PRIVACY-PRESERVING AUTHENTICATION SCHEME FOR ROAMING SERVICE IN GLOBAL MOBILITY NETWORKS

Sung Woon Lee[1], and Hyunsung Kim[2, 3]

[1]Department of Information Security, Tongmyong University, Busan, Korea
[2]Department of Mathematical Sciences, University of Malawi, Zomba, Malawi
[3]School of Computer Science, Kyungil University, Kyungbuk, Korea

Abstract

With the rapid development of mobile intelligent technologies and services, users can freely experience ubiquitous services in global mobility networks. It is necessary to provide authentications and protection to the privacy of mobile users. Until now, many authentication and privacy schemes were proposed. However, most of the schemes have been exposed to some security problems. Recently, Madhusudhan and Shashidhara (M&S) proposed a lightweight authentication scheme, denoted as the M&S scheme, for roaming services in global mobility networks. This paper shows that the M&S scheme has security flaws including two masquerading attacks and a mobile user trace attack. After that, we propose a privacy-preserving authentication scheme for global mobility networks. The proposed scheme not only focused on the required security but also added privacy concerns focused on anonymity based on a dynamic pseudonym, which is based on exclusive-or operation, hash operation and symmetric key cryptography. Formal security analysis is performed based on Burrow-Abadi-Needdham (BAN) logic and the ProVerif tool, which concludes that the proposed scheme is secure. The analysis shows that the proposed authentication scheme is secure and provides privacy with a reasonable performance.

KEYWORDS

Authentication, Communication System Security, Global Mobility Network, Health Information management, Privacy

1. INTRODUCTION

With the rapid development of wireless communication technology and artificial intelligence, mobility is becoming more and more important in our daily life. Users with mobile intelligent devices can enjoy rich and seamless services, such as social network services, online shopping, bank transfer and many more various services [1-3]. Roaming service shown in Fig. 1 enables a mobile user (MU) to use the services extended by his/her home agent (HA) in a foreign agent (FA). User authentications and privacy schemes play an important role in global mobility networks. There are three participants in a secure scheme for roaming service, namely MU, FA and HA. MU needs to be registered to his/her HA. When MU roams to a foreign network (FN) by a FA, MU should pass authentication from FA by helping HA in a home network (HN).

Until now, many user authentication and privacy schemes for roaming service were proposed [4-19]. Zhu and Ma proposed the first anonymous authentication scheme for roaming service based on hash function, symmetric key cryptosystem and asymmetric key cryptosystem [4]. However, Lee *et al*. pointed out that Zhu and Ma's authentication scheme is vulnerable to impersonation attack and does not achieve mutual authentication [12]. Furthermore, they also proposed an

DOI: 10.5121/ijcnc.2021.13507

improved scheme to solve Zhu and Ma's security weaknesses. Chang *et al*. showed that Lee *et al*.'s scheme has still security problem against the forgery attack and proposed an enhanced scheme to solve the security problem [13]. Yang *et al*. proposed a universal anonymous authentication scheme for roaming service [14]. It does not require the involvement of HA and thus is quite efficient in terms of communication. Zhou *et al*. showed that Chang *et al*.'s scheme in [13] could not provide user anonymity and that the session key could be compromised if MU's real identity is leaked [15]. Meanwhile, Kuo *et al*. proposed an anonymous roaming authentication scheme for mobility networks based on elliptic curve cryptography (ECC) [16]. However, their protocol is inefficient in terms of communication. In 2015, Liu *et al*. proposed an anonymous authentication protocol that uses time-bound credentials for an efficient revocation. It is based on bilinear pairing and thus is inefficient in terms of computation [17]. Recently, Karuppiah and Saravanan proposed an authentication scheme, denoted by K&S scheme, with user anonymity for roaming services in global mobility networks [18]. They argued that their authentication scheme provides user anonymity and untraceability, and that it is secure against various attacks. However, Madhusudhan and Shashidhara provided cryptanalysis that K&S scheme has security weaknesses against insider attacks, stolen-verifier attacks, offline guessing attacks, denial of service (DoS) attacks and forgery attacks [19]. In addition to this, Madhusudhan and Shashidhara proposed a remedy scheme to solve the weaknesses, which is named as M&S scheme.

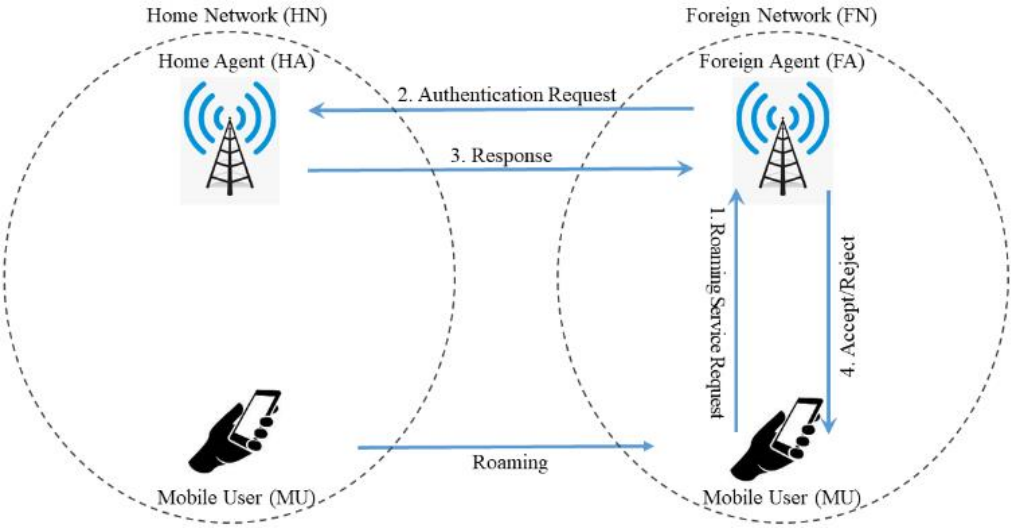

Figure 1. Roaming authentication in global mobility network

There are two purposes of this paper. First of all, we analyze M&S scheme and show that the scheme has two design flaws and suffers from HA masquerading attack, FA masquerading attack and MU trace attack. To overcome the weaknesses, we propose a privacy-preserving authentication scheme based on only hash function and symmetric key cryptosystem. Formal security analysis is provided based on Burrow-Adadi-Needham (BAN) logic and ProVerif tool to show that the proposed scheme is secure and provide privacy [20-21]. Informal analysis will be provided focused on the various aspects of security attacks. Compared with the other related schemes, the proposed scheme not only gets better security with privacy but also achieves similar performance compared to M&S scheme.

2. RELATED WORKS

There are several works, which investigated user authentication and privacy schemes for roaming services [4-19]. These schemes can be implemented based on different cryptographic mechanisms for the roaming service. Zhu and Ma devised the first anonymous authentication scheme for roaming service using smart cards [4]. Zhu and Ma's scheme is based on hash function, symmetric key cryptosystem and public key cryptosystem. However, MUs in Zhu and Ma's scheme only use symmetric encryption and decryption. They also planned to provide anonymity and untraceability to their scheme based on the one-time use of key between MU and FN.

However, Lee *et al*. pointed out that Zhu and Ma's scheme has three security weaknesses, not achieving perfect backward secrecy, not achieving mutual authentication and not protecting against forgery attack [12]. Furthermore, they proposed an improved scheme to solve Zhu and Ma's security weaknesses, which is based on exclusive-or operation, hash function, symmetric key cryptosystem and asymmetric key cryptosystem. Both Zhu and Ma's scheme in [4] and Lee *et al.*'s scheme in [12] requires the public key certificate based on X.509 that requires a big overhead for a public key infrastructure [22].

Chang *et al*. pointed out that Lee *et al*.'s scheme cannot provide anonymity under legal user's forgery attack and proposed an improved scheme with anonymity to remedy the security problem of Lee *et al*.'s scheme [13]. It uses random numbers to avoid possible attacks and uses one-way hash functions to reduce the computation cost. So, Chang *et al.*'s schemes are lightweight because it only uses exclusive-or operations and a one-way hash function for MDs.

Yang *et al*. proposed a universal anonymous authentication scheme for roaming service, which uses an elliptic curve digital signature algorithm (ECDSA) [14]. It does not require the involvement of HA and thus is quite efficient in terms of communication and uses the same protocol and signalling flows regardless of the domain (home or foreign) that MU is visiting. Furthermore, they proposed a user revocation mechanism to support strong user anonymity.
Zhou et al. introduced a formal security model suitable for roaming service in global mobility networks and proposed a new authentication scheme based on it [15]. After Zhou et al. showed that Chang *et al.*'s scheme in [13] fails to achieve user anonymity and that the leakage of MU's real identity is related to the compromise of the session key, they proposed their new scheme. Meanwhile, Kuo *et al*. proposed an anonymous roaming authentication scheme for mobility networks based on ECC [16]. It does not rely on asymmetric cryptography, which needs certificates usage based on X.509, but instead uses point multiplications. However, Kuo *et al*.'s scheme is inefficient in terms of communication.

In 2015, Liu *et al.* proposed an anonymous authentication protocol for a large scale network that uses time-bound credentials for an efficient revocation [17]. They designed a group signature scheme as a building block based on bilinear pairing over q-strong Diffie-Hellman assumption and thus it is inefficient in terms of computation even if it improved the revocation check process.

Recently, Karuppiah and Saravanan proposed K&S scheme based on asymmetric key cryptosystem with user anonymity for roaming service [18]. It is aimed to provide user anonymity and untraceability, and they argued that K&S scheme is secure against various attacks in global mobility networks. But Madhusudhan and Shashidhara showed that K&S scheme has security weaknesses against insider attack, stolen-verifier attack, offline guessing attack, DoS attack and forgery attack [19]. In addition to this, they proposed M&S scheme as a remedy scheme to solve the weaknesses in K&S scheme.

Unfortunately, this paper will show that M&S scheme still has security flaws including two masquerading attacks and MU trace attack. After that, we will propose a privacy-preserving authentication scheme for global mobility networks as a solution to M&S scheme.

3. REVIEW OF M&S SCHEME

This section reviews the M&S scheme for roaming service in global mobility networks [19]. M&S scheme is consisted with four phases, initialization phase, registration phase, login and authentication phase, and password change phase. Table 1 shows the notations used in this paper.

3.1. Initialization Phase

HA chooses two random numbers p and q and a generator g of a finite field in Z_p^*. It computes $n = p \times q$ and $\Phi(n) = (p-1) \times (q-1)$. Next, HA selects a random integer e such that $GCD(e, \Phi(n)) = 1$ and $1 < e < \Phi(n)$. Then, HA calculates the value of an integer d such that $d = e^{-1}$ where d is HA's secret key, and $y = g^d \bmod n$, where y is the public key. HA keeps $[d, p, q]$ secretly.

Table 1. Notations.

Notation	Description
MU	Mobile user
FA	Foreign agent
HA	Home agent
MD	Mobile device of MU
SK	Session key
ID_{MU}	Identity of MU
ID_{HA}	Identity of HA
ID_{FA}	Identity of FA
PW_{MU}	Password of MU
y, d	Public key and private key of HA
K_{FH}	Shared key between FA and HA
R_i, N	Random numbers
$E_k(.)$, $D_k(.)$	Symmetric key encryption/decryption with key k
$h(.)$	One-way hash function
$\|\|$	Bitwise concatenation
$\oplus$	Bitwise exclusive-or

3.2. Registration Phase

If MU wants to register with HA, he/she sends the necessary information through a secure channel.

R1: A new MU chooses his/her identity ID_{MU} and password PW_{MU}, and generates a random nonce N. Then, MU computes and submits $R_1 = h(ID_{MU}||N)$ to HA through a secure channel.
R2: Upon receiving R_1, HA computes $R = (R_1||ID_{HA}||d)$, $a = h(d)$ and $C_{MU} = (g^a \bmod p) \oplus h(R)$. Then, HA initializes the counter value $K = 0$ for MU and stores $\{K, R\}$ in its database. Finally, HA sends $\{R, C_{MU}, K, h(.)\}$ to MU through a secure socket layer.

R3: After receiving authentication information from HA, MU device computes $K_{MU} = h(ID_{MU}||PW_{MU}||R)$, stores $\{K_{MU}, R, C_{MU}, K, h(.)\}$ on his/her mobile device (MD) and sets threshold timeout to ensure the correctness of the authentication information. If the information stored in the device may be altered maliciously or carelessly, MU re-registration is necessary to get the

new authentication information when he/she does not receive HA's response within the predefined time limit.

3.3. Login and Authentication Phase

It is assumed that MU associated with HA visits an FA and tries to access services. The details of this phase are as follows:

A1: MU → FA: $M_1 = \{U, V, W\}$

MU retrieves the authentication related information on the device and inputs ID_{MU} and PW_{MU}. Then, MD computes $K_{MU^*} = h(ID_{MU}||PW_{MU}||R)$ and verifies whether $K_{MU^*} = K_{MU}$ or not. If verification fails, it terminates the session. Otherwise, the legality of MU is ensured. Then, MD chooses a random number R_{MU} and computes $U = R \oplus R_{MU}$, $V = (C_{MU} \oplus h(R)||ID_{FA}) \oplus R_{MU}$ and $W = (U||K||C_{MU} \oplus h(R))$. Finally, MD sends $M_1 = \{U, V, W\}$ to FA.

A2: FA → HA: $M_2 = \{ID_{FA}, E_{KFH}(M_1, R_{FA})\}$

After receiving M_1, FA generates a random number R_{FA} and encrypts the message M_1 with R_{FA}. After that, FA sends $M_2 = \{ID_{FA}, E_{KFH}(M_1, R_{FA})\}$ to HA.

A3: HA → FA: $M_3 = \{E_{KFH}(SK)\}$

Upon receiving the message M_2, HA checks for the identity ID_{FA} and finds the secret key corresponding to ID_{FA}. Then HA decrypts the received information and performs authentication on it. If authentication is successful, HA generates a SK between FA and MU. If verification fails, HA rejects the request. The procedure of authentication performed by HA is as $D_{KFH}(E_{KFH}(M_1, R_{FA}))$, $a = h(d)$, $g^a \bmod p$, $R_{MU^*} = V \oplus ((g^a \bmod p)||ID_{FA})$ and $R^* = U \oplus R_{MU^*}$. HA checks whether R^* exists in its database. If it is not, HA terminates the session. Otherwise, HA computes $W^* = (U||K||(g^a \bmod p))$ and checks whether W^* is equal to W. If the comparison fails, HA terminates the process. Otherwise, HA compute a session key $SK = h(g^a \bmod p) \oplus R_{MU} \oplus R_{FA}$, forms the message $M_3 = \{E_{KFH}(SK)\}$, and sends it to FA.

A4: FA → MU : $M_4 = \{X, R_{FA}\}$

After receiving M_3, FA computes $D_{KFH}(E_{KFH}(SK))$ and $X = h(SK||R_{FA})$ and sends the message $M_4 = \{X, R_{FA}\}$ to MU.

A5: Upon receiving M_4, MD generates a session key $SK^* = C_{MU} \oplus h(R) \oplus R_{MU} \oplus R_{FA}$ and $X^* = h(SK^*||R_{FA})$ and verifies whether X^* is equal to the received X. If the verification fails, MD stops the process. Otherwise, MU successfully authenticates FA.

3.4. Password Change Phase

In this phase, MU can easily change his/her password, which does not need involvement of any FA or HA. The detailed steps of the password change phase are:

P1: If a legal MU wants to change the password, MU inputs his/her identity ID_{MU} and password PW_{MU}. The password change request is submitted through the terminal.

P2: MU's device computes $K_{MU}^{*} = h(ID_{MU}||PW_{MU})$ and verifies whether K_{MU}^{*} is equal to K_{MU}. If verification is successful, the authenticity of MU is ensured. Otherwise, the request is rejected.

P3: MU inputs a new password PW_{MU}^{*} and replaces $K_{MU} = h(ID_{MU}||PW_{MU}^{*})$.

4. CRYPTANALYSIS ON M&S SCHEME

This section shows that the M&S scheme has two design flaws and some security weaknesses against HA masquerading attacks, FA masquerading attacks and MU trace attacks.

4.1. Design Flaw

A cryptographic protocol is a concrete protocol that performs a security related function and applies cryptographic methods. A detailed protocol is recommended to a security protocol, which can be used to implement multiple and interoperable versions of a program [23]. However, since M&S scheme changes a new password improperly at password change phase, it is incomplete, which results to make a legal MU could not use the service anymore. First of all, MU verification requires to compute improper $K_{MU}^{*} = h(ID_{MU}||PW_{MU})$, which should be $K_{MU}^{*} = h(ID_{MU}||PW_{MU}||R)$ as the definition of K_{MU} at R3 in registration phase. Similar to this, new password should be replaced as $K_{MU} = h(ID_{MU}||PW_{MU}^{*}||R)$ not as $K_{MU} = h(ID_{MU}||PW_{MU}^{*})$ at P3.

Furthermore, M&S scheme establishes a wrong session key in MU side because of $SK^{*} = C_{MU} \oplus h(R) \oplus R_{MU} \oplus R_{FA}$ computation at A5 in the login and authentication phase. MU will always reject any legal FA's message $M_4 = \{X, R_{FA}\}$ because it always fails from the verification check of SK^{*}, which is different from FA's computation of SK.

4.2. Security Weaknesses

This subsection shows that M&S scheme in [19] has security problems against HA masquerading attack, FA masquerading attack and MU trace attack.

4.2.1. HA Masquerading Attack

Authenticity of MU in M&S scheme is checked of the possession of (g^a mod p) in the authentication message, which is related with the private key of HA. However, each legal user could know the information. Furthermore, M&S scheme does not provide authenticity check of HA to FA because the format of M_3, which is the combination of two random numbers. That is why there is possibility that FA just accept any message with the same length of M_3 from attacker. This means that M_3 does not provide integrity of the message. Thereby, M&S scheme is weak against HA masquerading attack.

4.2.2. FA Masquerading Attack

Authenticity of FA in M&S scheme is checked by MU focused on X, which uses the session key SK. However, any legal user could be an attacker to perform FA masquerading attack. For the attack, the attacker performs the authenticity check of the smart card and gets the information g^a mod p. (1) After receiving $M_1 = \{U, V, W\}$ from MU, the attacker generates a random number R_{FA^*}, computes $R_{MU^*} = V \oplus ((g^a \bmod p)||ID_{FA})$, $SK = h(g^a \bmod p) \oplus R_{MU^*} \oplus R_{FA^*}$ and $X = h(SK||R_{FA^*})$, and sends $M_4 = \{X, R_{FA^*}\}$ to MU. (2) M_4 could be successfully passed MU's verification check at A5 of the login and authentication phase. Thereby, M&S scheme is weak against FA masquerading attack.

4.2.3. MU Trace Attack

Anonymity and untraceability of MU are based on the amplification of dynamic identity of MU by using the session dependent random number R_{MU} at A1 in the login and authentication phase. However, any legal user could be an attacker to perform FA masquerading attack. For the attack, the attacker performs the authenticity check of the smart card and gets the information g^a mod p. (1) After intercepting $M_1 = \{U, V, W\}$ from MU, the attacker computes $R_{MU^*} = V \oplus ((g^a \bmod p) \| ID_{FA})$. (2) The attacker could remove the session dependent random number from U and by computing $R = U \oplus R_{MU}$ and find out the connectivity between sessions based on R. Thereby, M&S scheme is weak against MU trace attack.

5. PRIVACY-PRESERVING AUTHENTICATION SCHEME

This section proposes a privacy-preserving authentication scheme to overcome the weaknesses of M&S scheme. We need to design a new authentication scheme, which provide integrity check with the other aspects to resist various attacks. The design goals of our authentication scheme are as follows:

- Achieve mutual authentication with the provision of privacy
- Session key establishment fairly
- Resist common security attacks
- Provide user-friendliness of password change
- Achieve computational and communicational efficiency.

The proposed privacy-preserving authentication scheme has four phases, initialization phase, registration phase, login and authentication phase and password change phase. MU registers any specific services to HA in the registration phase by using an amplified identity through secure channel after the proper initialization of the system. Unlike M&S scheme, the proposed scheme does not need to use a verification table in HA, which improves the security of the scheme. The login and authentication phase provides mutual authentication and key agreement among communication parties. In this phase, MU and FA can authenticate each other via HA assistance with proper session key establishment. The password change phase allows MU to update the password only after the proper MU authentication, which does not require HA involvement.

5.1. Initialization Phase

HA selects two prime numbers p and q and a generator g of a finite field in Z_{p^*}. It computes $n = p \times q$ and $\Phi(n) = (p-1) \times (q-1)$. After that, HA chooses an integer e such that $GCD(e, \Phi(n)) = 1$ and $1 < e < \Phi(n)$. Then, HA calculates $d = e^{-1}$ where d is HA's secret key, and $y = g^d$ mod n, where y is the public key. HA keeps $[d, p, q]$ secretly. Furthermore, HA and FA should share a secret key K_{FH} securely.

5.2. Registration Phase

If MU wants to register with its' HA, he/she must send the necessary information through a secure channel as shown in Fig. 2.

R1: A new MU chooses his/her identity ID_{MU} and password PW_{MU}, and generates a random nonce N. Then, MU computes and submits $R_1 = h(ID_{MU} \| N)$ to HA through a secure channel. Note that MU can change N if MU wants to be registered HA again with the same identity ID_{MU}. R_1could be a pseudonym.

R2: Upon receiving R_1, HA computes $R = h(R_1||ID_{HA}||d)$, $B_{MU} = R_1 \oplus h(d)$, $C_{MU} = R \oplus h(d||y)$ and $F_{MU} = R_1 \oplus R$. Then, HA sends $\{B_{MU}, C_{MU}, F_{MU}, h(.)\}$ to MU through secure socket layer.

R3: After receiving authentication information from HA, MU computes $Z_{MU} = F_{MU} \oplus h(ID_{MU}||PW_{MU})$ and $A_{MU} = h(F_{MU})$, and stores $\{B_{MU}, C_{MU}, Z_{MU}, A_{MU}, h(.)\}$ on his/her MD and sets threshold timeout to ensure the correctness of the authentication information. Note that when MU does not receive HA's response in the threshold time, MU should reregister to get the new authentication information, which means that the information stored in the device may be altered maliciously or carelessly.

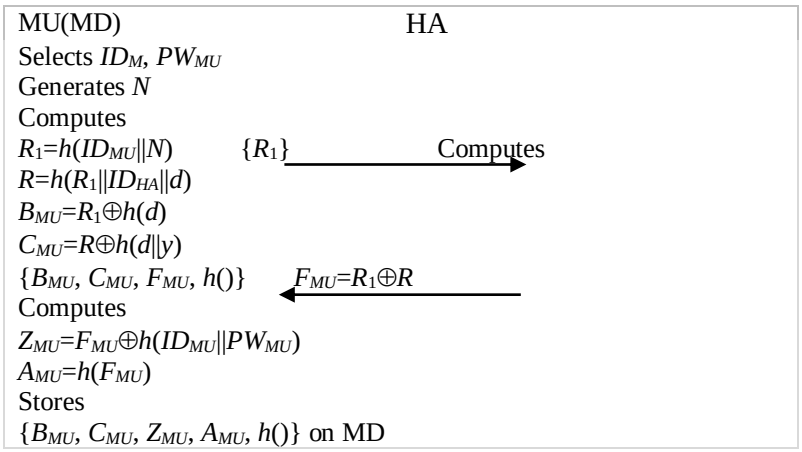

Figure 2. Registration phase of the proposed scheme

5.3. Login and Authentication Phase

It is assumed that MU associated with HA visits an FA and tries to access services. As shown in Fig. 3, the detailed procedure of this phase is as follows:

A1: MU → FA : $M_1 = \{ID_{HA}, U, V, W, MAC_1\}$

MU checks the authentication information on the device and inputs ID_{MU^*} and PW_{MU^*}. Then, MD computes $F_{MU^*} = Z_{MU} \oplus h(ID_{MU^*}||PW_{MU^*})$ and verifies whether $A_{MU} = h(F_{MU^*})$ or not. If verification fails, it terminates the session. Otherwise, the legality of MU is ensured. Then, MD chooses a random number R_{MU} and computes $U = B_{MU} \oplus R_{MU}$, $V = C_{MU} \oplus R_{MU}$, $W = F_{MU^*} \oplus R_{MU}$ and $MAC_1 = h(F_{MU^*}||R_{MU}||U||V||W||ID_{FA})$. Finally, MD sends $M_1 = \{ID_{HA}, U, V, W, MAC_1\}$ to FA.

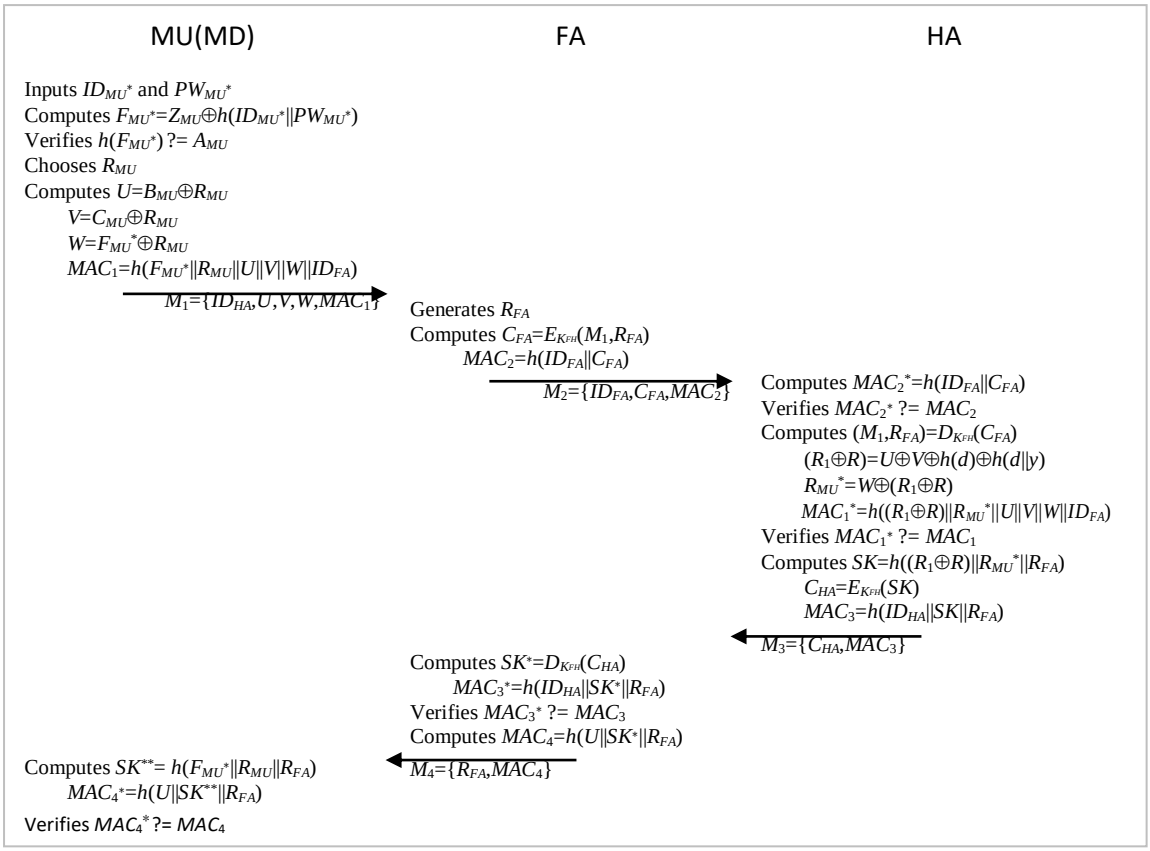

Figure 3. Login and authentication phase of the proposed scheme

A2: FA → HA : $M_2 = \{ID_{FA}, C_{FA}, MAC_2\}$

After receiving M_1, FA generates a random number R_{FA}, encrypts the message M_1 and R_{FA} by using the shared key K_{FH} with HA as $C_{FA} = E_{KFH}(M_1, R_{FA})$ and computes $MAC_2 = h(ID_{FA}||C_{FA})$. After that, FA sends $M_2 = \{ID_{FA}, C_{FA}, MAC_2\}$ to HA.

A3: HA → FA : $M_3 = \{C_{HA}, MAC_3\}$

Upon receiving the message M_2, HA computes $MAC_2^* = h(ID_{FA}||C_{FA})$ and checks whether MAC_2^* is equal to MAC_2. Only if the verification is successful, HA checks for the identity ID_{FA} and finds the secret key corresponding to ID_{FA}. Then HA decrypts the received information as $(M_1, R_{FA}) = D_{KFH}(C_{FA})$. Note that M_1 is $\{ID_{HA}, U, V, W, MAC_1\}$ at A1. After that, HA computes $(R_1\oplus R) = U\oplus V\oplus h(d)\oplus h(d||y)$, $R_{MU^*} = W\oplus(R_1\oplus R)$ and $MAC_1^* = h((R_1\oplus R)||R_{MU^*}||U||V||W||ID_{FA})$. HA verifies whether MAC_1^* is equal to MAC_1. If the comparison fails, HA terminates the process. Otherwise, HA compute a session key $SK = h(R_1\oplus R||R_{MU^*}||R_{FA})$, $C_{HA} = E_{KFH}(SK)$ and $MAC_3 = h(ID_{HA}||SK||R_{FA})$, forms a message $M_3 = \{C_{HA}, MAC_3\}$, and sends it to FA.

A4: FA → MU : $M_4 = \{R_{FA}, MAC_4\}$

After receiving M_3, FA computes $SK^* = D_{KFH}(C_{HA})$ and $MAC_3^* = h(ID_{HA}||SK^*||R_{FA})$ and verifies whether MAC_3^* is equal to MAC_3. If the comparison fails, FA terminates the process. Otherwise, FA compute $MAC_4 = h(U||SK^*||R_{FA})$, forms a message $M_4 = \{R_{FA}, MAC_4\}$, and sends it to MU.

A5: Upon receiving M_4, MD generates a session key $SK^{**} = h(F_{MU^*}||R_{MU}||R_{FA})$ and $MAC_{4^*} = h(U||SK^{**}||R_{FA})$ and verifies whether MAC_{4^*} is equal to the received MAC_4. If the verification fails, MD stops the process. Otherwise, MU successfully authenticates FA.

5.4. Password Change Phase

In this phase, MU can change his/her password alone, which means that there are no communication requirement with FA or its' HA. The detailed steps of the password change phase are:

P1: If a legal MU wants to change the password, MU inputs his/her identity ID_{MU^*} and password PW_{MU^*}. The password change request can be submitted through terminal.

P2: MD computes $F_{MU^*} = Z_{MU} \oplus h(ID_{MU^*}||PW_{MU^*})$ and verifies whether $A_{MU} = h(F_{MU^*})$ or not. If verification is successful, MU authenticity is ensured. Otherwise, the request is rejected.
P3: MD asks MU inputs a new password $PW_{MU^{**}}$ and replaces $Z_{MU} = V_{MU^*} \oplus h(ID_{MU^*}||\ PW_{MU^{**}})$.

6. SECURITY AND PERFORMANCE ANALYSIS

This section performs formal security analysis for the proposed scheme, which is based on BAN logic and ProVerif tool, respectively [20-21]. Informal analysis shows that the proposed scheme solves the security and privacy problems in M&S scheme. After that, we provide performance analysis of the proposed scheme by comparing it with K&S scheme in [18] and M&S scheme in [19].

6.1. Formal Security Analysis

We provide a formal security analysis of the proposed scheme based on the BAN logic and ProVerif tool [20-21]. BAN logic uses axioms to verify message origin, message freshness and trustworthiness of the origin of the message to analyze security schemes [21]. BAN logic uses the following notations in formal security analysis:

- $Q \mid\equiv X$: Principal Q believes the statement X
- $\#(X)$: Formula X is fresh
- $Q \mid\Rightarrow X$: Principal Q has jurisdiction over the statement X
- $Q \triangleleft X$: Principal Q sees the statement X
- $Q \mid\sim X$: Principal Q once said the statement X
- (X, Y): Formula X or Y is one part of the formula (X, Y)
- $\langle P \rangle_Q$: Formula P combined with the formula Q
- $Q \overset{SK}{\leftrightarrow} R$: Principal Q and R may use the shared session key, SK to communicate with each other. SK is good, in that any principal except Q and R, will never discover it.

The following logic rules are used to the proposed scheme to prove that it provides a secure mutual authentication between MU and FA:

1. Message-meaning rule: $\frac{R \mid\equiv R \overset{Y}{\leftrightarrow} S,\ \ R \triangleleft \langle X \rangle_Y}{R \mid\equiv S \mid\sim X}$

2. Nonce-verification rule: $\frac{R \mid\equiv \#(X),\ \ R \mid\equiv S \mid\sim X}{R \mid\equiv S \mid\equiv X}$

3. Jurisdiction rule: $\frac{R|\equiv S|\Rightarrow X,\ \ R|\equiv S|\equiv X}{R|\equiv X}$

4. Freshness rule: $\frac{R|\equiv \#(X)}{R|\equiv \#(X,Y)}$.

To show that the proposed scheme provides secure authentication between MU and FA, we need to achieve the following goals:

Goal 1: MU|≡(MU$\overset{SK}{\leftrightarrow}$FA), Goal 2: FA|≡(FA$\overset{SK}{\leftrightarrow}$MU), Goal 3: MU|≡FA|≡(FA$\overset{SK}{\leftrightarrow}$MU) and Goal 4: FA|≡MU|≡(MU$\overset{SK}{\leftrightarrow}$FA).

Idealized form: The arrangement of the transmitted messages among MU, FA and HA in the proposed scheme to the idealized forms is as follows:

Message 1. MU$\rightarrow$FA: ID_{HA},$<U>_{h(d)}$,$<V>_{h(d||y)}$,$<W>_{h(d||y)}$,$<MAC_1>_{h(d||y)}$
Message 2. FA$\rightarrow$HA: ID_{FA}, $<C_{FA}>_{KFH}$, MAC_2
Message 3. HA$\rightarrow$FA: $<C_{HA}>_{KFH}$, $<MAC_3>_{SK}$
Message 4. FA$\rightarrow$MU: R_{FA}, $<MAC_4>_{SK}$.

Assumptions: The initial assumptions of the proposed scheme are as follows:

A1: MU|≡#(R_{MU})
A2: FA|≡#(R_{FA})
A3: MU|≡(MU$\overset{h(d||y)}{\longleftrightarrow}$HA)
A4: HA|≡(HA$\overset{h(d||y)}{\longleftrightarrow}$MU)
A5: FA|≡(FA$\overset{K_{FH}}{\longleftrightarrow}$HA)
A6: HA|≡(HA$\overset{K_{FH}}{\longleftrightarrow}$FA)
A7: MU|≡FA|$\Rightarrow$MU$\overset{SK}{\leftrightarrow}$FA
A8: FA|≡MU|$\Rightarrow$FA$\overset{SK}{\leftrightarrow}$MU.

Proof: We prove the test goals of the proposed scheme to show the secure authentication and key agreement using the BAN logic rules and the assumptions.

Based on Message 1, we could derive:

Step 1. FA$\triangleleft$(ID_{HA},$<U>_{h(d)}$,$<V>_{h(d||y)}$,$<W>_{h(d||y)}$,$<MAC_1>_{h(d||y)}$)
According to assumption A3 and the message-meaning rule, we get:
Step 2. FA|≡MU|$\sim$(ID_{HA},$<U>_{h(d)}$,$<V>_{h(d||y)}$,$<W>_{h(d||y)}$,$<MAC_1>_{h(d||y)}$)
Based on assumption A1 and the freshness concatenation rule, we get:
Step 3: FA|≡#(ID_{HA},$<U>_{h(d)}$,$<V>_{h(d||y)}$,$<W>_{h(d||y)}$,$<MAC_1>_{h(d||y)}$)
According to Steps 2 and 3 and the nonce verification rule, we get:
Step 4. FA|≡U_i|≡(ID_{HA},$<U>_{h(d)}$,$<V>_{h(d||y)}$,$<W>_{h(d||y)}$,$<MAC_1>_{h(d||y)}$)
Based on Message 2, we derive
Step 5. HA$\triangleleft$(ID_{FA}, $<C_{FA}>_{KFH}$, MAC_2)
According to assumption A3 and the message-meaning rule, we get:
Step 6. HA|≡FA|$\sim$(ID_{FA}, $<C_{FA}>_{KFH}$, MAC_2)

Based on assumption A2 and the freshness concatenation rule, we get:
Step 7: HA|≡#(ID_{FA}, <C_{FA}>$_{KFH}$, MAC_2)
According to Steps 6 and 7 and the nonce verification rule, we get:
Step 8. HA|≡FA|≡(ID_{FA}, <C_{FA}>$_{KFH}$, MAC_2)
According to Step 8, assumptions A4 and A6 and the believe rule, we get:
Step 9. HA|≡FA|≡(FA$\overset{K_{FH}}{\longleftrightarrow}$HA) and HA|≡MU|≡(MU$\overset{h(d||y)}{\longleftrightarrow}$HA)
According to the jurisdiction rule, we get:
Step 10. HA|≡(HA$\overset{K_{FH}}{\longleftrightarrow}$FA) and HA|≡(HA$\overset{h(d||y)}{\longleftrightarrow}$MU)
Based on Message 3, we derive
Step 11. FA◁(<C_{HA}>$_{KFH}$, <MAC_3>$_{SK}$)
According to assumption A5 and the message-meaning rule, we get:
Step 12. FA|≡HA|∼(<C_{HA}>$_{KFH}$, <MAC_3>$_{SK}$)
According to assumptions A1 and A2 and the freshness concatenation rule, we get:
Step 13: FA|≡#(<C_{HA}>$_{KFH}$, <MAC_3>$_{SK}$)
According to Steps 12 and 13 and the nonce verification rule, we get:
Step 14. FA|≡HA|≡(<C_{HA}>$_{KFH}$, <MAC_3>$_{SK}$)
According to Step 14, assumptions A4 and A5 and the believe rule, we get:
Step 15. FA|≡HA|≡(HA$\overset{K_{FH}}{\longleftrightarrow}$FA) and FA|≡HA|≡(HA$\overset{h(d||y)}{\longleftrightarrow}$MU)
According to Steps 13, 14 and 15 and the nonce verification rule, we get:
Step 16. FA|≡HA|≡(HA$\overset{SK}{\leftrightarrow}$FA)
According to assumption A5 and the jurisdiction rule, we get:
Step 17. FA|≡(FA$\overset{SK}{\leftrightarrow}$HA)
According to Steps 2, 3 and 4 and the nonce verification rule, we conclude:
Step 18. FA|≡MU|≡(MU$\overset{SK}{\leftrightarrow}$FA) (Goal 4)
According to assumption A8 and the jurisdiction rule, we get:
Step 19. FA|≡(FA$\overset{SK}{\leftrightarrow}$MU) (Goal 2)
According to Message 4, we could derive
Step 20. MU◁(R_{FA}, <MAC_4>$_{SK}$)
According to assumption A5 and the message-meaning rule, we get:
Step 21. MU|≡FA|∼(R_{FA}, <MAC_4>$_{SK}$)
Based on assumption A2 and the freshness concatenation rule, we get:
Step 22: MU|≡#(R_{FA}, <MAC_4>$_{SK}$)
According to Steps 21 and 22 and the nonce verification rule, we get:
Step 23. MU|≡FA|≡(R_{FA}, <MAC_4>$_{SK}$)
According to Step 23, assumptions A4 and A7 and the believe rule, we get:
Step 24. MU|≡FA|≡(FA$\overset{SK}{\leftrightarrow}$MU) and MU|≡HA|≡(HA$\overset{h(d||y)}{\longleftrightarrow}$MU)
According to Steps 22, 23, and 24 and the nonce verification rule, we get:
Step 25. MU|≡FA|≡(FA$\overset{SK}{\leftrightarrow}$MU) (Goal 3)
According to assumption A8 and the jurisdiction rule, we get:
Step 26. MU|≡(MU$\overset{SK}{\leftrightarrow}$FA) (Goal 1)

According to Steps 19 and 26, the proposed scheme successfully achieves both goals (Goals 1 and 2). Both MU with MD and FA believes that they share a common session key $SK = h(R_1 \oplus R||R_{MU^*}||R_{FA}) = h(F_{MU^*}||R_{MU}||R_{FA})$.

ProVerif text output:

```
Completing equations...
Completing equations...
-- Process 1-- Query inj-event(UFend(t)) ==> inj-event(UFbegin(t)) in process 1
Translating the process into Horn clauses...
Completing...
200 rules inserted. Base: 187 rules (36 with conclusion selected). Queue: 24 rules.
Starting query inj-event(UFend(t)) ==> inj-event(UFbegin(t))
RESULT inj-event(UFend(t)) ==> inj-event(UFbegin(t)) is true.
-- Query inj-event(FUend(t)) ==> inj-event(FUbegin(t)) in process 1
Translating the process into Horn clauses...
Completing...
200 rules inserted. Base: 187 rules (36 with conclusion selected). Queue: 26 rules.
Starting query inj-event(FUend(t)) ==> inj-event(FUbegin(t))
RESULT inj-event(FUend(t)) ==> inj-event(FUbegin(t)) is true.
-- Query not attacker(svalueA[]); not attacker(svalueB[]) in process 1
Translating the process into Horn clauses...
Completing...
200 rules inserted. Base: 188 rules (36 with conclusion selected). Queue: 22 rules.
Starting query not attacker(svalueA[])
RESULT not attacker(svalueA[]) is true.
```

Figure 4. ProVerif results

We validated the security properties of the proposed scheme with a widely used formal verification tool, ProVerif [21]. Fig. 4 shows the proof result from ProVerif. svalueA and svalueB were used to check the security of *SK* in the tool. The results of the queries show that attacker could not get the session key between MU and FA. Fig. 4 shows that there are not found any attack traces for the attacker. Thus, our proposed scheme is secure via formal verification. Also, for more studies, the full code is accessible on Github [24].

6.2. Informal Security Analysis

The Dolev-Yao model is used for the security analysis [25]. We solved the weakness issues in the M&S scheme mentioned in Section 3. Unlike the M&S scheme and K&S scheme, the proposed authentication scheme does not need to consider the stolen verifier attack. Thereby, as shown in Table 2, the proposed authentication scheme provides more secure and efficient properties.

Table 2. Security properties comparison among related schemes

Feature / Scheme	**SP1**	**SP2**	**SP3**	**SP4**	**SP5**
K&S [18]	Yes	Yes	No	No	No
M&S [19]	No	Yes	No	No	No
Proposed	Yes	Yes	Yes	Yes	Yes

SP1: user anonymity, SP2: mutual authentication, SP3: prevention of masquerading attack, SP4: prevention of verifier attack, SP5: prevention of DoS attack.

6.2.1. Providing Mutual Authentication

The proposed authentication scheme uses a challenge-response mechanism together [23]. The goal of the proposed authentication scheme is to provide mutual authentication between MU and FA. However, FA has no way to directly authenticate MU, which requires the help from HA because HA has a credential relationship with MU. HA authenticates MU through U, V, W and MAC_1 by validating the possession of the correct pair of $h(d)$ and $h(d||y)$. Only the attacker with the knowledge of $h(d)$ and $h(d||y)$, at the same time, could have power to masquerade as a legal MU and the same for FA with K_{FH}. Furthermore, MU also authenticates FA based on MAC_4.

Only the legal FA could pass the correct MAC_4 via HA. Furthermore, FA authenticates HA using MAC_3, which only the correct HA could form it based on K_{FH}. Therefore, MU and FA perform the mutual authentication through the assistance of HA since an attacker based on the Dolev-Yao attack model could not masquerade any party in the proposed scheme.

6.2.2. Providing Key Agreement

A fair key agreement scheme uses the principle that the session key contains the contribution of each participant. In our proposed authentication scheme, the session key is derived based on MU's information and FA's session dependent random number, which satisfies the fair session key agreement. MU and FA achieve the key agreement by helping of HA securely since an attacker could not get any important knowledge on the session key in the proposed scheme.

6.2.3. Providing Anonymity of User

Since the wireless network is vulnerable to several attacks and MD's computational power is limited, anonymity is an important issue in authentication scheme design. Anonymity of an individual is the ability to seclude himself/herself or information about himself/herself. The proposed authentication scheme uses pseudonym related variables, U and V, for this purpose. Furthermore, the pseudonyms are dynamically chanced in each session depending on the session dependent random number R_{MU} to provide anonymity. An attacker could not do anything to know the identity of MU in the proposed scheme because of the lack of knowledge on $h(d)$, $h(d||y)$ and R_{MU}.

6.2.4. Prevention of Off-line Identifier and Password Guessing Attack

An attacker based on the Dolev-Yao attack model can achieve the messages, $M_1 = \{ID_{HA}, U, V, W, MAC_1\}$, $M_2 = \{ID_{FA}, C_{FA}, MAC_2\}$, $M_3 = \{C_{HA}, MAC_3\}$ and $M_4 = \{MAC_4, R_{FA}\}$ from the open communication channels. However, it is infeasible to know identifier to the attacker due to the lack of knowledge on $h(d)$, $h(d||y)$ and R_{MU}. Furthermore, MU's pseudonym is updated in each session based on R_{MU}. To perform the password guessing attack, the attacker needs to get MU's MD. Even if the attacker gets MU's MD and withdraws the information $\{B_{MU}, C_{MU}, Z_{MU}, A_{MU}, h(.)\}$ stored on it, the attacker needs to know both of ID_{MU} and PW_{MU} at the same time, which is not feasible. Thereby, the proposed authentication scheme could cope from the identifier and password guessing attack.

6.2.5. Prevention of DoS Attack

The password renewal phase of the proposed authentication scheme provides authenticity check of MU. So, an attacker with the Dolev-Yao attack model could not success for the DoS attack. MU can change his/her password with a new one and update related information on MD securely only after the success of the authorization check. Thereby, the proposed authentication scheme could cope from the DoS attack.

6.2.6. Prevention of Replay Attack

The proposed authentication scheme uses challenge-response mechanism to prevent replay attacks. Random numbers on the challenge-response mechanism could present the freshness of messages. There is no feasibility that attacker could forge the session related random numbers, R_{MU} and R_{FA}, which provide the integrity of messages. Thereby, the proposed authentication scheme could cope from various replay attacks.

6.3. Performance Analysis

This section discusses the performance with the consideration of computational cost and communicational cost of the related authentication schemes. This experiment was performed on a system sing the 64-bits Windows 7, 3.2 GHz processor and 4 GB memory. Visual C++ 2013 was used with Crypto++ library in [26]. We choose secure hash algorithm (SHA)-1 hash, advanced encryption standard (AES)-128 symmetric encryption/decryption and Rivest-Shamir-Adleman (RSA) 1,024 bits operation for the basic cryptographic operations.

The computational analysis is performed by focusing on operations performed by each party within the authentication schemes. So, we focused on the operations conducted by the parties in the network for the computational costs analysis: namely MU, FA and HA. We define the following notations for the analysis of the computational costs.

- T_h: the time to execute a one-way hash operation (0.00032s)
- T_x: the time to execute an XOR operation (0.00001s)
- T_s: the time to compute a symmetric key cryptosystem operation (0.0056s)
- T_e: the time to compute an asymmetric key cryptosystem operation (0.3862s).

Table 3 summarizes the accurate measurement results of related authentication schemes. K&S scheme in [18] requires big computational overhead than two other symmetric cryptography based schemes.

Table 3. Computational overhead comparison

Scheme \ Entity	MU(MD)	FA	HA	Total
K&S [18]	$8T_h+3T_e$ (1.16116s)	$3T_h$ (0.00096s)	$8T_h+3T_s+1T_e$ (0.40556s)	$19T_h+3T_s+4T_e$ (1.56768s)
M&S [19]	$3T_h+5T_x$ (0.00101s)	$1T_h+2T_s$ (0.01152s)	$2T_h+4T_x+2T_s$ (0.01188s)	$6T_h+9T_x+4T_s$ (0.02441s)
Proposed	$5T_h+4T_x$ (0.00276s)	$3T_h+2T_s$ (0.01216s)	$4T_h+4T_x+2T_s$ (0.01252s)	$12T_h+8T_x+4T_s$ (0.02632s)

Note that we removed two hash operations overhead for $h(d)$ and $h(d||y)$ in HA computation in the proposed scheme since they are used as they are for every authentication after the first computation. From Table 3, we could know that the proposed authentication scheme has only 8% more operations than M&S scheme but has better security and privacy than the other scheme. It is mainly to provide ownership check for MD, remove the verification table in HA and add some more good features to the proposed authentication scheme.

The communication overhead is performed in terms of bit-length of each message in the authentication schemes. The length of random number, timestamp, identity and symmetric key operation results are 128 bits, respectively, and the length of hash function and RSA operation is 160 bits and 1024 bits [6]. Table 4 lists the comparison of communication costs among the related schemes. The required communication bits for the schemes are 4,640 bits for K&S scheme in [18], 2,888 bits for M&S scheme in [19] and 1,760 bits for the proposed scheme. Therefore, the proposed scheme minimizes communication costs by 40% compared to M&S scheme in [19].

Table 4. Communicational overhead comparison

Scheme \ Entity	MU(MD)	FA	HA	Total
K&S [18]	1,024+2*160+2*128 (1,600 bits)	1,024+4*160+6*128 (2,432 bits)	3*160+128 (608 bits)	4,640 bits
M&S [19]	2*1,024+160 (2,208 bits)	160+3*128 (544 bits)	128 (128 bits)	2,888 bits
Proposed	4*160+128 (768 bits)	2*160+3*128 (704 bits)	160+128 (288 bits)	1,760 bits

7. CONCLUSION

This paper has been investigated the design of privacy-preserving authentication scheme for roaming services, which is to provide security and privacy at the same time. First of all, we have analyzed the M&S scheme and shown that, the scheme has two design flaws and suffers from HA masquerading attack, FA masquerading attack and MU trace attack. To overcome the problems, we proposed a privacy-preserving authentication scheme. Formal security analysis using BAN logic and the ProVerif tool was provided. From the security analysis, we found that neither the adversary nor the agents can get any information of the mobile user's identity. Compared with other related authentication schemes, the proposed scheme has better security with privacy but gets similar performance with the M&S scheme. As a result, the proposed authentication scheme is more suitable for roaming services in the global mobility networks. However, we found out that there are some computational overheads in the proposed scheme compared to the M&S scheme, which could think as the costs to provide security and privacy.

For the future work, the performance of the proposed scheme will be measured by implementing and conducting experiments over devices on real networks and will improve the proposed scheme based on the trial results. Furthermore, we will investigate more efforts on improving the proposed scheme in the concern of computational.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

[1] Curado, M., Tortosa, L., Vincent, J. F. & Yeghikyan, G., (2021) "Understanding mobility in Rome by means of a multiplex network with data," Journal of Computational Science, 101305.

[2] Cao, J., Li, Q., Tu, W., Gao, Q., Cao, R., & Zhong, C., (2021) "Resolving urban mobility networks from individual travel graphs using massive-scale mobile phone tracking data," Cities, Vol. 110, 103077.

[3] Almalki, F. A., (2021) "Developing an Adaptive Channel Modelling using a Genetic Algorithm Technique to Enhance Aerial Vehicle-to-Everything Wireless Communications," International Journal of Computer Networks & Communications, Vol. 14, No. 2, pp. 37-56.

[4] Zhu, J., & Ma, J., (2004) "A new authentication scheme with anonymity for wireless environment," IEEE Transactions on Consumer Electronics, Vol. 50, No. 1, pp. 231-235.

[5] Wei, F., Vijayakumar, P., Jiang, Q., & Zhang, R., (2018) "A mobile intelligent terminal based anonymous authenticated key exchange protocol for roaming service in global mobility networks," IEEE Transactions on Sustainable Computing, Vol. 14, No. 8, pp. 268-278.

[6] Kapito, B., Nyirenda, M., & Kim, H. (2021) "Privacy-Preserving Machine Authenticated Key Agreement for Internet of Things," International Journal of Computer Networks & Communications, Vol. 14, No. 2, pp. 99-120.

[7] Zhao, D., Peng, H., Li, L., & Yang, Y., (2014) "A secure and effective anonymous authentication scheme for roaming service in global mobility networks," Wireless Personal Communications, Vol. 78, No. 1, pp. 247-269.
[8] Morsi, A. M., Barakat, T. M., & Nashaat, A. A., (2020) "An Efficient and Secure Malicious Node Detection Model for Wireless Sensor Networks," International Journal of Computer Networks & Communications, Vol. 12, No. 1, pp. 97-108.
[9] 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, Vol. 73, No. 3, pp. 993-1004.
[10] 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, Vol. 68, No. 4, pp. 1477-1491.
[11] 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, Vol. 55, No. 1-2, pp. 214-222.
[12] 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, Vol. 53, No. 5, pp. 1683-1687.
[13] Chang, C. C., Lee, C. Y., & Chiu, Y. C., (2009) "Enhanced authentication scheme with anonymity for roaming service in global mobility networks," Computer Communications, Vol. 32, No. 4, pp. 611-618.
[14] Yang, G., Huang, Q., Wong, D. S., & Deng, X., (2010) "Universal authentication protocols for anonymous wireless communications," IEEE Transactions on Wireless Communications, Vol. 9, No. 1, pp. 1536-1276.
[15] Zhou, T., & Xu, J., (2011) "Provable secure authentication protocol with anonymity for roaming service in global mobility networks," Computer Networks, Vol. 55, No. 1, pp. 205-213.
[16] 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, Vol. 19, No. 1, pp. 18-24.
[17] Liu, J. K., Chu, C. K., Chow, C. M., Huang, X., Au, M. H., & Zhou, J., (2015) "Time-bound anonymous authentication for roaming networks," IEEE Transactions on Information Forensics and Security, Vol. 10, No. 1, pp. 178-189.
[18] Karuppiah, M., & Saravanan, R., (2015) "A secure authentication scheme with user anonymity for roaming service in global mobility networks," Wireless Personal Communications, Vol. 84, No. 3, pp. 2055-2078.
[19] Madhusudhan, R., & Shashidhara, (2018) "A secure and lightweight authentication scheme for roaming service in global mobile networks," Journal of Information Security and Applications, Vol. 38, pp. 96-110.
[20] Burrows, M., Abadi, M., & Needham, R., (1989) "A logic of authentication", Royal Society of London Mathematical, Physical and Engineering Sciences, Vol. 426, pp. 233-271.
[21] Blanchet, B., (2013) "Automatic Verification of Security Protocols in the Symbolic Model: The Verifier ProVerif," Lecture Notes in Computer Science, Vol. 8604, pp. 54-87.
[22] Housley, R., Polk, W., Ford, W., & Solo, D., (2002) Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC3280, The Internet Society.
[23] Schineier, B., (2015) Applied Cryptography: Protocols, Algorithms and Source Code in C, John Wiley & Sons Inc.
[24] https://github.com/hs-kim-andre/roaming.git.
[25] Dolev, D., & Yao, A. C., (1983) "On the Security of Public Key Protocols," IEEE Transactions on Information Theory, Vol. IT-29, No. 2, pp. 198-208.
[26] Dai, W., Crypto++ Library, Available online: http://www.cryptopp.com, Accessed on 1 August. 2021.

AUTHORS

Sung Woon Lee received the Ph.D. degree in Computer Engineering from Kyungpook National University, Korea, in 2005. He is a Professor at the Department of Information Security, Tongmyong University, Korea, from 2005. He was a visiting scholar at Georgia State University in 2017. From 1996 to 2000, he had been worked as a program developer at Korea Information System, Daegu, Korea. His research focus is considering how cryptography can be applied to improve the security and privacy of healthcare system's patient information communicated wirelessly in Internet of Things applications. Furthermore, he is interested in database security and privacy.

Hyunsung Kim received the M.Sc. and Ph.D. degrees in computer engineering from Kyungpook National University, Korea, in 1998 and 2002, respectively. He is a Full Professor at the School of Computer Science, Kyungil University, Korea from 2012. Furthermore, he is currently a visiting professor at the Department of Mathematical Sciences, Chancellor College, University of Malawi, Malawi from 2015. He also was a visiting researcher at Dublin City University in 2009. From 2000 to 2002, he had been worked as a senior researcher at Ditto Technology. He had been an associate professor from 2002 to 2012 with the Department of Computer Engineering, Kyungil University. His research interests include cryptography, VLSI, authentication technologies, network security, ubiquitous computing security, and security protocol.