Wireless Pers Commun (2015) 84:2055–2078
DOI 10.1007/s11277-015-2524-x

# A Secure Authentication Scheme with User Anonymity for Roaming Service in Global Mobility Networks

**Marimuthu Karuppiah**[1] · **R. Saravanan**[2]

Published online: 28 March 2015


**Abstract** In global mobility networks, user authentication is an essential security mechanism that permits mobile users to use the roaming services offered by foreign agents with the support of home agent in mobile network environment. Recently, Rhee et al. analyzed Wu et al. and Wei et al. authentication scheme, and proposed a smart card based user authentication scheme with user anonymity in global mobility networks. However, in this paper, we find that Rhee et al. scheme is vulnerable to user impersonation attacks and off-line password guessing attacks. Moreover, the scheme does not preserve user anonymity; does not provide perfect forward secrecy, and an option to change/update the password; and does not detect wrong password quickly. Hence we propose a secure authentication scheme with user anonymity for roaming service in global mobility networks. Furthermore, performance analysis shows that compared with existing authentication schemes, our proposed scheme is simple and secure.

**Keywords** Mobile network · Authentication · Security · User anonymity · Smart card

## 1 Introduction

With the recent advancement and tremendous growth of wireless communication technology and the increasing demand for low power mobile devices, secure communication among low-power wireless communication devices is becoming important. A special network provides global roaming service that permits mobile user to use the services

✉ Marimuthu Karuppiah
marimuthume@gmail.com; k.marimuthu@vit.ac.in

R. Saravanan
rsaravanan@vit.ac.in

[1] School of Computing Science and Engineering, VIT University, Vellore 632014, India

[2] School of Information Technology and Engineering, VIT University, Vellore 632014, India

provided by his/her home agent in a foreign network, called the global mobility network [1]. When a mobile user roams into a foreign network, mutual authentication must first be solved to thwart illegal user from accessing services and to guarantee that mobile users are connected to a trusted networks. Authentication is a method for verifying the identities of remote users in global mobility network before they can access a service(see Fig. 1). Generally, there are three types of authentication methods 1. Identity authentication of something known, such as password. This is called single factor authentication. 2. Identity authentication of something possessed, such as smart cards. This is called two-factor authentication. 3. Identity authentication of some personal characteristics, such as fingerprint, voiceprint and iris scan. This is called three-factor authentication. Most early authentication schemes are only based on password. While such schemes are relatively easy to execute, passwords have several vulnerabilities [2]. Smart card based password authentication provides two-factor authentication, that is a successful login requires the user to have a legal smart card and a proper password. Three-factor authentication is very similar to smartcard based password authentication, with the only difference that it requires biometric characteristics as an additional authentication factor. However, there is a risk in using biometric factor that most people do not like to talk about, but it is important to consider. People suffer from accidents all the time. In some serious cases, these lead to disfiguration of hands, eye damage, vocal cord damage, etc. Notwithstanding these, even the implementation cost is too high. As a result, three-factor authentication is more expensive than single or two-factor authentication. Due to these concerns, the password authentication scheme using smart card is one of the simplest and most convenient authentication methods for handling secret data in global mobility network.

In general, a strong user authentication scheme in global mobility network should satisfy the following security requirements (SR): the achievement of user anonymity and untraceability$(SR_1)$; the ability to resist known-key attack$(SR_2)$; the achievement of perfect forward secrecy$(SR_3)$; the ability to resist insider attack$(SR_4)$; the ability to resist password guessing attack$(SR_5)$; the ability to resist replay attack$(SR_6)$; the ability to resist stolen-verifier attack$(SR_7)$; the ability to resist forgery attacks or impersonation attacks$(SR_8)$; the

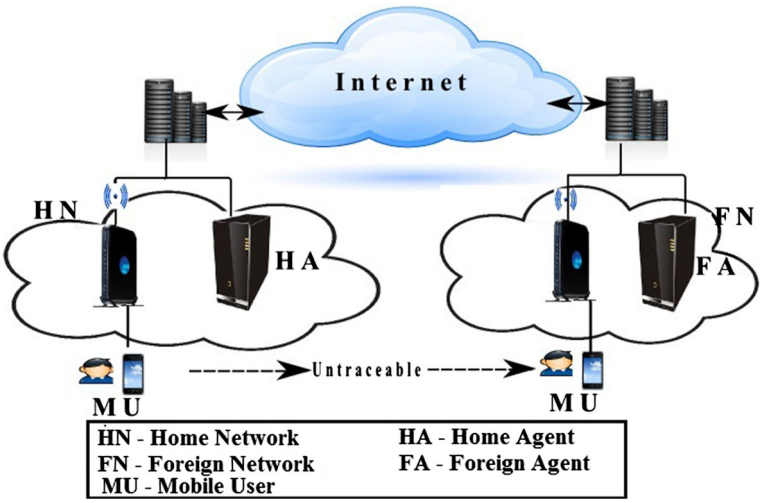


**Fig. 1** Privacy-reserving user authentication for roaming service

achievement of mutual authentication($SR_9$); the ability to resist man-in-middle attack($SR_{10}$); local password verification($SR_{11}$); user friendly($SR_{12}$). In order to achieves above listed security requirements in global mobility network, several authentication schemes using smart cards have been proposed in the past, some of which are discussed below.

In 2004, Zhu et al. [3] proposed an authentication scheme with anonymity for wireless environments. However, Lee et al. [4] pointed out that this scheme cannot achieve mutual authentication and perfect backward secrecy, and is vulnerable to forgery attack. The authors further proposed an enhanced anonymous authentication scheme in 2006. Additionally, Wei et al. [5] also proved that Zhu et al.'s scheme does not satisfy user anonymity, and proposed an improved scheme. Subsequently, Wu et al. [6] analyzed Lee et al.'s scheme and proved that it cannot achieve user anonymity, backward secrecy in 2008. Moreover, Wu et al. proposed a secure authentication scheme with anonymity for wireless communication and claimed their scheme achieves both user anonymity and backward secrecy, but Xu et al. [7] and Lee et al. [8] demonstrated that Wu et al.'s scheme fails to provide user anonymity. Wang et al. [9] also established the same, and thereafter proposed an enhanced scheme. Be that as it may, Jeon et al. [10] showed that Wang et al.'s scheme is vulnerable to a malicious attacker and does not provide user anonymity.

In 2009, Chang et al. [11] remonstrated Lee et al.'s scheme cannot provide user anonymity under the forgery attack and then proposed an enhanced authentication scheme. Nevertheless, Youn et al. [12] exhibited that Chang et al.'s scheme cannot achieve user anonymity and cannot resist a known session key attack. Zeng et al. [13] too remarked that Zhu et al.'s scheme [3], Lee et al.'s scheme [4] and Wu et al.'s scheme [6] cannot achieve user anonymity. In 2010, He et al. [14] found Wu et al.'s scheme [6] does not provide user anonymity and furthermore is vulnerable to replay and impersonation attack. They then proposed a strong user authentication scheme with smart cards for wireless communications.

In 2011, Li et al. [15] found that He et al.'s scheme [14] lacks user friendliness, and cannot provide user anonymity and fairness in key agreement. Thus, Li et al. [15] proposed a new authentication scheme with user anonymity for wireless communications. However, in 2013, Jeon et al. [16] demonstrated that Li et al.'s scheme is inefficient due to computational overhead and does not provide session key update. Subsequently, they proposed an efficient user authentication scheme with smart cards for wireless communications. Thereafter, Das [17] also showed that Li et al.'s [15] scheme fails to update the user's password appropriately in the password change phase and cannot withstand replay attack. Additionally, Das proposed an improved scheme, but Wen et al. [18] pointed out that Das's scheme is insecure against impersonation attack and then they too proposed an improved scheme. In the same year, Xu et al. [19] reanalyzed Lee et al.'s scheme [4] and proved that it cannot achieve user anonymity, and proposed then a new authentication scheme to achieve user anonymity. Rhee et al. [20] analyzed Wu et al.'s scheme [6] and Wei et al.'s scheme [5] and presented that Wu et al.'s scheme fails to preserves user anonymity, and that Wei et al.'s scheme [5] allows the user to login without smart card. Furthermore, Rhee et al. proposed an improved authentication scheme and claimed their scheme achieves user anonymity and restricts user login without smart card. However, Xiong et al. [21] showcased that Rhee et al.'s scheme does not achieve user anonymity and then proposed an enhanced scheme. Later on, He et al. [22] and Yoon et al. [23] also proposed new schemes and they claimed their schemes achieves all the security requirements.

In 2012, Niu and Li [24] showed that Yoon et al.'s scheme [23] cannot achieve user anonymity and unfairness in key agreement, and then they proposed a novel user

authentication scheme with user anonymity. Chun [25] also proved that Yoon et al.'s scheme [23] can not resist insider attack and achieve user anonymity, and then the author proposed an improved scheme. Subsequently, Mun et al. [26] reanalyzed Wu et al.'s scheme [6], and remonstrated that Wu et al.'s scheme also fails to achieve user anonymity, perfect forward secrecy, and discloses legitimate user's password. Further, they proposed an improved anonymous authentication scheme. However, Kim et al. [27] presented that Mun et al.'s scheme is vulnerable to replay and man-in-the middle attack and then they proposed an improved scheme.

In 2013, Jiang et al. [28] analyzed He et al.'s scheme [22], and pointed out that He et al.'s scheme suffers from privileged insider attack, domino effect, session key and replay attack, fails to achieve strong two-factor security, and there is no password change option. Then they proposed an improved scheme to enhance the security strength of He et al.'s scheme. However, Wen et al. [29] exhibited that Jiang et al.'s scheme [28] is vulnerable to replay, stolen-verifier and denial of service attack, and moreover proposed an improved scheme to withstand security flaws of Jiang et al.'s scheme. Later on, Li et al. [30], Xie et al. [31] and Xu et al. [32] also proposed new authentication schemes and they claimed their schemes achieve all the security requirements.

Recently (2014), Zhao et al. [33] found Mun et al.'s scheme [26] vulnerable to insider, off-line password guessing, impersonation attacks, and it cannot achieve user anonymity, user friendliness, local verification and proper mutual authentication. Subsequently they proposed a new authentication scheme to overcome the security flaws of Mun et al.'s scheme. Later on, Hu et al. [34] reanalyzed Li et al.'s scheme [15], and figured out that it is vulnerable to off-line password guessing attack. To remedy this security flaw, they proposed an improved scheme. Kuo et al. [35] too proposed an efficient and secure authentication scheme for wireless network and claimed their scheme to be competent to increase efficiency and improve security. Most recently, Ding et al. [36] showed that Li et al.'s scheme [30] cannot provide user anonymity and is vulnerable to off-line password guessing attacks. Furthermore, Ding et al. presented an enhanced scheme to overcome the defects of Li et al.'s scheme. Later on, Zhou et al. [37], Jiang et al. [38] and He et al. [39] also proposed new authentication schemes and they claimed their schemes achieve all the security requirements.

However, in this paper, we present a brief review of Rhee et al.'s scheme [20] and demonstrate the vulnerability of their scheme to off-line password guessing attack, user impersonation attack. Besides, the scheme fails to provide user anonymity, perfect forward secrecy and an option to change/update the password. Moreover, we find that Rhee et al.'s scheme cannot detect incorrect password in login phase immediately-it is detected by the home agent($HA$) only in the authentication phase. Due to that, unnecessary communication and computation is incurred. We also propose a new authentication scheme with user anonymity for roaming service in global mobility, which is secure and achieves forward secrecy. In our scheme, a mobile user can freely change his/her password of the smartcard without the help of the home agent. We demonstrate that the proposed scheme can withstand off-line password guessing attack and user impersonation attack. Also, our proposed scheme can detect an incorrect password in login phase immediately. We also show that our proposed scheme is well suitable for mobile environments, and manifest the advantages of our scheme as compared to the related schemes [14, 20, 23, 28, 30].

The rest of the paper is organized as follows. In Sect. 2, we briefly introduce the discrete logarithm problem, the one-way hash function, and the Diffie–Hellman problem; these mathematical concepts form the basis of the security of our proposed scheme. In Sect. 3, we review Rhee et al.'s scheme. Section 4 describes the weakness of Rhee et al.'s scheme.

Our proposed scheme and corresponding scheme analysis are presented in Sects. 5 and 6, respectively. The performance analysis and security requirement comparisons are presented in Sect. 7. We lastly present our conclusions in Sect. 8.

## 2 Preliminaries

In this section, we provide brief introductions to the discrete logarithm problem [40], the one-way hash function (e.g., MD5 [41] or SHA-1 [42], and the Diffie-Hellman problem [43]; these mathematical concepts form the basis of the security of our proposed scheme.

### 2.1 Discrete Logarithm Problem and Diffie–Hellman Problem

Until now, the discrete logarithm problem has been intractable. Detailed information about the discrete logarithm problem can be found in [40], and we briefly introduce the discrete logarithm problem in the following text. Assume that $g$ is a generator of $Z_p^*$ and that $p$ is a large prime number. Consider the following equation:

$$X = g^x mod\, p \tag{1}$$

If we know $g$, $x$ and $p$, computing the modular exponentiation $X = g^x mod p$ is trivial. However, if we know $g$, $X$, and $p$, it is computationally infeasible to find $x$ due to the factoring of prime numbers [44]. The problem of solving equation (1) for $x$ is called the discrete logarithm problem. Furthermore, given $g$, $p$, $X = g^x mod\, p$, and $Y = g^y mod\, p$, the computation of $K = g^{xy} mod\, p$ is termed the Diffie–Hellman problem [43].

### 2.2 One-Way Hash Function

A one-way hash function $h : x \rightarrow y$ is a function with the following properties:

- The function $h(\cdot)$ takes message of variable length as the input and converts it into the output of a fixed-length message digest.
- The function $h(\cdot)$ is one-way in the sense that, given $x$, it is trivial to compute $h(x) = y$. However, given $y$, it is difficult to compute $h^{-1}(y) = x$.

## 3 Review of Rhee et al.'s Scheme

In this section, we review Rhee et al.'s authentication scheme [20]. It comprises of three phases: registration phase, login phase, and authentication phase. The notations used in Rhee et al.'s scheme are defined in Table 1. Rhee et al. consider the scenario where a mobile user $U_i$, associated with its home agent $HA$, is visiting a foreign network with foreign agent $FA$. They assume that $N$ is a secret key which is held only by $HA$. The detailed steps of these phases are revealed as follows.

### 3.1 Registration Phase

In this phase, whenever a mobile user $U_i$ enrolls in his/her home agent $HA$, $U_i$ chooses his/her identity $ID_U$ and sends $ID_U$ to $HA$. After receiving identity $ID_U$ of a mobile user $U_i$, the

**Table 1** The notations used in Rhee et al.'s scheme

| Notations | Descriptions |
|---|---|
| $U_i$ | $i$th mobile user |
| $PWD_U$ | Password of $U_i$ |
| $ID_U$ | Identity of $U_i$ |
| $HA$,$FA$ | Home agent, Foriegn agent |
| $(X)_K$ | Encryption of a message $X$ using a symmetric key $K$ |
| $E_{PA}(X)$ | Encryption of a message $X$ using a public key $P_A$ |
| $S_{SA}(X)$ | Signature on a message $X$ using a secret key $S_A$ |
| $N$ | Secret key of $HA$ |
| $Cert_A$ | Certificate of an entity $A$ |
| $h(\cdot)$ | Cryptographic one-way hash function |
| $T_A$ | Timestamp generated by an entity $A$ |
| $\|\|$ | Concatanation |
| $\oplus$ | Bitwise $XOR$ operation |

home agent $HA$ generates $PWD_U$, $r_1$ and $r_2$, and stores $ID_{HA}$, $r_1$, $r_2$ and a one-way hash function $h(\cdot)$ in the smart card of $U_i$.

$$\begin{aligned} PWD_U &= h(N||ID_U) \\ r_1 &= h(N||ID_{HA}) \\ r_2 &= h(N||ID_U) \oplus ID_{HA} \oplus ID_U \end{aligned}$$

where $N$ is a secret key kept by $HA$. $HA$ then sends $PWD_U$ and a smart card containing $ID_{HA}$, $r_1$, $r_2$ and $h(\cdot)$ to $U_i$ via a secure communication channel.

### 3.2 Login Phase and Authentication Phase

A foreign agent $FA$ authenticates mobile user $U_i$ by interacting with home agent $HA$ as follows.

**Step 1:** $U_i \rightarrow FA : \{n, (h(ID_U)||x_0||x)_L, ID_{HA}, T_U\}$

1. If $U_i$ keys $PWD_U$ to $U_i$'s mobile device, then $U_i$'s mobile device selects secret random values $x_0$ and $x$ and computes $n$ and $L$ as follows.

$$\begin{aligned} n &= h(T_U||r_1) \oplus r_2 \oplus PWD_U \\ L &= h(T_U||PWD_U) \end{aligned}$$

2. $U_i$'s mobile device sends login request message $\{n, (h(ID_U)||x_0||x)_L, ID_{HA}, T_U\}$ to foreign agent $FA$, where $T_U$ is a current timestamp.

**Step 2:** $FA \rightarrow HA : \{n, (h(ID_U)||x_0||x)_L, T_U, S_{S_{FA}}((h(ID_U)||x_0||x)_L, T_U, Cert_{FA}), Cert_{FA}, T_F\}$

3. When $FA$ receives the message at time $T_F$, it verifies the validity of $T_U$. On successful verification, $FA$ selects a random number $b$ and sends the message $\{n, (h(ID_U)||x_0||x)_L, T_U, S_{S_{FA}}((h(ID_U)||x_0||x)_L, T_U, Cert_{FA}), Cert_{FA}, T_F\}$ to home agent $HA$, where $T_F$ is a current timestamp, $S_{FA}$ is a $FA$'s private key and $Cert_{FA}$ is a certificate of $FA$.

**Step 3:** $HA \rightarrow FA : \{c, W, b, S_{S_{HA}}(h(b, c, W, Cert_{HA})), Cert_{HA}, T_H\}$

4. When $HA$ receives the message, it verifies the validity of certificate $Cert_{FA}$ and timestamp $T_F$. If both conditions hold, then $HA$ computes mobile user's identity as

$$\begin{aligned} ID_U &= h(T_U||h(N||ID_{HA})) \oplus n \oplus ID_{HA} \\ &= h(T_U||h(N||ID_{HA})) \oplus h(T_U||r_1) \oplus r_2 \oplus PWD_U \oplus ID_{HA} \\ &= \cancel{h(T_U||h(N||ID_{HA}))} \oplus \cancel{h(T_U||h(N||ID_{HA}))} \oplus r_2 \oplus PWD_U \oplus ID_{HA} \\ &= r_2 \oplus PWD_U \oplus ID_{HA} \\ &= h(N||ID_U) \oplus ID_{HA} \oplus ID_U \oplus PWD_U \oplus ID_{HA} \\ &= \cancel{PWD_U} \oplus \cancel{ID_{HA}} \oplus ID_U \oplus \cancel{PWD_U} \oplus \cancel{ID_{HA}} \\ &= ID_U \end{aligned}$$

Then, it computes $L = h(T_U||h(N||ID_U)$ and decrypts $(h(ID_U)||x_0||x)_L$.

5. $HA$ verifying if $h(ID_U) = h(ID_U^*)$. If verification holds, then HA computes $W = E_{P_F}(h(h(N||ID_U))||x_0||x)$ and generates its signature $S_{S_{HA}}(h(b, c, W, Cert_{HA}))$ using its private key $S_{HA}$. Then, $HA$ sends a message $\{c, W, b, S_{S_{HA}}(h(b, c, W, Cert_{HA})), Cert_{HA}, T_H\}$ to $FA$ where $T_H$ is current timestamp, $Cert_{HA}$ is certificate of $HA$ and $c$ is a random number.

**Step 4:** $FA \rightarrow U_i : \{(TCert_U||h(x_0||x))_k\}$

6. When $FA$ receives the message, it verifies the validity of certificate $Cert_{HA}$ and timestamp $T_H$. If both conditions hold, then $FA$ issues temporary certificate $TCert_U$, which includes a timestamp and other information, to mobile user $U_i$.
7. To attain $(h(h(N||ID_U))||x_0||x)$, $FA$ decrypts $W$ with the secret key corresponding to $P_{FA}$. To establish session key $k_i$ for the $i$th session, $FA$ saves $(TCert_U, h(PWD_U), x_0)$. $FA$ encrypts $(TCert_U||h(x_0||x))_k$ with session key $k = h(h(h(N||ID_U))||x_0||x)$ and sends $(TCert_U||h(x_0||x))_k$ to $U_i$.
8. $U_i$ can compute session key $k = h(h(PWD_U)||x_0||x)$ and obtain $TCert_U$ by decrypting the message $(TCert_U||h(x_0||x))_k$ using $k$. And mobile user $U_i$ can authenticate foreign agent $FA$ by verifying whether computed $h(x_0||x)$ is equal to decrypted $h(x_0||x)$. Therefore, mobile user $U_i$ can be sure that it is communicating with a legal $FA$.

## 4 Cryptanalysis of Rhee et al.'s Scheme

Rhee et al. [20] proposed a simple authentication scheme, based on the public-key cryptosystem, through which mobile users simply perform symmetric encryption and decryption. However, Xiong et al. [21] showed that the scheme of Rhee et al.'s fails to preserve user anonymity due to an inherent design weakness. In this section, we will show that Rhee et al.'s scheme is also vulnerable to other attacks. Before analyzing Rhee et al.'s scheme, we make the following three assumptions regarding capability of an adversary $\mathscr{A}$ as suggested by Xu et al. [45], Kocher et al. [46], Messerges et al. [47] and Ding et al. [48] respectively. Note that these three assumptions, which are also made in the most recent works [36, 48–56] and [57] are quite reasonable.

1. The adversary $\mathscr{A}$ has total control over the communication channel between the users and the remote server. That is, $\mathscr{A}$ may eavesdrop, block, insert, delete, modify, or intercept any messages transmitted in the channel [45].

2. $\mathscr{A}$ may either steal a user's smart card or pick up the user's smart card for short time period, and then extract the secret values stored in the smart card by side-channel attack techniques [46, 47, 58]
3. The adversary $\mathscr{A}$ can off-line enumerate the password dictionary space [54].

Following above mentioned assumptions, in the subsequent discussions of the security weakness of the scheme of Rhee et al., we assume that an adversary $\mathscr{A}$ can extract the security parameters $\{ID_{HA}, r_1, r_2, h(\cdot)\}$ stored in the legal user's smart card and that the adversary $\mathscr{A}$ can also intercept the login request message $\{n, (h(ID_U)||x_0||x)_L, ID_{HA}, T_U\}$ sent out by the mobile user $U_i$ and all other messages transferred between home agent *HA* and foreign agent *FA*. Now, we highlight various security loopholes existing in Rhee et al.'s scheme:

### 4.1 Absence of User Anonymity

Assume that an adversary $\mathscr{A}$ has registered as a valid user of home agent *HA*, then he/she can find the identity of other users as long as they are registered at the same home agent *HA*. Note that an adversary $\mathscr{A}$ can derive $PWD_A, ID_{HA}, r_1, r_2$ and $h(\cdot)$ from the home agent *HA* (see Sect. 3.1), where

$$\begin{aligned} PWD_A &= h(N||ID_A) \\ r_1 &= h(N||ID_{HA}) \\ r_2 &= h(N||ID_A) \oplus ID_{HA} \oplus ID_A = PWD_A \oplus ID_{HA} \oplus ID_A \end{aligned}$$

Let $U_i$ be a mobile user who is registered at the same home agent *HA* and is executing the first phase with a foreign agent *FA*. It is clear that $\mathscr{A}$ can intercept the messages $\{n, (h(ID_U)||x_0||x)_L, ID_{HA}, T_U\}$ from Step 1 in authentication phase because broadcast is wireless and anyone within range of a wireless device can intercept the packets being sent out without interrupting the data flow [3]. Later, an adversary $\mathscr{A}$ can confirm that $U_i$ is a legal user of home agent *HA* based on $ID_{HA}$. Then, $\mathscr{A}$ can compute $h(T_U||r_1)$ using intercepted $T_U$ and find out the original identity of $U_i$ as home agent *HA* does at Step 3 in authentication phase. That is,

$$\begin{aligned} n \oplus ID_{HA} \oplus h(T_U||r_1) &= \cancel{h(T_U||r_1)} \oplus r_2 \oplus PWD_U \oplus ID_{HA} \oplus \cancel{h(T_U||r_1)} \\ &= r_2 \oplus PWD_U \oplus ID_{HA} \\ &= h(N||ID_U) \oplus \cancel{ID_{HA}} \oplus ID_U \oplus PWD_U \oplus \cancel{ID_{HA}} \\ &= \cancel{PWD_U} \oplus ID_U \oplus \cancel{PWD_U} \\ &= ID_U \end{aligned}$$

The above attack demonstrates that it is trivial for an adversary $\mathscr{A}$ to find the identity of mobile users and defeat the anonymity claimed by Rhee et al.'s scheme. The reason this attack is successful is that home agent *HA* computes $r_1$ for each mobile user with the same secret key $N$.

### 4.2 No Password Change Option

An ideal user authentication scheme allows the user to change his/her password freely and it can be completed without assistance from the server to ensure user friendliness and the efficiency. When the user's password is expired or disclosed, mobile user may desire to change $PWD_U$ for maintaining security. Nevertheless, it is a widely suggested security policy for highly secure applications that user's password should be updated or changed

regularly. Conversely, in Rhee et al.'s scheme, in order to change/update the password, there is no provision. Therefore, Rhee et al.'s scheme is not user friendly.

### 4.3 Vulnerable to Off-Line Password Guessing Attack

In password authentication schemes where the user is permitted to choose his/her password, the user tends to choose a password that can be easily remembered for his/her convenience. However, these easy-to-remember passwords are potentially vulnerable to password guessing attack, in which an adversary can try to guess the user's password and then verify his guess. Password guessing attacks include online and off-line password guessing attacks. Online password guessing attacks can easily be thwarted by limiting the number of failed logins and limiting the number of continuous login attempts that can occur within a short time interval. However, in off-line password guessing attack, the adversary $\mathscr{A}$ intercepts some password related messages transmitted between the user and the server, and then iteratively guesses the users password and verifies whether his/her guess is correct or not in an off-line manner. The main defect of Rhee et al.'s is that, in the login phase, a mobile user $U_i$ has to input a long and random password $PWD_U$ because password $PWD_U = h(N||ID_U)$ is computed by home agent $HA$. We wonder how any common user will be able to remember such a lengthy password. If $PWD_U$ is a long string, the Rhee et al.'s scheme is hardly usable; If $PWD_U$ is a short string, then an adversary $\mathscr{A}$ can easily off-line guess password $PWD_U$. Suppose the user's smart card is lost, an adversary $\mathscr{A}$ can retrieve all the data $\{ID_{HA}, r_1, r_2, h(\cdot)\}$ under Assumption 2. Moreover, adversary $\mathscr{A}$ can achieve user's identity $ID_U$ as discussed in Sect. 4.1. Further, with the previously intercepted login request message $\{n, (h(ID_U)||x_0||x)_L, ID_{HA}, T_U\ \}$ from the public channel, $\mathscr{A}$ can obtain $U_i$'s password $PWD_U$ as follows:

$$\begin{aligned} r_2 \oplus ID_{HA} \oplus ID_U &= h(N||ID_U) \oplus ID_{HA} \oplus ID_U \oplus ID_{HA} \oplus ID_U \\ &= h(N||ID_U) \\ &= PWD_U \end{aligned}$$

Therefore, Rhee et al.'s scheme is vulnerable to off-line password guessing attacks.

### 4.4 Vulnerable to User Impersonation Attack (Spoofing Attack)

An adversary $\mathscr{A}$ can impersonate a legal mobile user by successfully logging in without a smart card, and spoof the foreign agent and home agent $HA$ as follows:

1. The adversary $\mathscr{A}$ achieves user's identity $ID_U$ as discussed in Sect. 4.1.
2. The adversary $\mathscr{A}$ achieves user's password $PWD_U$ as discussed in Sect. 4.3.
3. The adversary $\mathscr{A}$ chooses a random number $x'$ and $x_0'$, and compute following values:

$$\begin{aligned} r_2 &= PWD_U \oplus ID_{HA} \oplus ID_U = h(N||ID_U) \oplus ID_{HA} \oplus ID_U \\ n &= h(T_A||r_1) \oplus r_2 \oplus PWD_U \\ L &= h(T_A||PWD_U) \end{aligned}$$

   Then, $\mathscr{A}$ sends the login request message $\{n,(h(ID_U)||x_0'||x')_L, ID_{HA},T_A\}$ to foreign agent $FA$ where $T_A$ is the current timestamp of adversary $\mathscr{A}$.
4. After that, the foreign agent $FA$ and home agent $HA$ precede the subsequent Steps 2–4 of authentication phase successfully because the login request message

$\{n, (h(ID_U)||x_0^{'}||x^{'})_L, ID_{HA}, T_A\}$ sent by an adversary $\mathscr{A}$ is valid. Finally, foreign agent $FA$ sends the message $(TCert_U||h(x_0^{'}||x^{'}))_k$ to mobile user $U_i$, where $k = h(h(h(N||ID_U))||x_0^{'}||x^{'})$ is a session key. The adversary $\mathscr{A}$ can intercept this message and he/she can compute session key $k = h(h(PWD_U)||x_0^{'}||x^{'})$ and obtain $TCert_U$ by decrypting the message $(TCert_U||h(x_0^{'}||x^{'}))_k$ using $k$. An adversary $\mathscr{A}$ can authenticate a foreign agent $FA$ by verifying computed $h(x_0^{'}||x^{'})$ is equal to decrypted $h(x_0^{'}||x^{'})$.

The above discussion shows that an adversary $\mathscr{A}$ can pass the verification of the home agent $HA$ and establish the session key $k$. Therefore Rhee et al.'s scheme is vulnerable to user impersonation attack/spoofing attack.

### 4.5 Wrong Password Cannot be Quickly Detected: Local Password Verification

In the login phase of Rhee et al.'s scheme, the mobile user $U_i$ inputs his/her identity $ID_U$ and password $PWD_U$; however the smart card does not verify the legality of user's password $PWD_U$ and identity $ID_U$. Therefore, even if the user $U_i$ incorrectly inputs his/her password $PWD_U$ or identity $ID_i$ or both by mistake, Steps 1–4 of authentication phase are still performed. It shows the inefficiency of scheme in incorrect input detection. This leads to unnecessarily extra communication and computational overheads during the login and authentication phases. If $T_{hash}$, $T_{xor}$ and $T_{e/d}$ denote the running time for a hash function, $XOR$ operation and encryption/decryption, respectively, then the computational overheads are $7T_{hash} + 4T_{xor} + 2T_{e/d}$.

### 4.6 Absence of Perfect Forward Secrecy

Forward secrecy guarantees that the session key remains unbroken even after the disclosure of systems secret key. However, Rhee et al.'s scheme is failing to provide perfect forward secrecy is as follows.

1. $\mathscr{A}$ achieves user's password $PWD_U$ as discussed in Sect. 4.3.
2. $\mathscr{A}$ can intercept the message $\{n, (h(ID_U)||x_0||x)_L, ID_{HA}, T_U\}$.
3. $\mathscr{A}$ can compute $L = h(T_U||PWD_U) = h(T_U||h(N||ID_U))$ and decrypts $(h(ID_U)||x_0||x)_L$ by using $L$. As a result, $\mathscr{A}$ can find $x_0$, $x$ and $h(ID_U)$.
4. $\mathscr{A}$ can compute first session key $k_1 = h(h(PWD_U)||x_0||x)$ by using $x_0$, $x$ and $PWD_U$.
5. $\mathscr{A}$ can intercept $\{ TCert_U,(x_1||TCert_U||OtherInfo)_{k_1} \}$ at first session and decrypt it by using $k_1$. As a result, $\mathscr{A}$ can obtain $x_1$.
6. $\mathscr{A}$ can compute second session key $k_2 = h(h(PWD_U)||x_1||x)$ by using $x_1$, $x$ and $PWD_U$. $\mathscr{A}$ can guess further $i$th session key by using this attack method.

Therefore, Rhee et al.'s scheme does not provide perfect forward secrecy.

## 5 Proposed Scheme

In this section, we propose a secure authentication scheme with user anonymity for roaming service in global mobility networks. Our scheme is divided into five phases: the initialisation phase, the registration phase, the login phase, the authentication phase, and the password change phase. Table 2 lists some notations used in our proposed scheme. We

consider the scenario where a mobile user *MU*, associated with its home agent *HA*, is visiting a foreign network with foreign agent *FA*. We assume that $d$ is a secret key, and $y$ is a public key, which are held only by *HA*. It is assumed that before the system starts, each pair of *FA* and *HA* shares a long-term common secret key $K_{FH}$ using any key agreement method, such as the Diffie–Hellman key agreement protocol [43]. The detailed steps of these phases are revealed as follows

### 5.1 Initialisation Phase

The home agent *HA* performs smart card issue operations whenever a new mobile user *MU* registers through the registration phase.The detailed steps of this phase are revealed as follows. Initially, *HA* selects two large prime number $p$; $q$ and generator $g$ of a finite field in $Z_p^*$. It computes $n = p \times q$ and $\phi(n) = (p-1) \times (q-1)$. Next, it selects an integer $e$ such that $gcd(e, \phi(n)) = 1$ and $1 < e < \phi(n)$. Since $gcd(e, \phi(n)) = 1$, the inverse of $e$ in the finite group integer modulo $\phi(n)$ exists. It computes an integer $d$ such that $d \equiv e^{-1} mod\ \phi(n)$, where $d$ is the secret key(private key) of *HA*, and $y = g^d mod\, n$; $y$ is the public key. *HA* keeps $(d, p, q)$ secretly.

### 5.2 Registration Phase

The detailed steps of this phase are revealed as follows

1. The mobile user *MU* freely selects his/her identity $ID_{mu}$, password $PWD_{mu}$, and a random number $b$, which is used to protect $PWD_{mu}$. Then, he/she sends the registration request message $M = \{ID_{mu}, (b \oplus PWD_{mu})\}$ to the *HA* through a secure channel.
2. After receiving the registration request message $M$, *HA* computes

**Table 2** Notations used in our proposed scheme

| Notations | Descriptions |
|---|---|
| $MU, FA, HA$ | Mobile user, Foriegn agent, home agent |
| $PWD_{mu}$ | Password of *MU* |
| $ID_{mu}, ID_{FA}, ID_{HA}$ | Identity of *MU*, Identity of *FA*, Identity of *HA* |
| $p, q, n$ | $p$ and $q$ are two larger prime numbers, and $n = p \times q$ |
| $d$ | Secret key of *HA* |
| $y$ | Public key of *HA* |
| $(X)_K$ | Encryption/decryption of a message $X$ using a symmetric key $K$ |
| $Sess_{key}$ | Session key between *MU* and *FA* |
| $K_{FH}$ | Pre-shared secret key between *FA* and *HA* |
| $x, r_f, X_{mu}$ | Random number generated by *MU*, *FA* and *HA* |
| $h(\cdot)$ | Cryptographic one-way hash function |
| $T_A$ | Timestamp generated by an entity $A$ |
| $\Delta T_A$ | Expected legal time interval for the transmission delay |
| $\|\|$ | Concatanation |
| $\oplus$ | Bitwise *XOR* operation |

$$C_i = h(h(ID_{mu}) \oplus h(b \oplus PWD_{mu}))mod\, n$$
$$K_{mu} = h(ID_{mu}||ID_{HA}||X_{mu}||T_R) \oplus h(b \oplus PWD_{mu})$$

where $T_R$ is registration time of the mobile user $MU$ and $X_{mu}$ is a random number chosen by $HA$ corresponding to each user to make sure $K_{mu}$ is unique for each user. $HA$ creates an entry for mobile user $MU$ in its database and stores an encrypted form of $\{ID_{mu}, X_{mu}, T_R\}$ in this entry. Then, $HA$ personalizes the smart card with $\{C_i, g, y, n, ID_{HA}, K_{mu}, h(\cdot)\}$ and issues it to $MU$.

3. After receiving the smart card, $MU$ enters his/her random number $b$ into his smart card. Finally, the smart card contains $\{C_i, g, y, n, ID_{HA}, K_{mu}, b, h(\cdot)\}$.

### 5.3 Login and Authentication Phase

The detailed steps of this phase are revealed as follows and also in Fig. 2. We assume that the mobile user roams into a foreign network administrated by a foreign agent $FA$ and tries to access services, the foreign agent $FA$ needs to authenticate the mobile user $MU$ through home agent $HA$.

**Step 1:** $MU \rightarrow FA{:}M_1 = \{B_1, SID, V_1, ID_{HA}, T_{mu}\}$

1. Mobile user $MU$ inserts his/her smart card into a card reader and enters his/her identity $ID^*_{mu}$ and password $PWD^*_{mu}$. Then, smart card computes $C^*_i = h(h(ID^*_{mu}) \oplus h(b \oplus PWD^*_{mu}))mod\, n$ and verifies whether $C^*_i = C_i$ or not. If verification holds, then legality of $ID^*_{mu}$ and $PWD^*_{mu}$ is ensured. Otherwise, the session is terminated.
2. The smart card selects a random number $x$ and computes

$$B_1 = g^x mod\, n$$
$$B_2 = y^x mod\, n$$
$$SID = (ID_{mu}||B_1)_{B_2} \oplus h(B_1 \oplus B_2)$$
$$K = K_{mu} \oplus h(b \oplus PWD_{mu}) = h(ID_{mu}||ID_{HA}||X_{mu}||T_R)$$
$$V_1 = h(K||B_2||SID||T_{mu})$$

where the $T_{mu}$ is current timestamp value observed from card reader's clock. Finally mobile user $MU$ sends login request message $M_1 = \{B_1, SID, V_1, ID_{HA}, T_{mu}\}$ to the foreign agent $FA$.

**Step 2:** $FA \rightarrow HA : M_2 = \{W_1, ID_{FA}, r_f, T_F, B_1, SID, V_1, T_{mu}\}$

3. Upon receiving $M_1, FA$ verifies the freshness of $T_{mu}$ by comparing $T_F - T_{mu} \leq \Delta T_1$, where $T_F$ is the current timestamp of $FA$ and $\Delta T_1$ is the expected legal time interval for the transmission delay between $MU$ and $FA$. If the comparison fails, $FA$ rejects the login request message $M_1$.
4. $FA$ generates a random number $r_f$ and computes

$$W_1 = h(K_{FH}||ID_{FA}||r_f||T_F||B_1||V_1||SID)$$

where $K_{FH}$ is the pre-shared secret key between $FA$ and $HA$. Then, $FA$ sends the message $M_2 = \{W_1, ID_{FA}, r_f, T_F, B_1, SID, V_1, T_{mu}\}$ to $HA$.

**Step 3:** $FA \rightarrow HA$: $M_3 = \{K_1, V_2, S_2, T'_H\}$

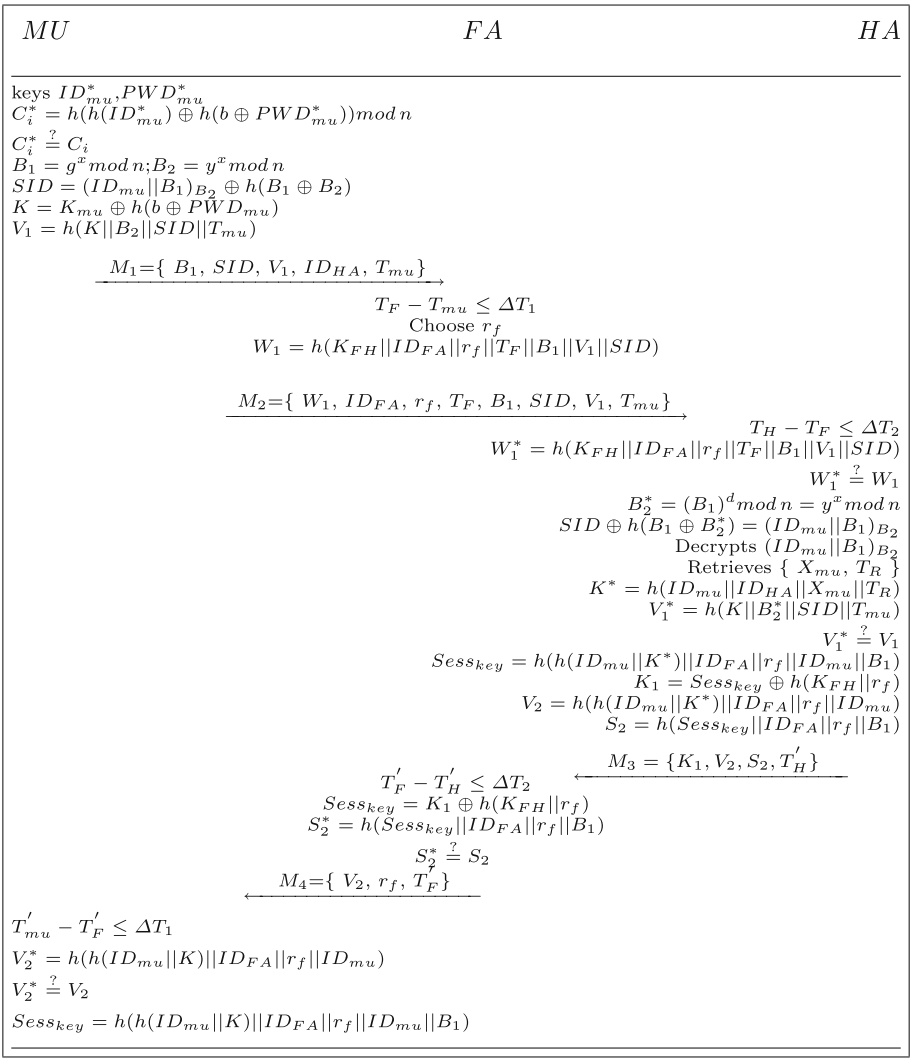


**Fig. 2** Scene of the proposed scheme

5. Upon receiving $M_2$, *HA* verifies the freshness of $T_F$ by comparing $T_H - T_F \leq \Delta T_2$, where $T_H$ is the current timestamp of *HA* and $\Delta T_2$ is the expected legal time interval for the transmission delay between *FA* and *HA*. If the comparison fails, *HA* rejects message $M_2$.
6. *HA* retrieves $K_{FH}$ according to $ID_{FA}$ and computes

$$W^*_1 = h(K_{FH}||ID_{FA}||r_f||T_F||B_1||V_1||SID).$$

Then, it verifies whether $W^*_1 = W_1$ or not. If the verification holds, *HA* ensures the legality of the foreign agent *FA*. Otherwise, *HA* terminates the session.

7. *HA* computes $B_2^* = (B_1)^d mod\, n = y^x mod\, n$ and derives

$$SID \oplus h(B_1 \oplus B_2^*) = (ID_{mu}||B_1)_{B_2} \oplus \cancel{h(B_1 \oplus B_2)} \oplus \cancel{h(B_1 \oplus B_2^*)}$$
$$= (ID_{mu}||B_1)_{B_2}$$

Then, *HA* decrypts $(ID_{mu}||B_1)_{B_2}$ using $B_2^*$ to disclose $ID_{mu}$. Then, *HA* retrieves $\{X_{mu}, T_R\}$ according to $ID_{mu}$ from its database. It computes $K^* = h(ID_{mu}||ID_{HA}||X_{mu}||T_R)$ and $V_1^* = h(K||B_2^*||SID||T_{mu})$, and check whether $V_1^* = V_1$ or not. If true, the authenticity of mobile user *MU* is ensured. Otherwise, the *HA* terminates the session.

8. HA computes the follwing

$$Sess_{key} = h(h(ID_{mu}||K^*)||ID_{FA}||r_f||ID_{mu}||B_1)$$
$$K_1 = Sess_{key} \oplus h(K_{FH}||r_f)$$
$$V_2 = h(h(ID_{mu}||K^*)||ID_{FA}||r_f||ID_{mu})$$
$$S_2 = h(Sess_{key}||ID_{FA}||r_f||B_1)$$

and sends message $M_3 = \{K_1, V_2, S_2, T_H^{'}\}$ to *FA*

**Step 4:** $FA \rightarrow MU$: $M_4 = \{V_2, r_f, T_F^{'}\}$

9. Upon receiving $M_3$, *FA* verifies the freshness of $T_H^{'}$ by comparing $T_F^{'} - T_H^{'} \leq \Delta T_2$, where $T_F^{'}$ is the current timestamp of *FA* and $\Delta T_2$ is the expected legal time interval for the transmission delay between *FA* and *HA*. If the comparison fails, *FA* rejects message $M_3$.
10. Then, FA computes

$$Sess_{key} = K_1 \oplus h(K_{FH}||r_f)$$
$$= h(h(ID_{mu}||K^*)||ID_{FA}||r_f||ID_{mu}||B_1)$$
$$S_2^* = h(Sess_{key}||ID_{FA}||r_f||B_1)$$

Then, *FA* verifies whether $S_2^* = S_2$ or not. If the verification holds, *FA* ensures the legality of the home agent *HA* and sends the message $M_4 = \{V_2, r_f, T_F^{'}\}$ to *MU*.

11. Upon receiving $M_4$, *MU* verifies the freshness of $T_F^{'}$ by comparing $T_{mu}^{'} - T_F^{'} \leq \Delta T_1$, where $T_{mu}^{'}$ is the current timestamp of *MU* and $\Delta T_1$ is the expected legal time interval for the transmission delay between *MU* and *FA*. If the comparison fails, *MU* rejects message $M_4$.
12. *MU* computes $V_2^* = h(h(ID_{mu}||K)||ID_{FA}||r_f||ID_{mu})$ and verifies whether $V_2^* = V_2$ or not.
13. If verification holds, *MU* ensures the legality of *FA* and *HA*, and computes agreed session key $Sess_{key} = h(h(ID_{mu}||K)||ID_{FA}||r_f||ID_{mu}||B_1)$.

### 5.4 Password Change Phase

With this phase the mobile user *MU* can change his/her password whenever he/she wants

1. *MU* inserts his/her smart card into a card reader, enters his/her identity $ID_{mu}^*$ and password $PWD_{mu}^*$, and submits a request to change his/her password.
2. Then, smart card computes $C_i^* = h(h(ID_{mu}^*) \oplus h(b \oplus PWD_{mu}^*))mod\, n$ and verifies whether $C_i^* = C_i$ or not. If verification holds, then legality of $ID_{mu}^*$ and $PWD_{mu}^*$ is

ensured and smart card asks the mobile user $MU$ to enter the new password $PWD_{mu\_new}$. Otherwise, the password change request is rejected.

3. Then, the smart card computes

$$\begin{aligned} C_{i\_new} &= h(h(ID_{mu}) \oplus h(b \oplus PWD_{mu\_new}))mod\, n \\ K^*_{mu} &= K_{mu} \oplus h(b \oplus PWD_{mu}) \oplus h(b \oplus PWD_{mu\_new}) \\ &= h(ID_{mu}||ID_{HA}||X_{mu}||T_R) \oplus h(b \oplus PWD_{mu\_new}) \end{aligned}$$

and smart card replaces $\{C_i, K_{mu}\}$ with $\{C_{i\_new}, K^*_{mu}\}$, respectively. Finally, the smart card contains $\{C_{i\_new}, g, y, n, ID_{HA}, K^*_{mu}, b, h(\cdot)\}$.

## 6 Security Analyses

In this section, we analyse the security of the proposed scheme and show that our scheme can achieve all of the security requirements described in Sect. 1.

### 6.1 User Anonymity and Untraceability

A protocol with user anonymity protects an individual's sensitive personal information, such as preferences, lifestyles, social circle, shopping patterns, and so on, from being acquired by an adversary through analyzing the login information, the resources, or the services being accessed. Additionally, in mobile environment, the leakage of user-specific information may facilitate an unauthorized entity to track the user's login history and current location. Moreover, anonymity makes remote user authentication mechanism stronger as an attacker cannot track which users are interacting with the server. A simple way to preserve anonymity is to hide the user's valid identity during communication.

In our proposed scheme, the anonymity of $MU$ is achieved by one-way hash function and symmetric encryption technique. In the registration phase, the identity of $MU$ is submitted to $HA$ through a secure communication channel, thus the attacker cannot obtain the identity of $MU$. Suppose an attacker intercepts the message $M_1 = \{B_1, SID, V_1, ID_{HA}, T_{mu}\}$ and extracts the secret values such as $\{C_i, g, y, n, ID_{HA}, K_{mu}, b\}$ stored in the mobile user's $MU$ smart card by Assumption 2. Then, the attacker may try to retrieve information about $ID_{mu}$ from the intercepted parameters $B_1 = g^x mod\, n$ and $SID = (ID_{mu}||B_1)_{B_2} \oplus h(B_1 \oplus B_2)$. For retrieving $ID_{mu}$, the attacker must know the value of $B_2 = y^x mod\, n$, but $B_2$ is neither stored in the smart card nor transmitted through any of the messages $\{M_1, M_2, M_3, M_4\}$. An attacker cannot compute $B_2$ without a random number $x$ and secret key $d$ of $HA$. In addition, the values $B_1$ and $B_2$ are freshly generated for each session using the random number $x$. However, the attacker cannot retrieve the real identity $ID_{mu}$ of mobile user $MU$ without knowing the secret key $d$ and a random number $x$. Thus, the attacker cannot obtain the identity of $MU$. Only $HA$ can obtain the real identity $ID_{mu}$ of $MU$ by computing $(ID_{mu}||B_1)_{B_2} = SID \oplus h(B_1 \oplus B^*_2)$ and decrypting $(ID_{mu}||B_1)_{B_2}$ with $B^*_2$, since only $HA$ compute $B^*_2 = y^x mod\, n$ using its secret key $d$. Therefore, our proposed scheme can preserve user anonymity.

User untraceability is a stronger property than user anonymity, which requires that any third party including the foreign agent $FA$ cannot link two conversations originated from the same mobile user $MU$. In other words, the attacker is not capable of identifying any past protocol runs which have the same mobile user $MU$ involved. In our proposed scheme, $B_1$, $SID$ and $V_1$ are associated with random number $x$ and dynamically changed. As a result,

the login request message $M_1 = \{B_1, SID, V_1, ID_{HA}, T_{mu}\}$ is different at each login. Due to the hardness of the discrete logarithm problem, the attacker is unable to tell whether two protocol runs has the same mobile user $MU$ involved. Therefore, our proposed scheme achieves user untraceability.

### 6.2 Known-Key Attack

The Known-key attack means that a key agreement protocol should still achieve its goal in the presence of an attacker who has found out some other session keys. Our proposed scheme uses the timestamps $\{T_{mu}, T'_{mu}, T_H, T'_H, T_F, T'_F\}$ and the random numbers $r_f$, $x$ each session. Moreover, $Sess_{key} = h(h(ID_{mu}||K)||ID_{FA}||r_f||ID_{mu}||B_1)$ is created by the legal mobile user $MU$ and the foreign agent $FA$ in each session. The timestamps and random numbers are independent in each session. Thus, the session keys are also independent. Therefore, the awareness of previous session keys does not help to derive a new session key, and vice versa. Therefore, our proposed scheme can withstand the known-key attack.

### 6.3 Perfect Forward Secrecy

Forward secrecy ensures that an attacker who knows a subset of old session keys cannot find out consequent session keys. In our proposed scheme, value of $x$ and $r_f$ are freshly generated in each session, all the past session keys will remain secure even if the secret key $d$ of $HA$ is compromised at a later stage. Therefore, our proposed scheme achieves perfect forward secrecy.

### 6.4 Insider Attack

Suppose an insider of the home agent $HA$ has obtained a mobile user $MU$'s password $PWD_{mu}$. Then, an insider of the home agent $HA$ may try to impersonate the mobile user to access any foreign agent. In our proposed scheme, the mobile user $MU$ generates a random number $b$ and computes $(b \oplus PWD_{mu})$. Then, $MU$ sends a registration request message $M = \{ID_{mu}, (b \oplus PWD_{mu})\}$ to the home agent $HA$ through secure channel. Hence, the insider of $HA$ cannot get the password $PWD_{mu}$ from $(b \oplus PWD_{mu})$ without knowing the random number $b$. Also, a legal $MU$ cannot perform an insider attack to impersonate a legal home agent $HA$ because there is no way to obtain the secret key $d$ of the home agent $HA$. Although mobile user $MU$ can extract $y = g^d mod\, n$, $g$ and $n$ from his/her smart card under Assumption 2, he/she still cannot obtain the $HA$'s secret key $d$ because of the hardness of discrete logarithm problem. Therefore, our proposed scheme can withstand the insider attacks by the legal $HA$ and the legal $MU$.

### 6.5 Off-Line Password Guessing Attack

Suppose an attacker (including a valid foreign agent and any other users except $MU$) steals or finds a lost smart card of a mobile user $MU$ and extracts all values $\{C_i, g, y, n, ID_{HA}, K_{mu}, b\}$ from it under Assumption 2. As demonstrated above, throughout our proposed scheme, the mobile user $MU$'s password $PWD_{mu}$ only makes three appearances as $C_i = h(h(ID_{mu}) \oplus h(b \oplus PWD_{mu}))mod\, n$ and $K_{mu} = h(ID_{mu}||ID_{HA}||X_{mu}||T_R) \oplus h(b \oplus PWD_{mu})$ and $K = K_{mu} \oplus h(b \oplus PWD_{mu})$. Obviously, the attacker cannot launch an

off-line password guessing attack without knowing *MU*'s identity $ID_{mu}$. Since it has been demonstrated that our scheme can preserve user anonymity (in Sect. 6.1), the proposed scheme can withstand off-line password guessing attack with smart card security breach.

### 6.6 Replay Attack

A replay attack refers to the retransmission of earlier intercepted untrue messages. An attacker may intercept messages $\{M_1, M_2, M_3, M_4\}$ under Assumption 1, which are transmitted among *MU*, *FA* and *HA*. An attacker might replay the old message $M_1 = \{B_1, SID, V_1, ID_{HA}, T_{mu}\}$ to FA and then receive the message $M_4 = \{V_2, r_f, T_F^{'}\}$. However, an attacker cannot compute the session key $Sess_{key} = h(h(ID_{mu}||K)||ID_{FA}||r_f||ID_{mu}||B_1)$ without knowing the secret $h(ID_{mu}||K)$ and an identity $ID_{mu}$. Since it has been demonstrated that our scheme can preserve user anonymity (in Sect. 6.1), an attacker cannot compute $h(ID_{mu}||K)$ and $ID_{mu}$. Thus, an attacker cannot access the service from *FA*. In addition, our proposed scheme uses random number and timestamps. If an adversary replays the transmitted messages, the receiver can detect the invalid timestamp and terminate the protocol. Therefore, our proposed scheme can withstand the replay attack.

### 6.7 Stolen-Verifier Attacks

The stolen-verifier attack means that an attacker stole the password-verifier from the server's database and applied an off-line password guessing attack on it to get the user's password and hence, he can impersonate as a legal user. In our proposed scheme, the password table or verification table is not stored on the home agent *HA*. Only the secret key $d$ and encrypted form of user-specific information $\{ID_{mu}, X_{mu}, T_R\}$ are maintained by the home agent *HA*. Besides, information stored on the *HA* are not password involved verifier. Thus, the attacker cannot steal and modify user passwords. Therefore, our scheme can withstand stolen-verifier attacks.

### 6.8 Forgery Attacks (Impersonation Attacks)

#### *6.8.1 MU Forgery Attack*

An attacker may intercept the login request message $M_1 = \{B_1, SID, V_1, ID_{HA}, T_{mu}\}$ sent out from a legal mobile user *MU* in Step 1 of the past authentication sessions and attempt to impersonate the legal mobile user *MU*. Then, the attacker sends the login request messages $M_1$ to *FA* in two ways. First, the attacker sends $M_1 = \{B_1, SID, V_1, ID_{HA}, T_{mu}\}$ without any alteration. Upon receiving $M_1$, *FA* verifies the freshness of $T_{mu}$ by comparing $T_F - T_{mu} \leq \Delta T_1$. As this comparison will fail, the attacker will not be considered a legal mobile user. Second, the attacker sends $M_1$ with an alteration such as $M_1^* = \{B_1, SID, V_1, ID_{HA}, T_{mu}^*\}$ where $T_{mu}^*$ is the modified current timestamp. Upon receiving $M_1^*$, *FA* verifies the freshness of $T_{mu}^*$ by comparing $T_F - T_{mu}^* \leq \Delta T_1$. Now the comparison will be true and *FA* will send the message $M_2^*$={ $W_1$, $ID_{FA}$, $r_f$, $T_F$, $B_1$, $SID$, $V_1$, $T_{mu}^*$ } to *HA*. Upon receiving the messages $M_2$ sent by *FA*, *HA* verifies if the messages are valid. However, the verification will be unsuccessful, because $V_1 = h(K||B_2||SID||T_{mu})$ is not equal to computed $V_1^* = h(K^*||B_2^*||SID||T_{mu}^*)$ by *HA* in Step 3. Since it has been demonstrated that our scheme can withstand password guessing attack (in Sect. 6.5), the attacker

cannot create valid login request messages $M_1$ without knowing $MU$'s password $PWD_{mu}$. Therefore, our proposed scheme can withstand the $MU$ forgery attack.

#### 6.8.2 FA Forgery Attack

Without knowing the pre-shared secret key $K_{FH}$ between $FA$ and $HA$, an attacker cannot forge the message $M_2 = \{W_1, ID_{FA}, r_f, T_F, B_1, SID, V_1, T_{mu}\}$ in Step 2 of the proposed scheme because $FA$ cannot compute the correct $W_1 = h(K_{FH}||ID_{FA}||r_f||T_F||B_1||V_1||SID)$. In addition, without knowing the shared session key $Sess_{key}$ between $MU$ and $FA$, an attacker cannot forge the message $M_4 = \{V_2, r_f, T_F^{'}\}$. Therefore, our proposed scheme can withstand the $FA$ forgery attack.

#### 6.8.3 HA Forgery Attacks

Without knowing the secret key $d$ of $HA$ and pre-shared secret key $K_{FH}$ between $FA$ and $HA$, an attacker cannot forge the messages $M_3 = \{K_1, V_2, S_2, T_H^{'}\}$ in Step 3 of our proposed scheme because he/she cannot compute $W_1^*$ and cannot derive $ID_{mu}$. Therefore, our proposed scheme can withstand the $HA$ forgery attack.

### 6.9 Mutual Authentication

With the purpose of thwart forgery, the mobile user $MU$, the foreign agent $FA$, and the home agent $HA$ should authenticate each other. Our proposed scheme provides explicit mutual authentication as follows:

#### 6.9.1 Mutual Authentication Between MU and HA

In Step 3 of authentication phase, $HA$ can authenticate $MU$ by verifying $V_1^* = V_1$. Because of $K = h(ID_{mu}||ID_{HA}||X_{mu}||T_R)$ in $V_1 = h(K||B_2||SID||T_{mu})$ shared secret authentication key, only legal $MU$ can generate a valid $V_1$. Thus, $MU$ is authenticated by $HA$. Similarly, $MU$ also can authenticate $HA$ by verifying $V_2^* = V_2$ in step 4. Thus, $HA$ is authenticated by $MU$.

#### 6.9.2 Mutual Authentication Between FA and HA

$HA$ authenticates $FA$ by verifying $W_1^* = W_1$ in step 3. Because of $K_{FH}$ in $W_1 = h(K_{FH}||ID_{FA}||r_f||T_F||B_1||V_1||SID)$ shared secret authentication key, only legal $FA$ can generate a valid $W_1$. Thus, $FA$ is authenticated by $HA$. $FA$ also authenticates $HA$ by verifying $S_2^* = S_2$ in Step 4. Because of $h(K_{FH}||r_f)$ in $K_1$, only legal $HA$ can compute valid $h(K_{FH}||r_f)$. Thus, $HA$ is authenticated by $FA$.

#### 6.9.3 Mutual Authentication Between MU and FA

$MU$ can authenticate $FA$ by verifying $V_2^* = V_2$ in Step 4. Thus, $HA$ is authenticated by $MU$. $FA$ can authenticate $MU$ by session key $Sess_{key} = h(h(ID_{mu}||K)||ID_{FA}||r_f||ID_{mu}||B_1)$.

Therefore, our proposed scheme can achieves proper mutual authentication.

### 6.10 Man-in-the-Middle Attacks

In our proposed scheme, Man-in-the-middle attacks are thwarted because of the authentication between *MU* and *HA*. Similarly, Man-in-the-middle attacks can be thwarted by the establishment of a session key between *MU* and *FA*. Since it has been demonstrated that our proposed scheme can achieve mutual authentication (in Sect. 6.9), Man-in-the-middle attacks are thwarted.

### 6.11 Local Password Verification

In our proposed scheme, smart card checks the validity of M*U*'s identity $ID_{mu}$ and password $PWD_{mu}$ before logging into foreign agent *FA*. An attacker cannot compute the correct $C_i = h(h(ID_{mu}) \oplus h(b \oplus PWD_{mu}))mod\, n$ without the knowledge of $ID_{mu}$ and $PWD_{mu}$ to pass the verification $C_i^* = C_i$ in Step 1. Therefore, our scheme can avoid the unauthorized accessing by the local password verification.

### 6.12 User Friendliness

In our proposed scheme, *MU* can freely choose their own password $PWD_{mu}$ and identity $ID_{mu}$. Also, *MU* is allowed to change his/her password $PWD_{mu}$ without *HA* assistance in less time because he/she need not go through the entire login-authentication procedure. This makes proposed scheme user-friendly. Since the smart card can verify the correctness of input efficiently, a *MU* can change his/her password correctly without any mistake. Thus, the password change phase will not become a security loophole as any attacker will not have all the sufficient data to modify the password. At the same time, for a legitimate mobile user, the password change process is not cumbersome and is secure.

## 7 Performance and Security Requirements Comparisons

To evaluate our proposed scheme, we compare it with other, related schemes. We compared the schemes of He et al. [14], Yoon et al. [23], Rhee et al. [20], Jiang et al. [28] and Li et al. [30] to our own in terms of the security requirements satisfied and performance. Because the login and authentication phases are executed much more frequently than the other phases in password authentication schemes, we consider only the computational costs of these two phases. Particularly, we focus on the number of cryptographic operations that mobile user *MU* needs to perform, because mobile devices usually are low-powered mobile devices and thus computation cost at the user end is always regarded as key criteria. Note that we ignore the computational cost of lightweight operations such as *XOR*, concatenation and comparison because they require very limited computation. To facilitate the computational costs analyses, we define the following notation:

- $t_h$: the computational cost of one hash operation;
- $t_{se}$: the computational cost of one small-modular exponent;
- $t_{mexp}$: the computational cost of one modular exponent;
- $t_{sym}$: the computational cost of one symmetric key encryption or decryption;

Table 3 illustrates the results of the performance comparisons of our proposed scheme and the other related schemes; from this table, it can be observed that the overall computational

**Table 3** Performance comparision

| Schemes | Computation cost on user side |
|---|---|
| He et al. [14] | $10t_h + 3t_{sym}$ |
| Yoon et al. [23] | $5t_h + 2t_{sym}$ |
| Rhee et al. [20] | $6t_h + 2t_{sym}$ |
| Jiang et al. [28] | $4t_h + t_{mexp}$ |
| Li et al. [30] | $5t_h + t_{sym}$ |
| Our scheme | $8t_h + 2t_{se} + t_{mexp}$ |

$t_h$ the computational cost of one hash operation, $t_{se}$ the computational cost of one small-modular exponent, $t_{mexp}$ the computational cost of one modular exponent, $t_{sym}$ the computational cost of one encryption/decryption

**Table 4** Security requirements comparision

| Schemes | Security requirements (SR) | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | $SR_1$ | $SR_2$ | $SR_3$ | $SR_4$ | $SR_5$ | $SR_6$ | $SR_7$ | $SR_8$ | $SR_9$ | $SR_{10}$ | $SR_{11}$ | $SR_{12}$ |
| He et al. [14] | N | N | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| Yoon et al. [23] | N | N | Y | N | Y | Y | Y | Y | Y | Y | N | N |
| Rhee et al. [20] | N | Y | N | Y | N | Y | Y | N | Y | Y | N | N |
| Jiang et al. [28] | Y | Y | Y | Y | Y | N | N | Y | Y | Y | N | Y |
| Li et al. [30] | N | Y | Y | Y | N | Y | Y | Y | Y | Y | Y | Y |
| Proposed scheme | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |

*Y* achieved, *N* not achieved

costs of mobile user *MU* (low-powered mobile devices) of schemes of He et al. [14], Yoon et al. [23], Rhee et al. [20], Jiang et al. [28], Li et al. [30] and our proposed scheme in the login and authentication phases are, respectively, $10t_h + 3t_{sym}$, $5t_h + 2t_{sym}$, $6t_h + 2t_{sym}$, $4t_h + t_{mexp}$, $5t_h + t_{sym}$ and $8t_h + 2t_{se} + t_{sym}$. It is worth noting that the small-exponent exponentiation operation is much less costly as compared to the common exponentiation operation, i.e. $t_{se} \ll t_{mexp}$. For example, Scott et al. [59] reported that, when the small-exponent $e$ is set to $2^{16} + 1$(and $|n| = 1024$ bit), one such small-exponent exponentiation only takes 5.384 ms on a 32-bit 36 **MHz RISC MIPS**-based smart card, while one common exponentiation costs 0.14 s. Therefore, from Table 3, it is obvious to see that our proposed scheme maintains reasonable efficiency than He et al.'s scheme [14] and satisfies more security requirements than He et al.'s scheme, as is shown in Table 4. Compared to the related schemes of Yoon et al. [23], Rhee et al. [20], Jiang et al. [28] and Li et al. [30], our scheme's computation cost for the *MU* is little increased. For the reason that, in our proposed scheme, smart card checks the validity of *MU*'s identity $ID_{mu}$ and password $PWD_{mu}$ before logging into foreign agent *FA*(i.e. local password verification), and the other related schemes do not.

Most of all, our proposed scheme exceeds He et al.'s scheme [14] in both security and performance. Our scheme provides a great improvement over the related schemes of Yoon et al. [23], Rhee et al. [20], Jiang et al. [28] and Li et al. [30] regarding security strength. The comparisons of the security requirements satisfied by our proposed scheme and the other schemes is summarized in Table 4; from this table, it can be seen that our proposed

scheme is more secure than the other related schemes. Concisely, our scheme maintains reasonable efficiency and is well suited to mobile environments.

## 8 Conclusion

In this paper, we have reanalyzed Rhee et al.'s scheme and shown that, this scheme cannot provide perfect forward secrecy, user friendliness and local password verification, and suffers from user impersonation attack, off-line password guessing attack. In order to overcome the weaknesses of Rhee et al.'s scheme, we propose a secure authentication scheme with user anonymity for roaming service in global mobility networks. Performance and security analysis show the proposed scheme is secure against various attacks, and is well suited to mobile environments.

**Acknowledgments** We would like to thank the anonymous reviewers for their positive suggestions and comments that highly improve the readability and completeness of the paper. Also we would like to acknowledge the management of VIT University for providing the wonderful support to do the research work.

## References

1. Suzuki, S., & Nakada, K. (1997). An authentication technique based on distributed security management for the global mobility network. *IEEE Journal on Selected Areas in Communications*, *15*(8), 1608–1617.
2. Huang, X., Xiang, Y., Chonka, A., Zhou, J., & Deng, R. H. (2011). A generic framework for three-factor authentication: Preserving security and privacy in distributed systems. *IEEE Transactions on Parallel and Distributed Systems*, *22*(8), 1390–1397.
3. Zhu, J., & Ma, J. (2004). A new authentication scheme with anonymity for wireless environments. *IEEE Transactions on Consumer Electronics*, *50*(1), 231–235.
4. Lee, C.-C., Hwang, M.-S., & Liao, I.-E. (2006). Security enhancement on a new authentication scheme with anonymity for wireless environments. *IEEE Transactions on Industrial Electronics*, *53*(5), 1683–1687.
5. Wei, Y., Qiu, H., & Hu, Y. (2006) Security analysis of authentication scheme with anonymity for wireless environments. In *International conference on communication technology, 2006 (ICCT'06)* (pp. 1–4), IEEE.
6. Chia-Chun, W., Lee, W.-B., & Tsaur, W.-J. (2008). A secure authentication scheme with anonymity for wireless communications. *IEEE Communications Letters*, *12*(10), 722–723.
7. Jing, X., & Feng, D. (2009). Security flaws in authentication protocols with anonymity for wireless environments. *ETRI Journal*, *31*(4), 460–462.
8. Lee, J.-S., Chang, J. H., & Lee, D. H. (2009). Security flaw of authentication scheme with anonymity for wireless communications. *IEEE Communications Letters*, *13*(5), 292–293.
9. Wang, C.-H., Wei, T.-C., Lee, P.-C., & Wu, C.-C. (2009). An improvement of secure authentication scheme with full anonymity for wireless communications. In *Proceedings of the 2nd international conference on interaction sciences: information technology, culture and human* (pp. 115–118), ACM.
10. Jeon, W., Kim, J., Lee, Y., & Won, D. (2012). Security analysis of authentication scheme for wireless communications with user anonymity. In *Information technology convergence, secure and trust computing, and data management* (pp. 225–231). Berlin: Springer.
11. Chang, C.-C., Lee, C.-Y., & Chiu, Y.-C. (2009). Enhanced authentication scheme with anonymity for roaming service in global mobility networks. *Computer Communications*, *32*(4), 611–618.
12. Youn, T.-Y., Park, Y.-H., & Lim, J. (2009). Weaknesses in an anonymous authentication scheme for roaming service in global mobility networks. *IEEE Communications Letters*, *13*(7), 471–473.
13. Zeng, P., Cao, Z., Choo, K., & Wang, S. (2009). On the anonymity of some authentication schemes for wireless communications. *IEEE Communications Letters*, *13*(3), 170–171.
14. He, D., Ma, M., Zhang, Y., Chen, C., & Jiajun, B. (2011). A strong user authentication scheme with smart cards for wireless communications. *Computer Communications*, *34*(3), 367–374.

15. Li, C.-T., & Lee, C.-C. (2012). A novel user authentication and privacy preserving scheme with smart cards for wireless communications. *Mathematical and Computer Modelling*, *55*(1), 35–44.
16. Jeon, W., Lee, Y., & Won, D. (2013). An efficient user authentication scheme with smart cards for wireless communications. *International Journal of Security & Its Applications, 7*(4), 1–5.
17. Ashok Kumar Das. (2013). A secure and effective user authentication and privacy preserving protocol with smart cards for wireless communications. *Networking Science*, *2*(1–2), 12–27.
18. Wen, F., Susilo, W., & Yang, G. (2014). A robust smart card-based anonymous user authentication protocol for wireless communications. *Security and Communication Networks*, *7*(6), 987–993.
19. Jing, X., Zhu, W.-T., & Feng, D.-G. (2011). An efficient mutual authentication and key agreement protocol preserving user anonymity in mobile networks. *Computer Communications*, *34*(3), 319–325.
20. Rhee, H. S. (2011). Improved user authentication scheme with user anonymity for wireless communications. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*,*94*(2), 860–864.
21. Jian-bin, H., Xiong, H., & Chen, Z. (2012). Further improvement of an authentication scheme with user anonymity for wireless communications. *IJ Network Security*, *14*(5), 297–300.
22. He, D., Chan, S., Chen, C., Jiajun, B., & Fan, R. (2011). Design and validation of an efficient authentication scheme with anonymity for roaming service in global mobility networks. *Wireless Personal Communications*, *61*(2), 465–476.
23. Yoon, E.-J., Yoo, K.-Y., & Ha, K.-S. (2011). A user friendly authentication scheme with anonymity for wireless communications. *Computers & Electrical Engineering*, *37*(3), 356–364.
24. Niu, J., & Li, X. (2014). A novel user authentication scheme with anonymity for wireless communications. *Security and Communication Networks*, *7*(10), 1467–1476.
25. Li, C.-T. (2012). A more secure and efficient authentication scheme with roaming service and user anonymity for mobile communications. *Information Technology and Control*, *41*(1), 69–76.
26. Mun, H., Han, K., Lee, Y. S., Yeun, C. Y., & Choi, H. H. (2012). Enhanced secure anonymous authentication scheme for roaming service in global mobility networks. *Mathematical and Computer Modelling*, *55*(1), 214–222.
27. Kim, J.-S., & Kwak, J. (2012). Improved secure anonymous authentication scheme for roaming service in global mobility networks. *International Journal of Security and Its Applications*, *6*(3), 45–54.
28. Jiang, Q., Ma, J., Li, G., & Yang, L. (2013). An enhanced authentication scheme with privacy preservation for roaming service in global mobility networks. *Wireless Personal Communications*, *68*(4), 1477–1491.
29. Wen, F., Susilo, W., & Yang, G. (2013). A secure and effective anonymous user authentication scheme for roaming service in global mobility networks. *Wireless Personal Communications*, *73*(3), 993–1004.
30. Li, H., Yang, Y., & Pang, L. (2013). An efficient authentication protocol with user anonymity for mobile networks. In *2013 IEEE wireless communications and networking conference (WCNC)* (pp. 1842–1847), IEEE.
31. Xie, Q., Bin, H., Tan, X., Bao, M., & Xiuyuan, Y. (2014). Robust anonymous two-factor authentication scheme for roaming service in global mobility network. *Wireless Personal Communications*, *74*(2), 601–614.
32. Jing, X., & Zhu, W.-T. (2013). A generic framework for anonymous authentication in mobile networks. *Journal of Computer Science and Technology*, *28*(4), 732–742.
33. Zhao, D., Peng, H., Li, L., & Yang, Y. (2013). A secure and effective anonymous authentication scheme for roaming service in global mobility networks. *Wireless Personal Communications*, *78*(1), 247–269.
34. Hu, B., Bao, M., & Dong, N. (2014). Improvement of user authentication protocol with anonymity for wireless communications. *Kuwait Journal of Science*, *41*(1), 155–169.
35. Kuo, W.-C., Wei, H.-J., & Cheng, J.-C. (2014). An efficient and secure anonymous mobility network authentication scheme. *Journal of Information Security and Applications*, *19*(1), 18–24.
36. Liu, J., Wang, D., & Wang, P. (2014). Improved privacy-preserving authentication scheme for roaming service in mobile networks. In *2014 IEEE wireless communications and networking conference (WCNC)*.
37. Zhou, N., Chen, X., Li, C., & Xue, Z. (2014). Secrecy rate of two-hop af relaying networks with an untrusted relay. *Wireless Personal Communications*, *75*(1), 119–129.
38. Jiang, Q., Ma, J., Li, G., & Yang, L. (2014). An efficient ticket based authentication protocol with unlinkability for wireless access networks. *Wireless Personal Communications*, *77*(2), 1489–1506.
39. He, D., Zhang, Y., & Chen, J. (2014). Cryptanalysis and improvement of an anonymous authentication protocol for wireless access networks. *Wireless Personal Communications*, *74*(2), 229–243.
40. ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. In *Advances in cryptology* (pp. 10–18). Berlin: Springer.
41. Rivest, R. (1992). *Rfc 1321: The md5 message-digest algorithm.* Technical report RFC 1321, IETFl.

42. Secure Hash Standard. Technical report fips pub 180-1. *US Department of Commerce/National Institute of Standards and Technology*, 1995.
43. Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, *22*(6), 644–654.
44. Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*(2), 120–126.
45. Jing, X., Zhu, W.-T., & Feng, D.-G. (2009). An improved smart card based password authentication scheme with provable security. *Computer Standards & Interfaces*, *31*(4), 723–728.
46. Kocher, P., Jaffe, J., & Jun, B. (1999). Differential power analysis. In *Advances in cryptology (CRYPTO99)* (pp. 388–397). Berlin: Springer
47. Messerges, T. S., Dabbish, E. A., & Sloan, R. H. (2002). Examining smart-card security under the threat of power analysis attacks. *IEEE Transactions on Computers*, *51*(5), 541–552.
48. Wang, D., Ma, C., & Wu, P. (2012). Secure password-based remote user authentication scheme with non-tamper resistant smart cards. In *Data and applications security and privacy XXVI* (pp. 114–121). Berlin: Springer
49. Sood, S. K. (2011). Secure dynamic identity-based authentication scheme using smart cards. *Information Security Journal: A Global Perspective*, *20*(2), 67–77.
50. Tapiador, J. E., Hernandez-Castro, J. C., Peris-Lopez, P., & Clark, J. A. (2011). *Cryptanalysis of song's advanced smart card based password authentication protocol*. arXiv preprint arXiv:1111.2744
51. Shim, K.-A. (2012). Security flaws in three password-based remote user authentication schemes with smart cards. *Cryptologia*, *36*(1), 62–69.
52. He, D., & Shuhua, W. (2013). Security flaws in a smart card based authentication scheme for multi-server environment. *Wireless Personal Communications*, *70*(1), 323–329.
53. Wang, D., Ma, C., Gu, D., & Cui, Z. (2012). Cryptanalysis of two dynamic id-based remote user authentication schemes for multi-server architecture. In *Network and system security* (pp. 462–475). Berlin: Springer.
54. Ma, C., Wang, D., & Zhao, S.-D. (2014). Security flaws in two improved remote user authentication schemes using smart cards. *International Journal of Communication Systems*, *27*(10), 2215–2227.
55. Wang, D., & Wang, P. (2014). Offline dictionary attack on password authentication schemes using smart cards. *IACR Cryptology ePrint Archive*, *2014*, 208.
56. Wang, D., & Wang, P. (2014). On the anonymity of two-factor authentication schemes for wireless sensor networks: Attacks, principle and solutions. *Computer Networks*, *73*(14), 41–57.
57. Karuppiah, M., & Saravanan, R. (2014). A secure remote user mutual authentication scheme using smart cards. *International Journal of Security and Its Applications*, *19*(4–5), 282–294.
58. Kasper, T., Oswald, D., & Paar, C. (2012). Side-channel analysis of cryptographic rfids with analog demodulation. In *RFID security and privacy* (pp. 61–77). Berlin: Springer.
59. Scott, M., Costigan, N., & Abdulwahab, W. (2006). Implementing cryptographic pairings on smartcards. In *Cryptographic hardware and embedded systems (CHES 2006)* (pp. 134–147). Berlin: Springer.

**Marimuthu Karuppiah** received his B.E. degree in Computer Science and Engineering from Madurai Kamaraj University, Madurai, India in 2003, M.E. degree in Computer Science and Engineering from Anna University, Chennai, India in 2005. In 2005, he has appointed as a Lecturer in Department of Computer Science and Engineering at Syed Ammal Engineering College, Ramanathapuram, India. He is now an Assistant professor (Senior) in School of Computing Science and Engineering, VIT University, Vellore, India. Now he is pursuing his Ph.D. degree at VIT University, Vellore, India. He has published more than 10 research papers in reputed international conferences and journals. He is a life member of Cryptology Research Society of India (CRSI). His main research interests include cryptography and wireless network security, in particular, authentication and encryption schemes.

**R. Saravanan** completed his doctoral thesis in the area of Approximation Algorithms in 1997 at Ramanujan Institute for Advanced Study in Mathematics and obtained the Ph.D. degree from University of Madras. He received M.E. degree in Computer Science and Engineering from College of Engineering, Guindy, Anna University, Chennai. He has rich research experience in areas of algorithms and published more than seventy five research papers in the peer reviewed international journals and numerous research papers in national journals, international and national conferences. He served as an academic council member and board of study member in many universities and autonomous colleges. He has about two decades of teaching and research experience. He is a life member of Computer Society of India (CSI), Cryptology Research Society of India (CRSI) and Ramanujan Mathematical Society and also he is a member of IEEE. Three research scholars completed their Ph.D under his guidance and supervision and ten more his research scholars are carrying out their research towards their Ph.D. His areas of research include approximation algorithms, mobile computing, cryptography, and network security.