Privacy preserving lightweight authentication scheme for roaming service in global mobile networks

Sungwoon Lee[1], **Hyunsung Kim**[2]
[1]Department of Information System and Security, International College, Tongmyong University, Busan, Korea
[2]Department of Computer Engineering, Graduate School of Engineering, Kyungil University, Kyungsan, Korea

Article Info

Article history:

Received Dec 29, 2023
Revised Apr 24, 2024
Accepted Jun 19, 2024

Keywords:

Authentication
Global roaming
Key agreement
Mobile network
User anonymity

ABSTRACT

The swift advancement of mobile intelligent terminals and services enables users to seamlessly access ubiquitous services across global mobile networks. Ensuring the authentication and safeguarding of the privacy of network entities is crucial. Numerous authentication and privacy schemes have been put forth over time, yet many of them have faced security and privacy challenges. A recent contribution introduces a lightweight authentication scheme (LAS) designed for roaming services within global mobile networks. They assert that their scheme offers user anonymity, mutual authentication, fair key agreement, and user-friendliness, claiming resilience against various attacks in global mobile networks. This paper, however, identifies two design flaws in the LAS and highlights its vulnerability to two masquerading attacks and a mobile user (MU) trace attack. Consequently, we propose a privacy-preserving LAS tailored for global mobile networks. Our analysis demonstrates that the proposed authentication scheme is secure and delivers enhanced privacy with efficient performance.

Corresponding Author:

Hyunsung Kim
Department of Computer Engineering, Graduate School of Engineering, Kyungil University
Gamasilgil 50, Kyungsan, Kyungbuk 38428, Korea
Email: secueye@gmail.com

1. INTRODUCTION

As wireless communication technology and artificial intelligence rapidly advance, mobility becomes increasingly integral to our daily lives. Users equipped with mobile intelligent devices (MD) can partake in a diverse range of seamless services, including online shopping, social network interactions, bank transfers, and various others [1]–[4]. The concept of roaming service allows a mobile user (MU) to access services provided by their home agent (HA) in a foreign agent (FA). In the realm of global mobility networks, user authentication and privacy schemes assume a pivotal role. A secure scheme for roaming services involves three key participants: MU, FA, and HA. MU is required to register with their HA, and when MU ventures into a foreign domain managed by an FA, authentication from the FA, with the assistance of HA, becomes a necessity.

Background: over the years, numerous user authentication and privacy schemes for roaming services have been put forward [5]–[22]. Zhu and Ma introduced the initial anonymous authentication scheme for roaming services, employing hash functions and symmetric encryption cryptosystems [5]. However, Lee *et al*. [15] demonstrated that Zhu and Ma's [5] authentication scheme lacks mutual authentication and is susceptible to impersonation attacks. Subsequently, they proposed an enhanced scheme to address the security vulnerabilities identified in Zhu and Ma’s work [5]. Chang *et al*. [16] highlighted that Lee *et al*. [15] scheme still faces the threat of forgery attacks and presented their refined scheme to mitigate this security weakness. Yang *et al.* [17] proposed a universal anonymous authentication scheme for roaming services that eliminates the need for involvement from the HA agent, resulting in efficient communication. Zhou and Xu [18] discovered that Chang *et al.*'s scheme [16] does not provide user anonymity, risking the exposure of MU's identity and compromising the session key. Meanwhile, Kuo *et al.* [19] suggested an anonymous roaming authentication scheme for mobility networks based on elliptic curves. However, their protocol was criticized for its inefficiency in terms of communicational overhead. Liu *et al.* [20] presented an anonymous authentication protocol supporting time-bound credentials for revocation efficiency using bilinear pairing and thus deemed computationally inefficient. Recently, Karuppiah and Saravanan [21] proposed a secure authentication scheme with user anonymity for roaming services in global mobility networks. They contended that their scheme can safeguard privacy focused on user anonymity and untraceability, claiming resilience against a variety of attacks. However, Madhusudhan and Shashidhara [22] identified security flaws in Karuppiah and Saravanan's scheme [21], including various security and privacy attacks. In response, Madhusudhan and Shashidhara [22] proposed a remedial lightweight authentication scheme (LAS) named as LAS to address these weaknesses.

The problem: various authentication schemes [5]–[22] have been proposed for roaming services on global mobile networks. However, vulnerabilities related to security and privacy continue to be reported in these schemes. Therefore, the development of new, lightweight, secure, and privacy-assured authentication schemes is necessary for the current convergence of diverse networks.

The proposed solution: this paper serves two primary objectives. Firstly, we aim to scrutinize the LAS in [22] and demonstrate that it exhibits two design flaws, vulnerable to a trace attack and two masquerading attacks. To address these issues, we present a privacy-preserving LAS. The security of the proposed scheme will be emphasized, considering various aspects of security attacks. In comparison to other relevant authentication schemes, our proposed authentication scheme achieves enhanced security with privacy while maintaining comparable performance to the LAS [22].

2. REVIEW OF MADHUSUDHAN AND SHASHIDHARA’S AUTHENTICATION SCHEME

In this section, we examine the LAS proposed by Madhusudhan and Shashidhara [22]. It comprises four phases: initialization phase, registration phase, login and authentication phase, and password change phase. The notations employed in this paper are presented in Table 1.

Table 1. Notations

Symbol	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

2.1. Initialization Phase

HA selects p and q, which are prime numbers, and g which is a generator of a finite field in Z_p^*. It performs $n=p\times q$ and $\Phi(n)$, which is an Euler’s totient function value and computed as $(p-1)\times(q-1)$. Subsequently, HA chooses e, an integer, which satisfies $1<e<\Phi(n)$ and $gcd(e, \Phi(n))=1$. d is then calculated as the inverse of e, where d serves as HA’s secret key. Additionally, the public key, y, is determined as $y=g^d$ mod n. HA maintains the secrecy of $[d, p, q]$.

2.2. Registration phase

If MU wishes to register with their HA, they must transmit messages through a secure channel.

- RG1: A newly registered MU selects its identity and password as ID_{MU} and PW_{MU}, and produces a nonce N. Subsequently, MU calculates R_1 using $h(ID_{MU}||N)$ and securely sends it to HA.
- RG2: After receiving R_1, HA determines R by computing $(R_1||ID_{HA}||d)$, calculates a as $h(d)$, and computes C_{MU} as $(g^a \ mod \ p)\oplus h(R)$. HA then sets K to 0 for MU, saves $\{K, R\}$ in its database, and securely sends $\{R, C_{MU}, K, h\ (.)\}$ to MU via a secure socket layer.
- RG3: After obtaining the message from HA, the MU device calculates K_{MU} as $h(ID_{MU}||PW_{MU}||R)$. It then stores $\{K_{MU}, R, C_{MU}, K, h(.)\}$ on the mobile device (MD) and establishes a threshold timeout to verify the accuracy of the message information. If the stored information is altered maliciously or accidentally, MU must reregister to receive new authentication information if HA's response is not received within the threshold time.

2.3. Login and authentication phase

Assuming MU, which is linked to HA, visits an FA and attempts to utilize services, the steps in this phase are as follows:

- LA1: MU begins by accessing the stored data and inputting ID_{MU} and PW_{MU}. MD calculates K_{MU^*} as $h(ID_{MU}||PW_{MU}||R)$ and checks if K_{MU^*} matches K_{MU}. If they do not match, the session is stopped. Otherwise, MU's legitimacy is confirmed. MD then chooses a nonce R_{MU} and calculates U as $R\oplus R_{MU}$, V as $(C_{MU}\oplus h(R)||ID_{FA})\oplus R_{MU}$ and W as $(U||K||C_{MU}\oplus h(R))$. After that, MD transmits $M_1=\{U, V, W\}$ to FA.
- LA2: After receiving M_1, FA creates a nonce R_{FA} and encrypts M_1 using R_{FA}. FA subsequently transmits $M_2=\{ID_{FA}, E_{KFH}(M_1, R_{FA})\}$ to HA.
- LA3: When HA receives M_2, it verifies ID_{FA} and retrieves the associated secret key. HA decrypts the message and performs authentication. If authentication is successful, HA generates an SK for communication between FA and MU. If it fails, HA rejects the login request. The procedure includes decrypting $D_{KFH}(E_{KFH}(M_1, R_{FA}))$ and calculating $a=h(d)$, g^a mod p, $R_{MU^*}= V\oplus((g^a \text{ mod } p)||ID_{FA})$ and $R^*=U\oplus R_{MU^*}$. HA checks the presence of R^* in its database. If absent, the session ends. If it does, HA calculates $W^*=(U||K||(g^a \text{ mod } p))$ and verifies if W^* matches W. If they do not match, the process terminates. Otherwise, HA calculates $SK=h(g^a \text{ mod } p)\oplus R_{MU}\oplus R_{FA}$, creates $M_3=\{E_{KFH}(SK)\}$, and transmits it to FA.
- LA4: Upon receiving M_3, FA decrypts $D_{KFH}(E_{KFH}(SK))$ and calculates $X=h(SK||R_{FA})$, subsequently sending $M_4=\{X, R_{FA}\}$ to MU.
- LA5: When MD receives M_4, it calculates $SK^*=C_{MU}\oplus h(R)\oplus R_{MU}\oplus R_{FA}$ and $X^*=h(SK^*||R_{FA})$. MD then checks if X^* matches X. If they do not match, the process is halted. If they match, MU completes the authentication of FA successfully.

2.4. Password change phase

During this phase, MU has the capability to change its password independently without requiring communication with FA or its HA. The steps involved in the phase are outlined as follows:

- PC1: When an authorized MU wishes to change their password, they enter ID_{MU} and PW_{MU} and submit the password change request via the terminal.
- PC2: MU's device calculates K_{MU}^* as $h(ID_{MU}||PW_{MU})$ and checks if K_{MU}^* matches K_{MU}. Upon successful verification, MU's legitimacy is confirmed; otherwise, the request is denied.
- PC3: MU enters a new password PW_{MU}^* and updates $K_{MU}=h(ID_{MU}||PW_{MU}^*)$, effectively concluding the password change process.

3. CRYPTANALYSIS ON MADHUSUDHAN AND SHASHIDHARA'S AUTHENTICATION SCHEME IN

This section demonstrates that the LAS in [22] exhibits two design flaws and vulnerabilities to security issues. First of all, the LAS scheme in [22] is weak against HA and FA masquerading attacks. Furthermore, it is vulnerable to MU trace attacks.

3.1. Design flaw

A security scheme refers to a specific scheme designed for security-related functions, incorporating cryptographic methods. It should be a detailed scheme capable of implementation in various versions of a program that are interoperable [23]. However, the LAS in [22] introduces improper changes to a new password during the password change phase, rendering it incomplete. This deficiency results in a situation where a legitimate MU cannot access the service. Specifically, the MU verification process involves computing an improper K_{MU}^* as $h(ID_{MU}||PW_{MU})$, whereas it should be calculated using $h(ID_{MU}||PW_{MU}||R)$, as defined in RG3 during the registration phase. Similarly, the replacement of the new password should follow the pattern $K_{MU}=h(ID_{MU}||PW_{MU}^{*}||R)$, not $K_{MU}=h(ID_{MU}||PW_{MU}^{*})$ as stated in P3.

Additionally, the LAS in [22] generates an incorrect session key on the MU side due to the computation SK^{*}, which is computed as $C_{MU}\oplus h(R)\oplus R_{MU}\oplus R_{FA}$ in LA5. Consequently, MU consistently rejects any legitimate FA's message $M_4=\{X, R_{FA}\}$ because it consistently does not pass the verification check for SK^{*}. This discrepancy arises from the difference between MU's and FA's calculation of SK.

3.2. Security weakness

This subsection reveals security vulnerabilities in the LAS proposed in [22], specifically in relation to HA and FA masquerading attacks and MU trace attacks. So, this subsection will provide attack feasibility on it. First of all, we will focus on two masquerading attacks. In addition, we will show one of the privacy weaknesses of the scheme focused on trace attacks.

[HA masquerading attack] within the LAS context in [22], the validity of MU is established by including g^a mod p in the authentication message, which is tied to the HA private key. However, this information is accessible to every legitimate user. Furthermore, the inclusion of nonces in M_3 complicates the authentication process between HA and FA. Consequently, there exists a risk that FA could mistakenly accept any message of the same length as M_3 from an attacker, compromising the integrity of the message. Thus, the LAS in [22] is susceptible to HA masquerading attacks.

[FA masquerading attack] the verification process of FA within the LAS outlined in [22] relies on MU's attention to X, which involves the utilization of SK. Nonetheless, it is worth noting that any legitimate user has the potential to act as an attacker in an FA masquerading attack scenario. Within this context, the intruder is validating the legitimacy of the smart card and gaining access to the value of g^a mod p. Upon intercepting $M_1 = \{U, V, W\}$ from MU, the attacker proceeds by generating a nonce R_{FA}^{*}, computing $R_{MU}^{*}=V\oplus((g^a \bmod p)||ID_{FA})$ and then determining $SK=h(g^a \bmod p)\oplus R_{MU}^{*}\oplus R_{FA}^{*}$ as well as $X=h(SK||R_{FA}^{*})$. Afterward, the attacker transmits $M_4=\{X, R_{FA}^{*}\}$ to MU, successfully bypassing MU's check at LA5. Thus, the LAS in [22] is vulnerable to FA masquerading attacks.

[MU trace attack] in the LAS in [22], maintaining MU's anonymity and preventing traceability are argued to be achieved by leveraging the session-dependent nonce R_{MU} at LA1. Despite this, any legitimate user has the potential to impersonate an attacker in a MU trace attack. Within this context, the attacker is verifying the authenticity of the smart card and gaining access to the details of g^a mod p. Upon intercepting $M_1=\{U, V, W\}$ from MU, the attacker proceeds by calculating R_{MU}^{*} as $V\oplus((g^a \bmod p)||ID_{FA})$. By extracting the nonce from U, the attacker can calculate R as $U\oplus R_{MU}$, enabling them to discern the correlation between sessions using R. This vulnerability means that the LAS in [22] is susceptible to malicious activities such as MU trace attacks.

4. PRIVACY-PRESERVING LIGHTWEIGHT AUTHENTICATION SCHEME

This section introduces a privacy-preserving LAS designed to address the vulnerabilities identified in the LAS. The objective is to develop a new authentication scheme that not only ensures integrity checks but also offers resistance against various attacks. The objectives of our authentication scheme are defined as follows: ensure mutual authentication while safeguarding privacy, establish the session key securely, withstand various attacks such as guessing, lost smart card, and denial of service attacks, ensure ease of use for password changes, and optimize computational and communication efficiency.

This LAS, emphasizing privacy preservation, encompasses four key phases: initialization, registration, login and authentication, and password change. During the registration phase, MU enrolls specific services with HA using an enhanced identity over a secure channel following the system's initial setup. Unlike the LAS, the security of our scheme, which prioritizes privacy, is heightened through the elimination of the verifier table typically found at HA. The phase of login and authentication ensures that both parties authenticate each other and reach a consensus on cryptographic keys necessary for secure communication. HA assists MU and FA in mutual authentication, enabling them to establish an appropriate session key for secure communication. MU is empowered to change their password independently in the password change phase following successful authentication, without HA's direct involvement.

4.1. Initialization phase

HA chooses p and q, which are prime numbers, and selects g, a group generator over a finite field in Z_p^{*}. Subsequently, it calculates n by multiplying p and q and derives $\Phi(n)$. After that, HA chooses two integers, an integer e such that $gcd(e, \Phi(n))=1$ and $1<e<\Phi(n)$ and an integer d such that $d=e^{-1}$. Then, HA calculates $y=g^d \bmod n$, where d becomes the private key for y representing the public key of HA. The parameters [d, p, q] are kept confidential by HA. Additionally, it is essential for HA and FA to securely share a secret key K_{FH}.

4.2. Registration phase

The registration process with HA commences with MU securely transmitting the necessary information through a protected channel. The procedure of this phase unfolds as follows:

- RG1: Upon enrollment, MU first selects ID_{MU} and PW_{MU}, followed by generating a nonce N, then calculating R_1 as $h(ID_{MU}||N)$, forwarding it securely to HA.
- RG2: After receiving R_1, HA calculates R=($R_1||ID_{HA}||d$), $C_{MU}=R_1 \oplus h(d)$, $D_{MU}=R \oplus h(d||y)$ and $V=R_1 \oplus R$ before securely transmitting {C_{MU}, D_{MU}, V, h (.)} to MU via a secure socket layer.
- RG3: Upon receiving {C_{MU}, D_{MU}, V, h (.)}, MU proceeds to computes $K_{MU}=D_{MU} \oplus h(ID_{MU}||PW_{MU})$, $A_{MU}=h(D_{MU})$, $N_{MU}=N \oplus h(ID_{MU}||PW_{MU})$ and $V_{MU}=V \oplus h(ID_{MU}||PW_{MU})$. On their MD, MU maintains {A_{MU}, C_{MU}, K_{MU}, N_{MU}, V_{MU}, h(.)} securely and implements a timeout mechanism to ensure authentication information remains accurate. In the event that stored information on the device is at risk of being altered maliciously or carelessly, MU must initiate a new registration procedure.

4.3. Login and authentication phase

In the scenario where a MU associated with HA visits an FA to access services, the procedural details for this phase, illustrated in Figure 1, unfold as outlined:

- LA1: Initially, MU accesses the stored information on their device and enters ID_{MU} and PW_{MU}. MD calculates $D_{MU}^*=K_{MU} \oplus h(ID_{MU}||PW_{MU})$ and $R_1 \oplus R=V_{MU} \oplus h(ID_{MU}||PW_{MU})$, followed by the validation of A_{MU} = $h(D_{MU}^*)$. In case the verification does not meet the required criteria, the session is ended as a security measure. Otherwise, M's legitimacy is confirmed without any doubts. MD proceeds by choosing a nonce R_{MU}, and then calculates $T=C_{MU} \oplus R_{MU}$, $U=D_{MU} \oplus R_{MU}$, $V=R_1 \oplus R \oplus R_{MU}$ and $W=h(R_1 \oplus R||R_{MU}||T||U||V||ID_{FA})$. MD concludes by transmitting M_1={ID_{HA}, T, U, V, W} to FA.
- LA2: Upon receipt of M_1, FA initiates by generating a nonce R_{FA} and proceeds to encrypt both M_1 and R_{FA} using K_{FH} as $C_{FA}=E_{KFH}(M_1, R_{FA})$ and to compute $X=h(ID_{FA}||C_{FA})$. Afterward, FA dispatches M_2={ID_{FA}, C_{FA}, X} to HA.

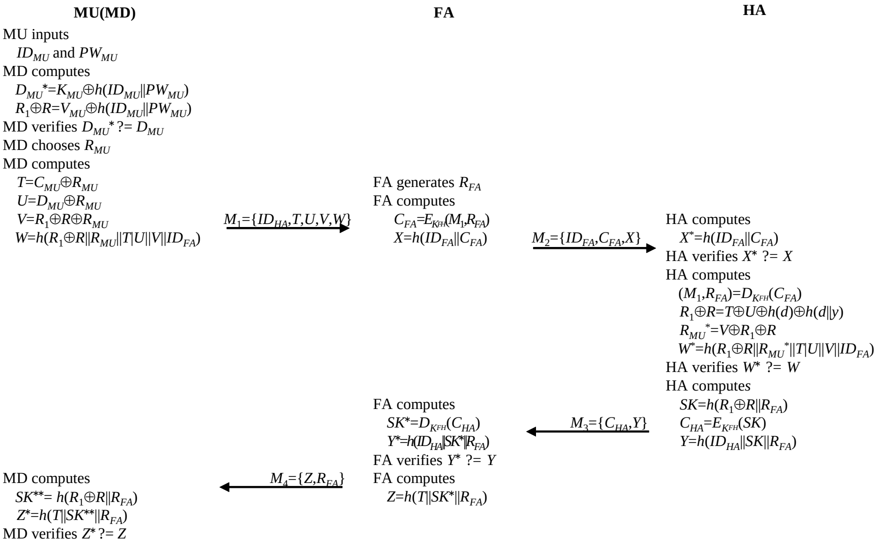
MU(MD)
FA
HA
MU inputs
ID_{MU} and PW_{MU}
MD computes
$D_{MU}^*=K_{MU} \oplus h(ID_{MU}||PW_{MU})$
$R_1 \oplus R=V_{MU} \oplus h(ID_{MU}||PW_{MU})$
MD verifies D_{MU}^* ?= D_{MU}
MD chooses R_{MU}
MD computes
$T=C_{MU} \oplus R_{MU}$
$U=D_{MU} \oplus R_{MU}$
$V=R_1 \oplus R \oplus R_{MU}$
$W=h(R_1 \oplus R||R_{MU}||T|U||V||ID_{FA})$
$M_1=\{ID_{HA},T,U,V,W\}$
FA generates R_{FA}
FA computes
$C_{FA}=E_{KFH}(M_1,R_{FA})$
$X=h(ID_{FA}||C_{FA})$
$M_2=\{ID_{FA},C_{FA},X\}$
HA computes
$X^*=h(ID_{FA}||C_{FA})$
HA verifies X^* ?= X
HA computes
$(M_1,R_{FA})=D_{KFH}(C_{FA})$
$R_1 \oplus R=T \oplus U \oplus h(d) \oplus h(d||y)$
$R_{MU}^*=V \oplus R_1 \oplus R$
$W^*=h(R_1 \oplus R||R_{MU}^*||T|U||V||ID_{FA})$
HA verifies W^* ?= W
HA computes
$SK=h(R_1 \oplus R||R_{FA})$
$C_{HA}=E_{KFH}(SK)$
$Y=h(ID_{HA}||SK||R_{FA})$
$M_3=\{C_{HA},Y\}$
FA computes
$SK^*=D_{KFH}(C_{HA})$
$Y^*=h(ID_{HA}||SK^*||R_{FA})$
FA verifies Y^* ?= Y
FA computes
$Z=h(T||SK^*||R_{FA})$
$M_4=\{Z,R_{FA}\}$
MD computes
$SK^{**}= h(R_1 \oplus R||R_{FA})$
$Z^*=h(T||SK^{**}||R_{FA})$
MD verifies Z^* ?= Z

Figure 1. Login and authentication phase of the proposed authentication scheme

- LA3: After M_2 is received, HA performs a calculation to determine $X^*=h(ID_{FA}||C_{FA})$ and subsequently checks for equality with the originally transmitted X. Upon successful verification, HA then verifies the identity ID_{FA} and retrieves the corresponding secret key. Following this, HA proceeds to decrypt the received information (M_1, R_{FA}), by applying $D_{KFH}(C_{FA})$ and to compute $R_1 \oplus R=T \oplus U \oplus h(d) \oplus h(d||y)$, $R_{MU}^*=V \oplus R_1 \oplus R$ and $W^*=h(R_1 \oplus R||R_{MU}^*||T||U||V||ID_{FA})$. HA ensures data integrity by confirming whether W^* is identical to W through a comparison process. In case of a mismatch, HA promptly halts the ongoing process. Alternatively, HA proceeds by calculating $SK=h(R_1 \oplus R \| R_{FA})$, $C_{HA}=E_{KFH}(SK)$ and $Y=h(ID_{HA} \| SK \| R_{FA})$. HA constructs a message $M_3=\{C_{HA}, Y\}$, which is then forwarded to FA.

- LA4: Upon receipt of M_3, FA proceeds by decrypting $SK^{*}=D_{KFH}(C_{HA})$ and calculating $Y^{*}=h(ID_{HA} \| SK^{*} \| R_{FA})$. After that FA verifies whether Y^{*} is equal to Y. If the validation fails, it terminates the session. Alternatively, FA calculates $Z=h(T \| SK^{*} \| R_{FA})$ and sends $M_4=\{Z, R_{FA}\}$ to MU.
- LA5: After receiving M_4, MD proceeds to compute $SK^{**}=h(R_1 \oplus R \| R_{FA})$ and $Z^{*}=h(T \| SK^{**} \| R_{FA})$ and to verify Z^{*}. If the validation fails, MD finishes the step. Alternatively, authentication between MU and FA is completed.

4.4. Password change phase

In this phase, MU has the autonomy to modify their passwords independently without requiring interaction with FA or their HA. Here is a breakdown of the steps involved in changing the password:

- PC1: When an authorized MU decides to change their password, they enter ID_{MU} and PW_{MU}. The process of changing the password is initiated by submitting a request through a terminal.
- PC2: After computing $D_{MU}{}^{*}=K_{MU} \oplus h(ID_{MU} \| PW_{MU})$, MD confirms if $A_{MU}=h(D_{MU}{}^{*})$. If the verification succeeds, the legality of MU is confirmed. Alternatively, it is rejected.
- PC3: MD prompts MU to input a new password $PW_{MU}{}^{*}$ and updates $K_{MU}=D_{MU} \oplus h(ID_{MU} \| PW_{MU}{}^{*})$, $N_{MU}=N \oplus h(ID_{MU} \| PW_{MU}{}^{*})$ and $V_{MU}=V \oplus h(ID_{MU} \| PW_{MU}{}^{*})$.

5. SECURITY AND PERFORMANCE ANALYSIS

In this section, we analyze the security and performance of the proposed privacy-preserving LAS by conducting a comparison with the authentication schemes presented by Karuppiah and Saravanan [21] and Madhusudhan and Shashidhara [22]. Security analysis is provided based on the Dolev and Yao model [24] with the comparisons among the proposed scheme and the related schemes. Then, performance analysis is provided focused on the computational overhead.

5.1. Security analysis

The security analysis follows the Dolev and Yao model as outlined in [24]. We addressed the vulnerabilities identified in Madhusudhan and Shashidhara [22] authentication scheme, as discussed in section 3. Notably, unlike both Karuppiah and Saravanan [21], and Madhusudhan and Shashidhara [22] authentication schemes, our proposed authentication scheme eliminates the need to address the stolen verifier attack. Consequently, as illustrated in Table 2, the proposed authentication scheme exhibits enhanced security and efficiency characteristics.

Table 2. Security properties between authentication schemes

Scheme	SP1	SP2	SP3	SP4	SP5
Karuppiah and Saravanan [21]	Provide	Provide	No	No	No
Madhusudhan and Shashidhara [22]	No	Provide	No	No	No
Proposed	Provide	Provide	Yes	Yes	Yes

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

[Enabling mutual authentication] within the proposed scheme, mutual authentication between MU and FA is facilitated through the implementation of a challenge-response mechanism [25]. FA lacks a direct means to authenticate MU and relies on the HA, which maintains a credential-based bond with MU. HA verifies MU’s authentication by checking T, U, V, and W against the correct pair of $h(d)$ and $h(d \| y)$. Only an attacker with knowledge of $h(d)$ and $h(d \| y)$ could impersonate a legal MU, and the same applies to FA with K_{FH}. Additionally, MU also authenticates FA with the assistance of HA based on Z. Only a legitimate FA can pass the correct Z through HA. Furthermore, FA authenticates HA based on Y, a value only the correct HA can form using K_{FH}. Consequently, with HA’s assistance, MU and FA achieve mutual authentication, making it challenging for an attacker within the model to masquerade any party in the proposed scheme.

[Facilitating key agreement] the proposed authentication scheme ensures a fair key agreement, where the session key incorporates contributions from each participant. Derived from MU’s data and FA’s session-specific nonce, the session key is established to ensure a balanced agreement. HA facilitates the secure key agreement process between MU and FA, effectively safeguarding the session key from unauthorized access in the proposed scheme.

[Ensuring anonymity of user] in consideration of the vulnerabilities inherent in wireless networks and the limited computational power of MD, user anonymity is a crucial aspect of authentication scheme design. Anonymity involves secluding individual information. The proposed authentication scheme addresses this by utilizing pseudonym-related variables, T and U. Moreover, these pseudonyms undergo dynamic changes in each session, influenced by the session-dependent nonce R_{MU}, ensuring anonymity. The lack of knowledge regarding $h(d)$, $h(d||y)$ and R_{MU} prevents attackers from identifying MU in the proposed scheme, thus ensuring MU’s anonymity.

[Preventing off-line identifier and password guessing attack] even if an attacker intercepts communication messages M_1={ID_{HA}, T, U, V, W}, M_2={ID_{FA}, C_{FA}, X}, M_3={C_{HA}, Y} and M_4={Z, R_{FA}}, it is infeasible for the attacker to deduce identifiers due to the lack of knowledge regarding $h(d)$, $h(d||y)$ and R_{MU}. In addition, MU adjusts its pseudonym for every session, aligning it with RMU to reinforce security measures, making it challenging for the attacker to perform password-guessing attacks. The proposed authentication scheme is robust against both identifier and password-guessing attacks.

[Preventing denial-of-service attack] as part of the proposed scheme’s password renewal phase, MU undergoes an authenticity check to prevent potential denial-of-service attacks. Only after successfully passing the ownership check can MU change the password securely and update related information on MD. Therefore, the proposed authentication scheme effectively mitigates denial-of-service attacks.

[Preventing replay attack] by incorporating a challenge-response mechanism, the proposed scheme enhances security by guarding against replay attacks. The use of nonces ensures the freshness of messages, and it is infeasible for an attacker to forge session-related random numbers, $R_{MU,}$ and R_{FA}, thereby maintaining the integrity of messages. Consequently, the proposed scheme effectively safeguards against various replay attacks.

5.2. Performance analysis

This section explores the performance considerations, taking into account the operation costs associated with relevant authentication schemes. The computational analysis of an authentication scheme typically involves examining the operations conducted by each party involved. Therefore, to assess computational costs, our focus lies on the operations carried out by the network participants, specifically MU, HA, and FA. For clarity in computational cost analysis, we introduce the following notation-T_h: the time for a one-way hash operation, T_x: the time for an XOR operation, T_s: the time for a symmetric key cryptosystem operation and T_e: the time for an asymmetric key cryptosystem operation.

Furthermore, to ensure precision in measurement, we conducted an experiment using the Crypto++ Library on a system featuring a 64-bit Windows 7 operating system, a 3.2 GHz processor, 4 GB memory, Visual C++ 2013 Software, the SHA-1 hash function, the AES symmetric encryption/decryption function, and the RSA encryption/decryption function. The summarized results are presented in Table 3. Table 3 indicates that the proposed scheme involves only five times more operations than the LAS [22], yet it outperforms the other scheme. This performance advantage can be attributed to the inclusion of ownership checks for MD, the elimination of the verification table for HA, and the incorporation of additional positive aspects into the authentication scheme, thereby enhancing security measures.

Table 3. Computational overhead between authentication schemes

Scheme	MU(MD)	FA	HA	Total
Karuppiah and Saravanan [21]	$8T_h+3T_e$	$3T_h$	$8T_h+3T_s+1T_e$	$19T_h+3T_s+4T_e$
Madhusudhan and Shashidhara [22]	$3T_h+5T_x$	$1T_h+2T_s$	$2T_h+4T_x+2T_s$	$6T_h+9T_x+4T_s$
Proposed	$4T_h+5T_x$	$3T_h+2T_s$	$4T_h+4T_x+2T_s$	$11T_h+9T_x+4T_s$

6. CONCLUSION

This paper delves into the development of LASs for roaming services, emphasizing security analysis and robust privacy measures for mobile users. Initially, we scrutinized the LAS, revealing two design flaws and vulnerabilities to HA and FA masquerading attacks, and MU trace attacks. To address these issues, we introduced a privacy-preserving LAS. The security analysis of our proposed scheme thoroughly examines various security attack scenarios, ensuring that neither adversaries nor agents can access any information regarding the mobile user's identity. In comparison to other relevant authentication schemes, our proposed authentication scheme offers superior security with privacy while maintaining similar performance levels to the LAS. Consequently, our proposed authentication scheme emerges as a more fitting solution for roaming services in global mobile networks.

ACKNOWLEDGEMENTS

This work was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2017R1D1A1B04032598).

REFERENCES

[1] M. A. Shaaban, A. S. Alsharkawy, M. T. AbouKreisha, and M. A. Razek, "Efficient ECC-based authentication scheme for fog-based IoT environment," *International journal of Computer Networks & Communications*, vol. 15, no. 04, pp. 55–71, Jul. 2023, doi: 10.5121/ijcnc.2023.15404.

[2] A. A. Alawad, M. T. Chughtai, and M. F. Alanzi, "Internet of things time saving and management system for bus passengers," *International Journal of Advances in Applied Sciences*, vol. 12, no. 2, pp. 171–178, Jun. 2023, doi: 10.11591/ijaas.v12.i2.pp171-178.

[3] S. Kaushal and B. Buksh, "A study secure multi authentication based data classification model in cloud based system," *International Journal of Advances in Applied Sciences*, vol. 9, no. 3, pp. 240–254, Sep. 2020, doi: 10.11591/ijaas.v9.i3.pp240-254.

[4] R. Shashidhara, S. K. Nayak, A. K. Das, and Y. Park, "On the design of lightweight and secure mutual authentication system for global roaming in resource-limited mobility networks," *IEEE Access*, vol. 9, pp. 12879–12895, 2021, doi: 10.1109/ACCESS.2021.3050402.

[5] J. Zhu and J. Ma, "A new authentication scheme with anonymity for wireless environments," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 1, pp. 231–235, Feb. 2004, doi: 10.1109/TCE.2004.1277867.

[6] F. Wei, P. Vijayakumar, Q. Jiang, and R. Zhang, "A mobile intelligent terminal based anonymous authenticated key exchange protocol for roaming service in global mobility networks," *IEEE Transactions on Sustainable Computing*, vol. 5, no. 2, pp. 268–278, Apr. 2020, doi: 10.1109/TSUSC.2018.2817657.

[7] A. Chaudhary, "Utilizing ultra-wideband with wireless telecommunications applications microstrip," *International Journal of Advances in Applied Sciences*, vol. 10, no. 4, pp. 283–287, Dec. 2021, doi: 10.11591/ijaas.v10.i4.pp283-287.

[8] H. Kim, "Enhanced mutual authenticated key agreement protocol for anonymous roaming service in global mobility networks," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 7, 2019, doi: 10.14569/IJACSA.2019.0100735.

[9] K. Mtonga, E. J. Yoon, and H. S. Kim, "Authenticated privacy preserving pairing-based scheme for remote health monitoring systems," *Journal of Information Security*, vol. 08, no. 01, pp. 75–90, 2017, doi: 10.4236/jis.2017.81006.

[10] M. Indushree, M. Raj, V. K. Mishra, R. Shashidhara, A. K. Das, and B. K. Vivekananda, "Mobile-chain: secure blockchain based decentralized authentication system for global roaming in mobility networks," *Computer Communications*, vol. 200, pp. 1–16, Feb. 2023, doi: 10.1016/j.comcom.2022.12.026.

[11] B. T. Ahmed, "A systematic overview of secure image steganography," *International Journal of Advances in Applied Sciences*, vol. 10, no. 2, p. 178, Jun. 2021, doi: 10.11591/ijaas.v10.i2.pp178-187.

[12] J. Ryu, H. Lee, Y. Lee, and D. Won, "SMASG: secure mobile authentication scheme for global mobility network," *IEEE Access*, vol. 10, pp. 26907–26919, 2022, doi: 10.1109/ACCESS.2022.3157871.

[13] Q. Jiang, J. Ma, G. Li, and L. Yang, "An enhanced authentication scheme with privacy preservation for roaming service in global mobility networks," *Wireless Personal Communications*, vol. 68, no. 4, pp. 1477–1491, Feb. 2013, doi: 10.1007/s11277-012-0535-4.

[14] H. Mun, K. Han, Y. S. Lee, C. Y. Yeun, and H. H. Choi, "Enhanced secure anonymous authentication scheme for roaming service in global mobility networks," *Mathematical and Computer Modelling*, vol. 55, no. 1–2, pp. 214–222, Jan. 2012, doi: 10.1016/j.mcm.2011.04.036.

[15] C.-C. Lee, M.-S. Hwang, and I.-E. Liao, "Security enhancement on a new authentication scheme with anonymity for wireless environments," *IEEE Transactions on Industrial Electronics*, vol. 53, no. 5, pp. 1683–1687, Oct. 2006, doi: 10.1109/TIE.2006.881998.

[16] C.-C. Chang, C.-Y. Lee, and Y.-C. Chiu, "Enhanced authentication scheme with anonymity for roaming service in global mobility networks," *Computer Communications*, vol. 32, no. 4, pp. 611–618, Mar. 2009, doi: 10.1016/j.comcom.2008.11.032.

[17] G. Yang, Q. Huang, D. S. Wong, and X. Deng, "Universal authentication protocols for anonymous wireless communications," *IEEE Transactions on Wireless Communications*, vol. 9, no. 1, pp. 168–174, Jan. 2010, doi: 10.1109/TWC.2010.01.081219.

[18] T. Zhou and J. Xu, "Provable secure authentication protocol with anonymity for roaming service in global mobility networks," *Computer Networks*, vol. 55, no. 1, pp. 205–213, Jan. 2011, doi: 10.1016/j.comnet.2010.08.008.

[19] W.-C. Kuo, H.-J. Wei, and J.-C. Cheng, "An efficient and secure anonymous mobility network authentication scheme," *Journal of Information Security and Applications*, vol. 19, no. 1, pp. 18–24, Feb. 2014, doi: 10.1016/j.jisa.2013.12.002.

[20] J. K. Liu, C.-K. Chu, S. S. M. Chow, X. Huang, M. H. Au, and J. Zhou, "Time-bound anonymous authentication for roaming networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 1, pp. 178–189, Jan. 2015, doi: 10.1109/TIFS.2014.2366300.

[21] M. Karuppiah and R. Saravanan, "A secure authentication scheme with user anonymity for roaming service in global mobility networks," *Wireless Personal Communications*, vol. 84, no. 3, pp. 2055–2078, Oct. 2015, doi: 10.1007/s11277-015-2524-x.

[22] R. Madhusudhan and Shashidhara, "A secure and lightweight authentication scheme for roaming service in global mobile networks," *Journal of Information Security and Applications*, vol. 38, pp. 96–110, Feb. 2018, doi: 10.1016/j.jisa.2017.12.002.

[23] B. A. Chiphiko and H. Kim, "Machine to machine authenticated key agreement with forward secrecy for internet of things," *International journal of Computer Networks & Communications*, vol. 15, no. 6, pp. 27–53, Nov. 2023, doi: 10.5121/ijcnc.2023.15602.

[24] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, Mar. 1983, doi: 10.1109/TIT.1983.1056650.

[25] J. Son, S. Noh, J. Choi, and H. Yoon, "A practical challenge-response authentication mechanism for a Programmable Logic Controller control system with one-time password in nuclear power plants," *Nuclear Engineering and Technology*, vol. 51, no. 7, pp. 1791–1798, Oct. 2019, doi: 10.1016/j.net.2019.05.012.

BIOGRAPHIES OF AUTHORS

Sungwoon Lee is a professor at the Department of Information Systems and Security, International College, Tongmyong University, Korea. He received the B.S. and M.S. degrees in Computer Science from Chonnam National University, Korea in 1994 and 1996, respectively, and the Ph.D. degree in Computer Engineering from Kyungpook National University, Korea, in 2005. He was with the Korea Information System as a researcher, in Korea, from 1996 to 2000. His research interests include cryptography, network security, and security protocol. He can be contacted at email: staroun@tu.ac.kr.

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