal to S'_4. If it does not hold, *MU* terminates this phase directly; otherwise, *MU* computes the session key $K_{MF_0} = h(b_0a_0P.x)$, $C'_{MF_0} = h(K_{MF_0} \,||\, b_0P.x)$, and $C''_{MF_0} = h(C'_{MF_0})$, and checks if $C_{MF_0} = C''_{MF_0}$. If it does not hold, *MU* terminates this phase directly; otherwise, *MU* computes $B_{MF_0} = h(c_0P.x \,||\, K_{MF_0})$, updates W to $W_{new} = PW_{MU} \oplus R_{MU_{new}}$ and V to $V_{new} = R_{MU_{new}} \oplus p_{HA\text{-}MU}$ and stores C'_{MF_0}, a_0P, b_0P, and the session key K_{MF_0}.

Step 12: *MU* sends $\{B_{MF_0}\}$ to *FA*.

Step 13: After obtaining $\{B_{MF_0}\}$, *FA* computes $B'_{MF_0} = h(c_0P.x \,||\, K_{MF_0})$ and checks if $B_{MF_0} = B'_{MF_0}$. If it does not hold, *FA* terminates this phase directly; otherwise, *FA* stores $\{C_{MF_0}, a_0P, b_0P, K_{MF_0}\}$ into its database.

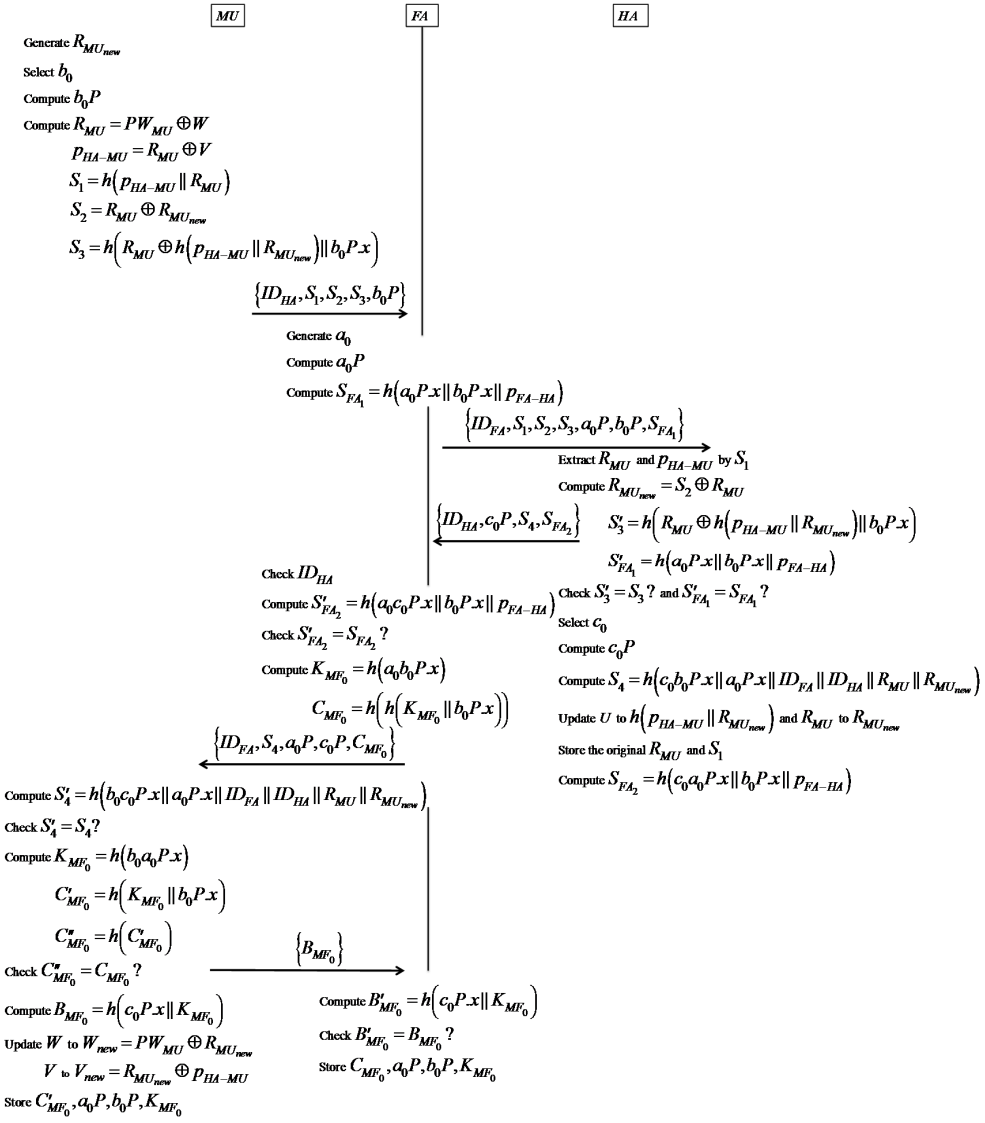

Figure 4. Authentication and establishment of the session key phase in our scheme.

After the above, *FA* and *MU* share the session key K_{MF_0}. Thereupon, the communication between *FA* and *MU* can be protected by K_{MF_0}.

2.4. Update Session Key Phase

After being authenticated by *HA* via *FA*, *MU* can update the session key shared with *FA* for some security issues while staying in the same *FA* continuously. For generality, assume that *MU* has stayed in the same *FA* and updated the session i times. Thus, the secret key shared between *FA* and *MU* is $K_{MF_i} = h(a_i b_i P.x) = h(b_i a_i P.x)$ while *FA* and *MU* store $\{C_{MF_i}, a_iP, b_iP, K_{MF_i}\}$ and $\{C'_{MF_i}, a_iP, b_iP, K_{MF_i}\}$, respectively. Update session key phase is depicted in Figure 5, and the details are as follows:

Step 1: *MU* selects a new random number b_{i+1} and computes $b_{i+1}P$ and $h_1 = h(b_iP.x \,||\, b_{i+1}P.x \,||\, K_{MF_i})$.

Step 2: *MU* sends $\{b_{i+1}P, C'_{MF_i}, h_1\}$ to *FA*.

Step 3: After receiving $\{b_{i+1}P, C'_{MF_i}, h_1\}$, *FA* checks if $h(C'_{MF_i})$ exists in its database, where $h(C'_{MF_i}) = C_{MF_i}$. If it does not exist, *FA* terminates this phase; otherwise, *FA* extracts $\{C_{MF_i}, a_iP, b_iP, K_{MF_i}\}$ from its database.

Step 4: *FA* computes $h'_1 = h(b_iP.x \,||\, b_{i+1}P.x \,||\, K_{MF_i})$ and checks if h'_1 is equal to h_1. If it does not hold, *FA* terminates this phase; otherwise, *FA* selects a new random number a_{i+1} and computes $a_{i+1}P$, $K_{MF_{i+1}} = h(a_{i+1}b_{i+1}P.x)$, $C_{MF_{i+1}} = h(h(K_{MF_{i+1}} \,||\, b_{i+1}P.x))$ and $h_2 = h(C_{MF_{i+1}} || K_{MF_i} || K_{MF_{i+1}})$.

Step 5: *FA* updates $\{C_{MF_i}, a_iP, b_iP, K_{MF_i}\}$ to $\{C_{MF_{i+1}}, a_{i+1}P, b_{i+1}P, K_{MF_{i+1}}\}$ in its database and sends $\{a_{i+1}P, h_2\}$ to *MU*.

Step 6: When *MU* receives $\{a_{i+1}P, h_2\}$ from *FA*, *MU* computes $K_{MF_{i+1}} = h(b_{i+1}a_{i+1}P.x)$, $C'_{MF_{i+1}} = h(K_{MF_{i+1}} \,||\, b_{i+1}P.x)$, and $h'_2 = h(h(C'_{MF_{i+1}}) \,||\, K_{MF_i} || K_{MF_{i+1}})$. Then, *MU* checks if h'_2 is equal to h_2. If it does not hold, *MU* terminates this phase; otherwise, *MU* updates $\{C'_{MF_i}, a_iP, b_iP, K_{MF_i}\}$ to $\{C'_{MF_{i+1}}, a_{i+1}P, b_{i+1}P, K_{MF_{i+1}}\}$ in the mobile device.

If this phase is terminated by *MU* or *FA* and *MU* still wants to access the roaming service, login phase is executed immediately.

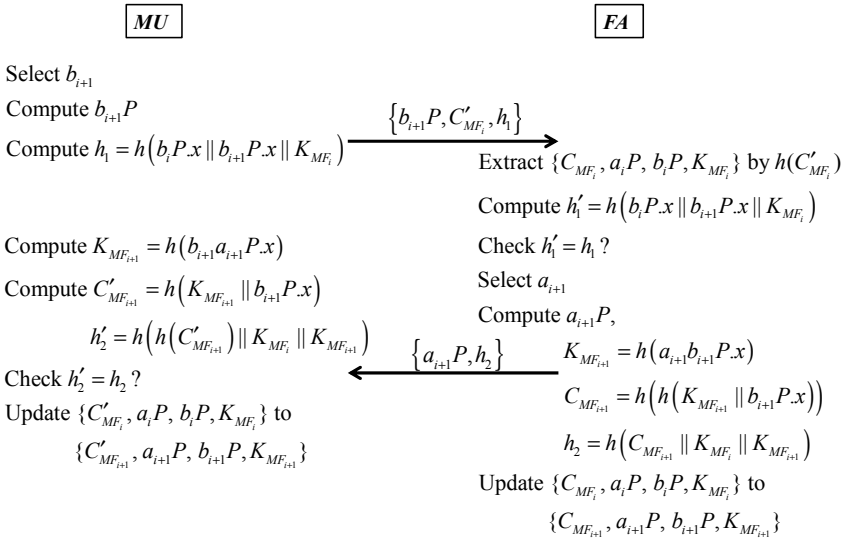

Figure 5. Update session key phase in our scheme.

2.5. Password Change Phase

MU can change his/her password with his/her smart card at will without *HA*'s help. Password change phase is depicted in Figure 6, and the details are as follows:

Step 1: *MU* inserts his/her smart card into his/her terminal device and enters ID_{MU} and p_{MU}.

Step 2: The smart card computes $PW_{MU} = h(ID_{MU} \,||\, p_{MU})$, $R_{MU} = W \oplus PW_{MU}$ and $L' = h(ID_{MU} \,||\, R_{MU} \,||\, PW_{MU})$.

Step 3: The smart card checks if L' is equal to L. If it does not hold, the smart card aborts the process.

Step 4: If L' equals L, MU selects the new password $p_{MU_{new}}$ and sends it to the smart card. Note that this approach can be executed by entering $p_{MU_{new}}$ with an embedded keyboard.

Step 5: When the smart card receives the new password $p_{MU_{new}}$, it will ask MU to enter $p_{MU_{new}}$ again for correctness. If the reentered password is different from the previous one, the smart card will inform MU of this issue. MU may resend the new password or terminate this phase. If the reentered password and the previous one are the same, the smart card computes $PW_{MU_{new}}$, $W_{new} = PW_{MU_{new}} \oplus R_{MU}$ and $L_{new} = h(ID_{MU} \,||\, R_{MU} \,||\, PW_{MU_{new}})$. Then, the smart card updates W to W_{new} and L to L_{new}.

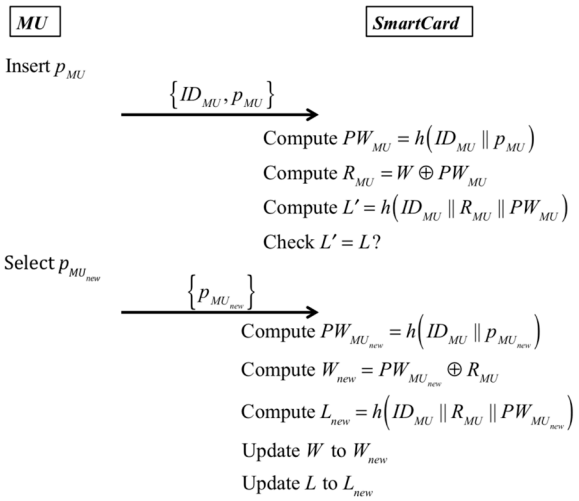

Figure 6. Password change phase in our scheme.

3. Property Analysis

In this section, we analyze our proposed scheme's security and convenience by taking the following four properties into consideration: (1) user anonymity; (2) resistance to common attacks; (3) local password change; and (4) mutual authentication. In the following, we discuss our scheme to show that it possesses these properties.

3.1. User Anonymity

In our proposed scheme, MU's real identifier is concealed in $PW_{MU} = h(ID_{MU} \,||\, p_{MU})$ and is never transmitted when MU wants to access the roaming service. In authentication and establishment of the session key phase, MU sends $\{ID_{HA}, S_1, S_2, S_3, b_0P\}$ to FA, where $S_1 = h(p_{HA\text{-}MU} \,||\, R_{MU})$, $S_2 = R_{MU} \oplus R_{MU_{new}}$, and $S_3 = h(R_{MU} \oplus h(p_{HA\text{-}MU} \,||\, R_{MU_{new}}) \,||\, b_0P.x)$. After authenticating MU and FA successfully, HA sends $\{ID_{HA}, c_0P, S_4, S_{FA_2}\}$ to FA, where $S_4 = h(c_0b_0P.x \,||\, a_0P.x \,||\, ID_{FA} \,||\, ID_{HA} \,||\, R_{MU} \,||\, R_{MU_{new}})$. Parameters S_1, S_2, S_3, and S_4 contain MU's specific information R_{MU} and $R_{MU_{new}}$ and are transmitted via public channels. Because R_{MU} and $R_{MU_{new}}$ will be updated in each session, it denotes that S_1, S_2, S_3, and S_4 in one session differ from those in other sessions. That is, no constant parameter is transmitted for MU in different sessions, and our scheme ensures user anonymity.

3.2. Resistance to Common Attacks

To show that the proposed authentication scheme can resist common attacks to ensure security, common attacks, man-in-the-middle attack, desynchronization attack, insider attack, replay attack,

and offline secret key guessing attack are taken into consideration. These attacks are chosen for security analysis because of the following reasons. First, *HA*, *MU*, and *FA* transmit data via public channels. It is essential to protect all communication parties from being threatened by an attacker without being detected when the authentication scheme is in progress. This denotes that the proposed scheme has to resist man-in-the-middle attack. Second, in authentication and establishment of the session key phase of the proposed scheme, the random nonce R_{MU} kept by *HA* will be updated to $R_{MU_{new}}$ after *MU* is authenticated successfully, and *MU* will update W to $W_{new} = PW_{MU} \oplus R_{MU_{new}}$ and V to $V_{new} = R_{MU_{new}} \oplus p_{HA\text{-}MU}$ after *MU* is assured that $C_{MF_0} = C''_{MF_0}$. If only *HA* updates U to $h(p_{HA\text{-}MU} \,||\, R_{MU_{new}})$ and R_{MU} to $R_{MU_{new}}$ while W and V are not updated, *MU* may be regarded as an illegal user. That is, the proposed scheme has to resist desynchronization attacks to ensure that an authorized mobile user can access the service even when the new authentication parameters are modified by an attacker. Third, the proposed scheme has to resist insider attacks such that no one can impersonate a legal mobile user even when a malicious insider with privileges can access the home agent's database. Forth, the proposed scheme has to resist replay attack such that no one can impersonate *MU* to cheat *FA* and *HA* by sending the intercepted data transmitted in previous sessions. Fifth, because the computational capacities of computers progress rapidly, an attacker can eavesdrop to get transmitted messages and analyze them offline. That is, an attacker may attempt to retrieve the secrets $p_{HA\text{-}MU}$ and $p_{FA\text{-}HA}$ by mounting an offline secret key guessing attack. The corresponding analysis is given as follows.

In authentication and establishment of the session key phase, an attacker may mount a man-in-the-middle attack by impersonating a communication party to establish the session key with another innocent communication party. First, we assume an attacker tries to impersonate *MU* and establish the session key with *FA* by modifying b_0P. However, this approach will never succeed because *MU* computes $S_3 = h(R_{MU} \oplus h(p_{HA\text{-}MU} \,||\, R_{MU_{new}}) \,||\, b_0P.x)$ for *HA* and *HA* verifies b_0P by checking whether $S_3 = S'_3$. *FA* can also verify b_0P by checking whether $S'_{FA_2} = S_{FA_2}$. On the other hand, if the attacker tries to impersonate *FA* and establish the session key with *MU* by modifying a_0P, this approach will never succeed because *HA* can verify a_0P by checking whether $S'_{FA_1} = S_{FA_1}$ and *MU* can verify a_0P by checking whether $S_4 = S'_4$. In the update session key phase, *FA* authenticates *MU* by checking if $h_1 = h'_1$ and *MU* authenticates *FA* by checking if $h_2 = h'_2$ Because of the above reasons, our scheme can resist man-in-the-middle attacks.

In the authentication and establishment of the session key phase, an attacker may attempt to mount a desynchronization attack by disturbing the authentication process after *HA* updates U to $h(p_{HA\text{-}MU} \,||\, R_{MU_{new}})$ and R_{MU} to $R_{MU_{new}}$ in its database. Although *MU* does not update W and V in his/her smart card, *MU* still can be authenticated by *HA* successfully because *HA* stores the original R_{MU} and the original U. Because of the above reasons, our scheme can resist desynchronization attack.

Assume that a malicious insider with privileges tries to get *MU*'s private data in *HA*'s database to impersonate *MU*. In our proposed scheme, this attack cannot be mounted successfully because *HA* does not store a user's password and his/her real identifier. No insider can obtain p_{MU} and ID_{MU} to compute *MU*'s secret PW_{MU}, where $PW_{MU} = h(ID_{MU} \,||\, p_{MU})$. Therefore, our scheme can resist insider attack.

In authentication and establishment of the session key phase, anyone can eavesdrop to intercept the transmitted data because the channel is public. In Step 3, *MU* sends $\{ID_{HA}, S_1, S_2, S_3, b_0P\}$ to *FA* and stores $R_{MU_{new}}$, where $S_1 = h(p_{HA\text{-}MU} \,||\, R_{MU})$, $S_2 = R_{MU} \oplus R_{MU_{new}}$, and $S_3 = h(R_{MU} \oplus h(p_{HA\text{-}MU} \,||\, R_{MU_{new}}) \,||\, b_0P.x)$. In Step 10, *FA* sends $\{ID_{FA}, S_4, a_0P, c_0P, C_{MF_0}\}$ to *MU*, where $C_{MF_0} = h(h(K_{MF_0} \,||\, b_0P.x)) = h(h(h(a_0b_0P.x) \,||\, b_0P.x))$. In Step 12, *MU* sends $\{B_{MF_0}\}$ to *FA*, where $B_{MF_0} = h(c_0P.x \,||\, K_{MF_0})$. In Step 13, *FA* computes $B'_{MF_0} = h(c_0P.x \,||\, K_{MF_0})$ and checks if $B_{MF_0} = B'_{MF_0}$ to determine whether *MU* is legal. After an attacker eavesdrops, he may use the intercepted data to cheat *HA* and *FA* to access services. However, the attacker cannot mount a reply attack successfully because of the following. $K_{MF_0} = h(a_0b_0P.x)$ and $B_{MF_0} = h(c_0P.x \,||\, K_{MF_0}) = h(c_0P.x \,||\, h(a_0b_0P.x))$. If the attacker wants to cheat, he has to obtain a_0b_0P. Although a_0P and b_0P are available, the attacker knows neither a_0 nor b_0 because of the difficulty of solving the elliptic curve discrete logarithm problem (ECDLP). As a result, the attacker

cannot compute a_0b_0P to obtain B_{MF_0}. Since B_{MF_0} cannot be obtained by the attacker, he cannot be authenticated by *FA* successfully by retransmitting the intercepted data. Therefore, our scheme can resist replay attack.

In the authentication and establishment of the session key phase, *HA* authenticates *FA* by checking whether $S'_{FA_1} = S_{FA_1}$, and *FA* authenticates *HA* by checking whether $S'_{FA_2} = S_{FA_2}$, where $S_{FA_1} = h(a_0P.x \,||\, b_0P.x \,||\, p_{FA\text{-}HA})$ and $S_{FA_2} = h(c_0a_0P.x \,||\, b_0P.x \,||\, p_{FA\text{-}HA})$. The secret $p_{FA\text{-}HA}$ shared between *FA* and *HA* is contained in both S_{FA_1} and S_{FA_2}. Although a_0P, b_0P and c_0P are available, an attacker cannot compute c_0a_0P because of the difficulty of solving ECDLP. On the other hand, *MU* authenticates *HA* by checking whether $S_4 = S'_4$ and *HA* authenticates *MU* by checking whether $S_3 = S'_3$, where $S_4 = h(c_0b_0P.x \,||\, a_0P.x \,||\, ID_{FA} \,||\, ID_{HA} \,||\, R_{MU} \,||\, R_{MU_{new}})$ and $S_3 = h(R_{MU} \oplus h(p_{HA\text{-}MU} \,||\, R_{MU_{new}}) \,||\, b_0P.x)$. The secret $p_{HA\text{-}MU}$ shared between *MU* and *HA* is contained in the transmitted parameters S_1 and S_3, where $S_1 = h(p_{HA\text{-}MU} \,||\, R_{MU})$. If an attacker wants to obtain $p_{HA\text{-}MU}$, he has to guess R_{MU} at the same time. This makes retrieving $p_{HA\text{-}MU}$ hard. Because of the above, offline secret key guessing attacks cannot be mounted on the proposed scheme.

3.3. Local Password Change

In our proposed scheme, *MU* can locally update his/her password. When *MU* wants to change his/her password PW_{MU} to the new password $PW_{MU_{new}}$, he/she does not need to connect to *HA*. This means a user can change his/her password at will.

3.4. Mutual Authentication

First, we make discussions on communication parties *MU*, *FA* and *HA* in authentication and establishment of the session key phase by the following three cases.

Case 1: Mutual authentication between *FA* and *HA*

HA authenticates *FA* by checking whether $S'_{FA_1} = S_{FA_1}$, and *FA* authenticates *HA* by checking whether $S'_{FA_2} = S_{FA_2}$, where $S_{FA_1} = h(a_0P.x \,||\, b_0P.x \,||\, p_{FA\text{-}HA})$ and $S_{FA_2} = h(c_0a_0P.x \,||\, b_0P.x \,||\, p_{FA\text{-}HA})$. Because $p_{FA\text{-}HA}$ is only known to *FA* and *HA*, it denotes that only *FA* and *HA* can compute the correct parameters to be authenticated successfully. That is, our proposed scheme provides mutual authentication between *FA* and *HA*.

Case 2: Mutual authentication between *MU* and *HA*

MU authenticates *HA* by checking whether $S_4 = S'_4$, and *HA* authenticates *MU* by checking whether $S_3 = S'_3$, where $S_4 = h(c_0b_0P.x \,||\, a_0P.x \,||\, ID_{FA} \,||\, ID_{HA} \,||\, R_{MU} \,||\, R_{MU_{new}})$ and $S_3 = h(R_{MU} \oplus h(p_{HA\text{-}MU} \,||\, R_{MU_{new}}) \,||\, b_0P.x)$. Only *MU* and *HA* can compute the correct parameters to be authenticated successfully because $p_{HA\text{-}MU}$, $R_{MU_{new}}$ and R_{MU} are only known to *MU* and *HA*. As the result, our proposed scheme provides mutual authentication between *MU* and *HA*.

Case 3: Mutual authentication between *MU* and *FA*

In authentication and establishment of the session key phase, *MU* authenticates *HA* by checking if $S_4 = S'_4$, where $S_4 = h(c_0b_0P.x \,||\, a_0P.x \,||\, ID_{FA} \,||\, ID_{HA} \,||\, R_{MU} \,||\, R_{MU_{new}})$. Because only *HA* and *MU* know $p_{HA\text{-}MU}$, $R_{MU_{new}}$ and R_{MU}, only *HA* can compute c_0b_0P and S_4. If $S_4 = S'_4$, it denotes (1) a_0P is valid because S_4 contains $a_0P.x$ and (2) *FA* has been already authenticated by *HA*. Then, *MU* computes the session key $K_{MF_0} = h(b_0a_0P.x)$, $C'_{MF_0} = h(K_{MF_0} \,||\, b_0P.x)$, and $C''_{MF_0} = h(C'_{MF_0})$ and checks if $C_{MF_0} = C''_{MF_0}$. If $C_{MF_0} = C''_{MF_0}$, it denotes that *FA* really knows $K_{MF_0} = h(a_0b_0P.x)$. Because *MU* has already authenticated *HA*, *MU* is assured that only *FA* knows a_0 to compute K_{MF_0}. As a result, *FA* is authenticated successfully by *MU*. Thereupon, *MU* computes $B_{MF_0} = h(c_0P.x \,||\, K_{MF_0})$ and sends it to *FA*. After obtaining $\{B_{MF_0}\}$, *FA* computes $B'_{MF_0} = h(c_0P.x \,||\, K_{MF_0})$ and checks if $B_{MF_0} = B'_{MF_0}$. If $B_{MF_0} = B'_{MF_0}$, *FA* is assured that *MU* knows b_0 to compute K_{MF_0}. *FA* has authenticated *HA* by checking if $S'_{FA_2} = S_{FA_2}$, where $S_{FA_2} = h(c_0a_0P.x \,||\, b_0P.x \,||\, p_{FA\text{-}HA})$. It denotes (1) b_0P is valid because

S_{FA_2} contains $b_0P.x$ and (2) *MU* has been already authenticated by *HA*. As a result, *MU* is authenticated successfully by *FA*. Therefore, our proposed scheme provides mutual authentication between *MU* and *FA*.

Second, we make discussions on communication parties *MU* and *FA* in the update session key phase. Because *MU* and *FA* have already shared the session key $K_{MF_i} = h(a_ib_iP.x)$ in the previous session, they can use K_{MF_i} and the stored data to authenticate each other. At the moment, *FA* stores $\{C_{MF_i}, a_iP, b_iP, K_{MF_i}\}$ and *MU* stores $\{C'_{MF_i}, a_iP, b_iP, K_{MF_i}\}$, where $C'_{MF_0} = h(K_{MF_0} \,||\, b_0P.x)$ and $C_{MF_0} = h(h(K_{MF_0} \,||\, b_0P.x)) = h(C'_{MF_0})$. *MU* selects r b_{i+1}, computes $b_{i+1}P$ and $h_1 = h(b_iP.x \,||\, b_{i+1}P.x \,||\, K_{MF_i})$, and sends $\{b_{i+1}P, C'_{MF_i}, h_1\}$ to *FA*. After receiving $\{b_{i+1}P, C'_{MF_i}, h_1\}$, *FA* checks if $h(C'_{MF_i})$ exists in its database, where $h(C'_{MF_i}) = C_{MF_i}$. Because it is hard to find the input of the hash function with a known hash value, this search approach protects *MU* from being traced even he stays in *FA*'s service domain and implies *MU*'s legality. After finding the matched C_{MF_i}, *FA* extracts $\{C_{MF_i}, a_iP, b_iP, K_{MF_i}\}$ from its database and selects a_{i+1}. *FA* computes $h'_1 = h(b_iP.x \,||\, b_{i+1}P.x \,||\, K_{MF_i})$ and checks if $h'_1 = h_1$. If $h'_1 = h_1$, it denotes (1) *MU* indeed knows K_{MF_i} and (2) $b_{i+1}P$ is valid. *FA* authenticates *MU* successfully. Then, *FA* computes $a_{i+1}P$, $K_{MF_{i+1}} = h(a_{i+1}b_{i+1}P.x)$, $C_{MF_{i+1}} = h(h(K_{MF_{i+1}} \,||\, b_{i+1}P.x))$ and $h_2 = h(C_{MF_{i+1}}||K_{MF_i}||K_{MF_{i+1}})$. *FA* updates $\{C_{MF_i}, a_iP, b_iP, K_{MF_i}\}$ to $\{C_{MF_{i+1}}, a_{i+1}P, b_{i+1}P, K_{MF_{i+1}}\}$ in its database and sends $\{a_{i+1}P, h_2\}$ to *MU*. After receiving $\{a_{i+1}P, h_2\}$, *MU* computes $K_{MF_{i+1}} = h(b_{i+1}a_{i+1}P.x)$, $C'_{MF_{i+1}} = h(K_{MF_{i+1}} \,||\, b_{i+1}P.x)$, and $h'_2 = h(h(C'_{MF_{i+1}}) \,||\, K_{MF_i}||K_{MF_{i+1}})$. Then, *MU* checks if $h'_2 = h_2$. If $h'_2 = h_2$, it denotes that *FA* indeed knows K_{MF_i} and $K_{MF_{i+1}}$. *MU* authenticates *FA* successfully. As a result, mutual authentication is ensured in update session key phase.

4. Further Discussions

In this section, we first make comparisons between the proposed scheme and the related works, and BAN logic is then used to deduce the completeness of the proposed authentication scheme.

4.1. Comparisons

In the following, we present a discussion of the properties of the proposed scheme and the related works. The term "Local password change" denotes whether the mobile user can locally change his password without the home agent's help in the corresponding scheme. The term "Anonymity" denotes whether the corresponding scheme can ensure user anonymity. The term "Insider attack resistance" denotes whether the corresponding scheme can resist insider attack. The term "Man-in-the-middle attack resistance" denotes whether the corresponding scheme can resist man-in-the-middle attack. The term "The synchronization problem resistance" denotes whether the corresponding scheme can resist the synchronization problem. "Replay attack resistance" denotes whether the corresponding scheme can resist replay attack. The comparisons between our scheme and the related works are given in Table 2. According to the comparisons, it is assured that our scheme can resist common attacks and ensure security and convenience at the same time while others cannot.

Table 2. Comparisons between our scheme and the related works.

Schemes	Ours	Kuo et al.'s [9]	Lu et al.'s [10]
Local password change	Yes	No	Yes
Anonymity	Yes	Yes	No
Insider attack resistance	Yes	No	Yes
Man-in-the-middle attack resistance	Yes	No	Yes
The synchronization problem resistance	Yes	No	Yes
Replay attack resistance	Yes	Yes	No

4.2. BAN Logic-Based Authentication Proof

In the following, BAN logic is used to deduce the completeness of the proposed authentication scheme. Notations used in BAN logic are listed in Table 3.

Table 3. Notations used in Burrows-Abadi-Needham logic (BAN logic).

Symbol	Definition
A, B	Principals indicate general instances participating in a protocol.
$A\mid\equiv M$	A believes the statement M.
$A \lhd M$	A sees M.
$A\mid\sim M$	A once said M.
$A \Rightarrow M$	A has jurisdiction over M.
$\#(M)$	M is a fresh message.
$<M>_N$	Formula M is combined with formula N.
(M, N)	M or N is one part of message (M, N).
$(M)_K$	M is hashed with the secret K.
$A \overset{K}{\longleftrightarrow} B$	K is the secret shared between A and B.

Fundamental rules for BAN logic analysis are listed as follows:

RBL1 (Message Meaning Rule 1): $\frac{A\mid\equiv A\overset{N}{\longleftrightarrow}B,\ A\lhd<M>_N}{A\mid\equiv B\mid\sim M}$.

RBL2 (Message Meaning Rule 2): $\frac{A\mid\equiv A\overset{K}{\longleftrightarrow}B,\ A\lhd(M)_K}{A\mid\equiv B\mid\sim M}$.

RBL3 (Nonce Verification Rule): $\frac{A\mid\equiv\#(M),A\mid\equiv B\mid\sim M}{A\mid\equiv B\mid\equiv M}$.

RBL4 (Jurisdiction Rule): $\frac{A\mid\equiv B\Rightarrow M,A\mid\equiv B\mid\equiv M}{A\mid\equiv M}$.

RBL5 (Freshness Conjunction Rule): $\frac{A\mid\equiv\#(M)}{A\mid\equiv\#(M,N)}$.

RBL6 (Belief Rule): $\frac{A\mid\equiv(M),A\mid\equiv(N)}{A\mid\equiv(M,N)}$.

RBL7 (Session Key Rule): $\frac{A\mid\equiv\#(M),A\mid\equiv B\mid\equiv M}{A\mid\equiv A\overset{K}{\longleftrightarrow}B}$.

The following goals must be satisfied by using the above rules to ensure the security of the proposed authentication scheme under BAN logic.

Goal 1: $HA\mid\equiv MU\overset{R_{MU_{new}},c_0b_0P}{\longleftrightarrow}HA$.

Goal 2: $HA\mid\equiv MU\mid\equiv MU\overset{R_{MU_{new}},c_0b_0P}{\longleftrightarrow}HA$.

Goal 3: $MU\mid\equiv MU\overset{R_{MU_{new}},\ b_0c_0P}{\longleftrightarrow}HA$.

Goal 4: $MU\mid\equiv HA\mid\equiv MU\overset{R_{MU_{new}},\ b_0c_0P}{\longleftrightarrow}HA$.

Goal 5: $HA\mid\equiv FA\overset{c_0a_0P}{\longleftrightarrow}HA$.

Goal 6: $HA\mid\equiv FA\mid\equiv FA\overset{c_0a_0P}{\longleftrightarrow}HA$.

Goal 7: $FA\mid\equiv FA\overset{a_0c_0P}{\longleftrightarrow}HA$.

Goal 8: $FA\mid\equiv HA\mid\equiv FA\overset{a_0c_0P}{\longleftrightarrow}HA$.

Goal 9: $MU\mid\equiv FA\overset{K_{MF_0}}{\longleftrightarrow}MU$.

Goal 10: $MU\mid\equiv FA\mid\equiv FA\overset{K_{MF_0}}{\longleftrightarrow}MU$.

Goal 11: $FA\mid\equiv FA\overset{K_{MF_0}}{\longleftrightarrow}MU$.

Goal 12: $FA| \equiv MU| \equiv FA \xleftrightarrow{K_{MF_0}} MU$.

Idealized transformation of the proposed scheme is as follows:

IM1: $MU \rightarrow FA$: ID_{HA}, S_1, S_2, S_3, b_0P:

$$\left\{ID_{HA}, h(p_{HA-MU}||R_{MU}), < R_{MU_{new}} >_{R_{MU}}, < b_0P >_{R_{MU} \oplus h(p_{HA-MU}||R_{MU_{new}})}, b_0P\right\}.$$

IM2: $FA \rightarrow HA$: ID_{FA}, S_1, S_2, S_3, a_0P, b_0P, S_{FA_1}:

$$\left\{ID_{FA}, h(p_{HA-MU}||R_{MU}), < R_{MU_{new}} >_{R_{MU}}, < b_0P >_{R_{MU} \oplus h(p_{HA-MU}||R_{MU_{new}})}, a_0P, b_0P, (a_0P, b_0P)_{p_{FA-HA}}\right\}.$$

IM3: HA $\rightarrow$ FA: ID_{HA}, c_0P, S_4, S_{FA_2}:

$$\left\{ID_{HA}, c_0P, (c_0b_0P, a_0P, b_0P, R_{MU_{new}})_{R_{MU}}, (c_0a_0P, b_0P)_{P_{FA-HA}}\right\}.$$

IM4: FA $\rightarrow$ MU: ID_{FA}, S_4, a_0P, c_0P, C_{MF_0}:

$$\left\{ID_{FA}, (c_0b_0P, a_0P, b_0P, R_{MU_{new}})_{R_{MU}}, a_0P, c_0P, (b_0P)_{K_{MF_0}}\right\}.$$

To evaluate the proposed scheme, assumptions regarding the preliminary state are shown as follows:

A1: $MU| \equiv MU \xleftrightarrow{R_{MU},\ p_{HA-MU}} HA$.
A2: $HA| \equiv MU \xleftrightarrow{R_{MU},\ p_{HA-MU}} HA$.
A3: $FA| \equiv FA \xleftrightarrow{p_{FA-HA}} HA$.
A4: $HA| \equiv FA \xleftrightarrow{p_{FA-HA}} HA$.
A5: $MU| \equiv \#(b_0)$.
A6: $FA| \equiv \#(a_0)$.
A7: $HA| \equiv \#(c_0)$.
A8: $HA| \equiv MU \Rightarrow b_0P$.
A9: $FA| \equiv MU \Rightarrow b_0P$.
A10: $MU| \equiv FA \Rightarrow a_0P$.
A11: $HA| \equiv FA \Rightarrow a_0P$.
A12: $MU| \equiv HA \Rightarrow c_0P$.
A13: $FA| \equiv HA \Rightarrow c_0P$.

Considering IM1 and IM2 of the idealized forms:

IM1: $MU \rightarrow FA$: ID_{HA}, S_1, S_2, S_3, b_0P:

$$\left\{ID_{HA}, h(p_{HA-MU}||R_{MU}), < R_{MU_{new}} >_{R_{MU}}, < b_0P >_{R_{MU} \oplus h(p_{HA-MU}||R_{MU_{new}})}, b_0P\right\}.$$

IM2: $FA \rightarrow HA$: ID_{FA}, S_1, S_2, S_3, a_0P, b_0P, S_{FA_1}:

$$\left\{ID_{FA}, h(p_{HA-MU}||R_{MU}), < R_{MU_{new}} >_{R_{MU}}, < b_0P >_{R_{MU} \oplus h(p_{HA-MU}||R_{MU_{new}})}, a_0P, b_0P, (a_0P, b_0P)_{p_{FA-HA}}\right\}.$$

By applying seeing rule, we have

S1: $FA \lhd ID_{HA}$, S_1, S_2, S_3, b_0P:

$$\left\{ID_{HA}, h(p_{HA-MU}||R_{MU}), < R_{MU_{new}} >_{R_{MU}}, < b_0P >_{R_{MU} \oplus h(p_{HA-MU}||R_{MU_{new}})}, b_0P\right\}.$$

S2: $HA \lhd ID_{FA}$, S_1, S_2, S_3, a_0P, b_0P, S_{FA_1}:

$$\left\{ID_{FA}, h(p_{HA-MU}||R_{MU}), < R_{MU_{new}} >_{R_{MU}}, < b_0P >_{R_{MU} \oplus h(p_{HA-MU}||R_{MU_{new}})}, a_0P, b_0P, (a_0P, b_0P)_{p_{FA-HA}}\right\}.$$

By S2, A2, and RBL1, we have

S3: $HA| \equiv MU| \sim \{h(p_{HA\text{-}MU} \,||\, R_{MU}), < R_{MU_{new}} >_{R_{MU}}, < b_0P >_{R_{MU} \oplus h(p_{HA-MU}||R_{MU_{new}})}, b_0P\}$.

By S3, A5, A8, RBL3, RBL4, and RBL7, we have

S4: $HA| \equiv MU \xleftrightarrow{R_{MU_{new}}, c_0b_0P} HA$. Goal 1

By S4, A7, A12, and RBL4, we have

S5: $HA| \equiv MU| \equiv MU \xleftrightarrow{R_{MU_{new}}, c_0b_0P} HA$. Goal 2

By S2, A4, and RBL2, we have

S6: $HA| \equiv FA| \sim \{ID_{FA}, a_0P, (a_0P, b_0P)_{p_{FA-HA}}\}$.

By S6, A6, A11, RBL3, RBL4, and RBL7, we have

S7: $HA| \equiv FA \xleftrightarrow{c_0a_0P} HA$ Goal 5

By S7, A7, A13, and RBL4, we have

S8: $HA| \equiv FA| \equiv FA \xleftrightarrow{c_0a_0P} HA$. Goal 6

Considering IM3 of the idealized form:

IM3: HA $\rightarrow$ FA: ID_{HA}, c_0P, S_4, S_{FA_2}:

$$\left\{ID_{HA}, c_0P, (c_0b_0P, a_0P, b_0P, R_{MU_{new}})_{R_{MU}}, (c_0a_0P, b_0P)_{P_{FA-HA}}\right\}.$$

By applying seeing rule, we have

S9: $FA \lhd ID_{HA}$, c_0P, S_4, S_{FA_2}:

$$\left\{ID_{HA}, c_0P, (c_0b_0P, a_0P, b_0P, R_{MU_{new}})_{R_{MU}}, (c_0a_0P, b_0P)_{P_{FA-HA}}\right\}.$$

By S9, A3, A7, A13, RBL2, RBL3, RBL4, and RBL7, we have

S10: $FA| \equiv HA| \sim \{ID_{HA}, c_0P, (c_0a_0P, b_0P)_{P_{FA-HA}}\}$,

S11: $FA| \equiv FA \xleftrightarrow{a_0c_0P} HA$, Goal 7

S12: $FA| \equiv HA| \equiv FA \xleftrightarrow{a_0c_0P} HA$, and Goal 8

S13: $FA| \equiv MU| \sim b_0P$.

By S13, A5, and A9, we have

S14: $FA| \equiv FA \xleftrightarrow{K_{MF_0}} MU$ and Goal 11

S15: $FA| \equiv MU| \equiv FA \xleftrightarrow{K_{MF_0}} MU$ Goal 12

Considering IM4 of the idealized form:

IM4: FA $\rightarrow$ MU: ID_{FA}, S_4, a_0P, c_0P, C_{MF_0}:

$$\left\{ID_{FA}, (c_0b_0P, a_0P, b_0P, R_{MU_{new}})_{R_{MU}}, a_0P, c_0P, (b_0P)_{K_{MF_0}}\right\}.$$

By applying seeing rule, we have

S16: $MU \lhd ID_{FA}, S_4, a_0P, c_0P, C_{MF_0}$:

$$\left\{ID_{FA}, (c_0b_0P, a_0P, b_0P, R_{MU_{new}})_{R_{MU}}, a_0P, c_0P, (b_0P)_{K_{MF_0}}\right\}.$$

By S16, A1, and RBL1, we have

S17: $MU| \equiv HA| \sim\{(c_0b_0P, a_0P, b_0P, R_{MU_{new}})_{R_{MU}}, a_0P, c_0P\}$.

By S17, A7, A12, RBL3, RBL4, and RBL7, we have

S18: $HA| \equiv MU \xleftrightarrow{R_{MU_{new}}, c_0b_0P} HA$ and Goal 3

S19: $MU| \equiv HA| \equiv MU \xleftrightarrow{R_{MU_{new}}, b_0c_0P} HA$. Goal 4

By S16, A6, A10, RBL3, RBL4, and RBL7, we have

S20: $MU| \equiv FA \xleftrightarrow{K_{MF_0}} MU$ and Goal 9

S21: $MU| \equiv FA| \equiv FA \xleftrightarrow{K_{MF_0}} MU$. Goal 10

The above BAN logic analysis formally proves the authentication process has any two of *MU*, *FA*, and *HA* authenticate each other and the shared secrets are established as claimed.

5. Conclusions

In this paper, we propose a user anonymity-ensured mobility network authentication scheme after analyzing the previous related schemes and the weaknesses that they suffer from. In our scheme, first the parameters for negotiating the session key are verified. In the authentication and establishment of the session key phase, S_{FA_1} and S_4 are employed by *HA* and *MU* to verify a_0P, and S_3 and S_{FA_2} are employed by *HA* and *FA* to verify b_0P. In the update session key phase, h_1 and h_2 are employed by *MU* and *FA* to authenticate each other. Second, *HA* does not store *MU*'s password anymore and *MU* can change his/her password locally without connecting to *HA*. Third, the smart card authenticates *MU* before the authentication and establishment of the session key phase and password change phase. Forth, no fixed parameters are transmitted, to ensure user anonymity.

Via these new approaches, the proposed mobility network authentication scheme can defend against the weaknesses that the previous schemes suffer from. The proposed scheme is also analyzed to show that it ensures security and convenience and can be applied to mobility networks.

Acknowledgments: This work was supported in part by Ministry of Science and Technology under the Grants MOST 106-2221-E-034-006-, MOST 106-2622-H-025-001-CC3, and MOST 106-2410-H-025-006-.

Author Contributions: Ya-Fen Chang designed the algorithm, conducted all experiments, analyzed the results, wrote the manuscript, and conducted the literature review. Wei-Liang Tai conceived the algorithm, analyzed the results, and wrote the manuscript. Min-How Hsu wrote the manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Suzukiz, S.; Nakada, K. An authentication techinque based on distributed security management for the global mobility network. *IEEE J. Sel. Areas Commun.* **1997**, *15*, 1608–1617. [CrossRef]
2. Buttyan, L.; Gbaguidi, C.; Staamann, S.; Wilhelm, U. Extensions to an authentication technique proposed for the global mobility network. *IEEE Trans. Commun.* **2000**, *48*, 373–376. [CrossRef]
3. Tzeng, Z.J.; Tzeng, W.G. Authentication of mobile users in third generation mobile systems. *Wirel. Pers. Commun.* **2001**, *16*, 35–50. [CrossRef]
4. Hwang, K.F.; Chang, C.C. A self-encryption mechanism for authentication of roaming and teleconference services. *IEEE Trans. Wirel. Commun.* **2003**, *2*, 400–407. [CrossRef]
5. Zhu, J.; Ma, J. A new authentication scheme with anonymity for wireless environments. *IEEE Trans. Consum. Electron.* **2004**, *50*, 230–234.

6. Lee, C.Y.; Chang, C.C.; Lin, C.H. User authentication with anonymity for global mobility networks. In Proceedings of the 2005 IEEE Mobility Conference, the Second Asia Pacific Conference on Mobile Technology, Guangzhou, China, 15–17 November 2005; pp. 1–5.
7. Lee, C.C.; Hwang, M.S.; Liao, I.E. Security enhancement on a new authentication scheme with anonymity for wireless environments. *IEEE Trans. Ind. Electron.* **2006**, *53*, 1683–1687. [CrossRef]
8. Chang, C.C.; Lee, C.Y.; Chiu, Y.C. Enhanced authentication scheme with anonymity for roaming service in global mobility networks. *Comput. Commun.* **2009**, *32*, 611–618. [CrossRef]
9. Kuo, W.C.; Wei, H.J.; Cheng, J.C. An efficient and secure anonymous mobility network authentication scheme. *J. Inf. Secur. Appl.* **2014**, *19*, 18–24. [CrossRef]
10. Lu, Y.; Wu, X.; Yang, X. A secure anonymous authentication scheme for wireless communications using smart cards. *Int. J. Netw. Secur.* **2015**, *17*, 237–245.
11. Chang, Y.F.; Hsu, M.H.; Tai, W.L. Comments on Kuo et al.'s anonymous mobility network authentication scheme. In Proceedings of the 4th Annual Conference on Engineering and Information Technology (ACEAIT 2016), Kyoto, Japan, 29–31 March 2016; pp. 778–785.
12. Chang, Y.F.; Peng, C.H.; Tai, W.L. Comments on a secure anonymous authentication scheme for wireless communications using smart cards. In Proceedings of the International Conference on Innovation and Management (IAM2017 Winter), Tokyo, Japan, 7–10 February 2017; pp. 527–536.
13. Alizadeh, M.; Baharun, S.; Zamani, M.; Khodadadi, T.; Darvishc, M.; Gholizadeh, S.; Ahmadi, H. Anonymity and Untraceability Assessment of Authentication Protocols in Proxy Mobile IPv6. *J. Teknol.* **2015**, *72*, 31–34. [CrossRef]
14. Ibrahim, M.H.; Kumari, S.; Das, A.K.; Wazid, M.; Odelu, V. Secure Anonymous Mutual Authentication for Star Two-tier Wireless Body Area Networks. *Comput. Methods Programs. Biomed.* **2016**, *135*, 37–50. [CrossRef] [PubMed]
15. Amin, R.; Islam, S.K.H.; Biswas, G.P.; Khan, M.K.; Leng, L.; Kumar, N. Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks. *Comput. Netw.* **2016**, *101*, 42–62. [CrossRef]
16. Wang, X.; Mu, Y. Communication security and privacy support in 6LoWPAN. *Inf. Secur. Appl.* **2017**, *34*, 108–119. [CrossRef]
17. Kumari, S.; Li, X.; Wu, F.; Das, A.K.; Choo, K.R. Design of a provably secure biometrics-based multi-cloud-server authentication scheme. *Future Gener. Comput. Syst.* **2017**, *68*, 320–330. [CrossRef]
18. Tai, W.L.; Chang, Y.F.; Li, W.H. An IOT notion–based authentication and key agreement scheme ensuring user anonymity for heterogeneous ad hoc wireless sensor networks. *Inf. Secur. Appl.* **2017**, *34*, 133–141. [CrossRef]
19. Burrows, M.; Abadi, M.; Needham, R.M. A logic of authentication. *ACM Trans. Comput. Syst.* **1990**, *8*, 18–36. [CrossRef]