Journal of Communication Engineering (JCE)

P- ISSN: 2322-4088 Vol. 11, No. 2, Jul.-Dec. 2022 E- ISSN: 2322-3936

A Forward-Secure Authentication Scheme for Global Mobility Network

M. Abd Ali Mohammed Al-Shuwkuh Department of Electrical Engineering; SR.C.; Islamic Azad University; Tehran, Iran;
Email: monafabdali57@gmail.com

M. Rajabzadeh Asaar* **[Corresponding Author]** Department of Electrical Engineering; SR.C.; Islamic Azad University; Tehran, Iran;
Email: m.r.asaar@iau.ir

Received: *05 Jun. 2022* ***Revised:*** *14 Aug. 2022* ***Accepted:*** *17 Oct. 2022*

Abstract: Services presented on mobile devices have been prompted with development of Internet of Things (IoT). The Global Mobility Network (GLOMONET) is a network which provides access to the Internet for mobile users from everywhere, and it is important to provide security and authentication of mobile devices at communications. A secure authentication protocol named as secure mobile authentication scheme for global mobility network (SMASG) in 2022 was presented by Ryu et al. However, we show that SMASG has some vulnerability that threatens its security. First, it is shown that it is not forward secure in a way that if long-term secret keys of entities are exposed, session keys are obtained. Second, it is not secure against known session-specific temporary information attack and subsequently it is vulnerable against mobile user impersonation attack. In this research, these vulnerabilities are presented and a modified authentication scheme named as modified-SMASG (m-SMASG) is proposed. Then, informal and formal security analysis using BAN Logic are given to show that the proposal is secure, and also its performance analysis is presented in the comparison section to show that it has a reasonable communication and computation overhead compared to the baseline papers. It should be highlighted that m-SMASG is the first proposal satisfies perfect forward secrecy in GLOMONET, while computation and communication costs are increased.

Index Terms: Global Mobility Network, Authentication, Internet of Things.

Citation: M. A. A. M. Al-Shuwkuh and M. Rajabzadeh Asaar, "A Forward-Secure Authentication Scheme for Global Mobility Network," *Journal of Communication Engineering*, vol. 11, no. 2, pp. 261-280, Jul.-Dec. 2022.
http://dx.doi.org/10.22070/jce.2025.19055.1268

I. INTRODUCTION

Rapid development of Internet of Things (IoT) makes mobile devices have access to the network, and so communication form everywhere is possible [1, 2]. Hence users can use various services even if travel to another country. As a consequence, users have access to the network in a secure way through global mobility network (GLOMONET) [3–11], and eligible mobile users can have global roaming services. However, several securities are such as privacy of a user have risen [11–14]. Mobile users (MU), Home Agents (HA) and Foreign Agents (FA) are entities of Global Mobility Network (GLOMONET) such that a mobile user MU has to register at the Home Agent (HA). When MU is not in the coverage area of the HA, and also tends to have access roaming services, MU sends it authentication request to the FA. Next, FA transfers this request to HA, and an authentication process is performed between HA, MU and FA to guarantee privacy and security. Authentication protocols must provide user anonymity and privacy, forward secrecy and security against replay attack. Various protocols for authentication in roaming services have been proposed since roaming security is vital. In 2018, Xu et al. [9] showed that the scheme of [8] is not secure against de-synchronization and replay attack, and gave a lightweight authentication scheme. In 2020, Shashidhara et al. [10] showed that the scheme [9] presented by Xu et al. is not secure against impersonation, denial of service and stolen verifier attack, and proposed an improved scheme for mobility networks. In 2021, Rahmani et al. [11] proved that their scheme is not secure against user traceability, impersonation and stolen smart card attack, and improved such that it was secure against aforementioned vulnerabilities. In 2022, Ryu et al. [15] proved that the scheme presented by Rahmani et al. [11] suffers from password guessing attack and also the derivation of session key by external attackers, and then a secure three-factor authentication scheme to be secure against the aforementioned vulnerabilities was presented.

A. OUR CONTRIBUTION

The major contributions of this paper are listed as follows.

- ◇ We analyze SMASG [15] and show that it is not only forward secure, but also it not secure against known- session-specific temporary information and user impersonation attack. Then, a three-factor authentication protocol is proposed which it tackles the aforementioned weaknesses. For this purpose, some secret parameters of mobile users are updated, and it is the most important feature of the m-SMASG scheme.
- ◇ In the formal security analyses, we prove that m-SMASG accomplishes session key security by using Burrow- Abadi-Needham (BAN) logic. In addition, the informal security analyses prove that our protocol is secure against various kinds of known attacks such as user impersonation

attack and also it provides forward secrecy.

◇ Then, the evaluation of our protocol in terms of security features and communication and computation over- heads are given, and we compare the results with other schemes to show that not only m-SMASG can satisfy the necessary security and usability features of IoT-based applications but also it has an acceptable communication and computation costs.

B. RELATED WORK

Mobile authentication is the most important challenge for services presented on mobile devices. Suzuki and Nakada [16] in 1997 proposed an authentication scheme in which a home agent is authenticated by a foreign agent on GLOMONET. In 2004, Zhu and *Ma* [4] gave a smart card-based authentication scheme for roaming services, and unfortunately, it was shown that their scheme does not have backward security and security against impersonation attack, and it was improved by Lee et al. [5] in 2006. Wu et al. [17] in 2008 proved that the scheme presented by Lee et al. [5] cannot provide back-ward secrecy and user anonymity, and proposed a new scheme. Security weaknesses of the scheme given by *Wu* et al. [17] were presented by Mun et al. [18] which they are violating forward secrecy, password leakage and and user anonymity. Then, an Elliptic Curve Cryptography (ECC)-based modified scheme was given by Wu et al. [17] to tackle these vulnerabilities. In 2014, Zhao et al. [19] proved that Wu et al. scheme has some vulnerabilities such as user impersonation, lack of mutual authentication and lack of user-friendliness. In 2011, Yoon et al. [20] gave a new authentication scheme to be resistant against the aforementioned weaknesses. In 2012, He et al. [21] also presented a lightweight authentication protocol employing hash functions and XOR operations. Although, their protocol has some vulnerabilities such as user impersonation and user traceability [22] which these weaknesses are given by Li et al. [22]. Similarly, Jiang et al. [23] in 2013 gave a anonymous authentication protocol which Wen et al. [24] showed that it is not resistant against replay and spoofing attacks, and gave a modified scheme. In 2016, a lightweight authentication protocol was introduced by Gope and Hwang [25], where it suffers from de-synchronization attack and it is impractical. Niu et al. [26] showed that Yoon et al. scheme [20] does not have users' anonymity, and also its key management system has some vulnerabilities in 2014. Then, Niu et al. [26] also presented a secure authentication scheme based on elliptic curve cryptography (ECC). Independently in 2017, Li et al. [27] and Chen and Peng [28] proposed authentication schemes using ECC. Currently lightweight authentication schemes that only use hash functions and XoR operations are proposed by Chang et al. [29] and Mun et al. [18]. In 2016, Gope et al. [30] showed that the proposed lightweight schemes [18, 29] are not secure. Similarly, Lee et al. [31] showed the Mun et al.'s scheme [18] is insecure against impersonation and

man-in-the-middle attacks, and also it is not forward secure. Then, they gave a new scheme that is vulnerable against denial-of-service attack in registration phase [18]. To tackle these weaknesses, Baig et al. [32] in 2018 gave a new scheme which is lightweight. In 2021, Kang et al. [33] showed that their scheme [32] does not meet user privacy, and proposed a modified scheme to provide user privacy and untrace ability and also security against password or identity guessing attacks. After that, various authentication schemes [34–38] using blockchain have been presented. Furthermore, numerous protocols [39–48] which are not efficient have been presented. In 2018, Xu et al. [9] showed that the scheme of [8] is not secure against de-synchronization and replay attack, and gave a lightweight authentication scheme. In 2020, Shashidhara et al. [10] showed that the scheme [9] presented by Xu et al. is not secure against impersonation, denial of service and stolen verifier attack, and proposed an improved scheme for mobility net- works. In 2021, Rahmani et al. [11] proved that their scheme is not secure against user traceability, impersonation and stolen smart card attack, and improved such that it was secure against aforementioned vulnerabilities. In 2022, Ryu et al. [15] proved that the scheme presented by Rahmani et al. [11] suffers from password guessing attack and also the derivation of session key by external attackers, and then a secure three-factor authentication scheme was given to be secure against the aforementioned vulnerabilities. In 2023, Roy and Bhattacharya [49] presented an ECC-based authentication protocol with a conditional privacy for FAs and MUs such that just HA can find their real identities from one-time pseudo identities. However, it is shown that this protocol cannot provide conditional privacy and anonymity for FAs and Mus, and also suffers from mobile user impersonation and foreign agent impersonation attacks. In 2024, Sadhukhan et al. [50] proposed an efficient authentication protocol which cannot support perfect forward secrecy. In 2025, E.H. Nurkifli [51] gave an authentication protocol leveraging biometrics and PUF, and claimed that it is secure candidate for GLOMONET; however, it not only is not efficient due to the employing PUF, but it does not meet perfect forward secrecy.

C. ORGANIZATION OF THE PAPER

The rest of this paper is organized as follows. Section II presents background information including system and adversary model used in the paper. In Section III and IV, Ryu et al.'s scheme and its security analysis is given. Then, the modified protocol and its security analysis are presented in Section V, VI and VII. Sections VIII and VIIII present the performance analysis and conclusion, respectively.

II. PRELIMINARES

A. SYSTEM MODEL

The communication system model of this paper is based on the used model in [15]. According to this model, there are three entities: the mobile user (MU), the home agent (HA), and the foreign agent (FA). The execution flow of the communication system model is as follows.

(1) The MU is registered by HA, and sends an authentication request through a public channel to FA(2) The FA receives the authentication request from MU, and sends it to HA.(3) The HA checks the correctness of the received message and sends a message and session key to FA using the public channel, and FA transfers a message to MU.(4) The MU establishes a session after it receives the message.

B. ADVERSARY MODEL

In this subsection, the following capabilities for adversaries are considered. (1) The adversary *A* can eavesdrop all messages exchanged between HA, FA and MUs on public channels. (2) The adversary *A* can extract all stored parameters of MU's smart card by doing side-channel attack. (3) The adversary *A* can extract all stored parameters of the HA's database, but at that time, it cannot access the user's smart card and a sensor's secret parameters.

C. SECURITY GOALS

In this subsection, the most important security requirements of GLOMONET are listed in the following.

- ◇ **Synchronization.** All three parties must be synchronized with each other.
- ◇ **Forward security.** The mobile user authentication is forward secure if long-term secret keys of entities are exposed to an attacker, session secret keys has not been accessed by the adversary.
- ◇ **No secret value table.** Entities HA and FA should not have tables including vital secret values for mobile users**.**
- ◇ **Efficiency.** The authentication scheme should have low computation and communication cost t be implemented on mobile devices effectively.
- ◇ **User anonymity.** Mobile users MU has to be anonymous in a way their identities is not revealed by adversaries.

D. NOTATIONS

In this subsection, notations are used throughout the paper, will be introduced in Table 1.

Table 1. Notations

Notation	Description
ID_M	Identity of mobile user (MU)
ID_H	Identity of home agent (HA)
PW_M	Password of mobile user (MU)
Bio_M	Biometric information of MU
SK_{H1}, SK_{H2}	Secret keys of HA
SK_F	Secret key of FA
r_M, v	Random numbers selected by MU
r_F, u	Random numbers selected by FA
r_H, w_M, z	Random numbers selected by HA
$GEN()$.	Probabilistic reproduction function
$REP()$.	Deterministic reproduction function
P	The generator of $\mathbb{G}$
q	The order of the group $\mathbb{G}$
$h()$.	One-way hash function
$\|x\|$	The size of the element of x
$\oplus$	XOR operation

III. REVIEW OF RYU ET AL' S SCHEME

In this section, first details of Ryu et al.'s scheme [15] are given. Then, it is shown that it has some security vulnerabilities.

A. MOBILE USER REGISTRATION PHASE

For mobile user registration, MU and HA do the following steps through a secure channel which are given.

- ◇ **Step I.** The MU enters ID_M, password PW_M and Bio_M when it inserts the smart card. It generates $(P, Q)=GEN(Bio_M)$. Then, it computes $L_1= h(ID_M, PW_M, P)$, $RID_M=h(ID_M, P)$, $PID_M=h(PW_M, ID_M)$, and sends PID_M to HA.
- ◇ **Step II.** The HA selects a random number w_M, calculates $HID_M= h(w_M, SK_{H1}, SK_{H2})$, and stores (w_M, PID_M) in its database, and sends HID_M to MU.
- ◇ **Step III.** The MU computes $Tag=h(L_1, HID_M)$ and $TID_M=HID_M \oplus RID_M$, and stores $(Q, h(),. REP, TID_M, Tag_M)$ into the smart card, and deletes HID_M.

B. LOGIN AND AUTHENTICATION PHASE

In this phase, a mobile user MU, a foreign agent FA and a home agent HA authenticates each other, and a session key between these entities will be generated, where the details are described in what follows.

- ◇ Step I. To login, a mobile user inputs its identity ID_M, password PW_M and biometric data Bio_M into its smart card, and it calculates $P = REP(\text{Bio}_M, Q)$, $L_1 = h(ID_M, PW_M, P)$, $RID_M^* = h(ID_M, P)$, $PID_M^* = h(ID_M, PW_M)$, $HID_M^* = TID_M \oplus RID_M$ and $\text{Tag}_M^* = h(L_1^*, HID_M^*)$, and checks if Tag_M^* is equal to Tag_M. If the equality holds, the smart card retrieves a time stamp T_M, and selects a random number x_M, and computes $B_1 = h(HID_M, T_M) \oplus x_M$, and sends m_1= $m_1 = \{B_1, ID_H, T_M\}$ to FA.
- ◇ Step II. The FA checks freshness of T_M. If it is not fresh, FA rejects the message m_1; otherwise, FA extracts timestamp T_{F1}, selects a random number x_F, and it calculates B_2=$h(B_1, ID_H, T_M, T_{F1}, SK_F) \oplus x_F$ and B_3=$h(B_2, x_F)$, and sends $m_2 = \{B_1, B_2, B_3, T_M, T_{F1}\}$ to HA.
- ◇ Step III. The HA checks freshness of T_{F1}. If T_{F1} is not fresh, it rejects m_2; otherwise, it computes SK_F=$h(ID_F, SK_H)$, $x_F = B_2 \oplus h(B_1, ID_H, T_M, T_{F1}, SK_F)$, and checks if $B_3^* = h(B_2, x_F)$ is equal to B_3. If so, HA computes D_M= $h(w_M, SK_{H1}, SK_{H2})$, and then $x_M = B_1 \oplus h(HID_M, T_M)$. Next, HA extracts a timestamp T_H, and generates a random numbers x_H, and computes $B_4 = x_F \oplus x_H$, B_5=$h(B_4, x_M, x_H, T_H, HID_M)$, B_6=$h(x_M, T_H)$ and B_7=$x_M \oplus x_H$, and then sends m_3=$\{B_4, B_5, B_6, B_7, T_H\}$ to FA.
- ◇ Step IV. The FA checks the validity of T_H. If it is valid, it computes $B_6^* = H(x_F, T_H)$, and checks if B_6^* is equal to B_6. If so, it computes $x_H = B_4 \oplus x_F$ and $x_M = B_7 \oplus x_H$, and $SK = h(x_M, x_F, x_H)$, and sends $m_4 = \{B_4, B_5, B_7, T_{F2}, T_H\}$ to MU.
- ◇ Step V. The MU verifies the validity of T_{F2}. If it is valid, it calculates $x_H = B_7 \oplus x_M$, $x_F = B_4 \oplus x_H$ and $B_5^* = h(B4, x_M, x_H, T_H, HID_M)$, and checks the equality of B_5^* and B_5. If the quality holds, the session key $SK = h(x_M, x_F, x_H)$ is computed.

IV. SECURITY ANALYSIS OF RYU ET AL 'S SCHEME

In this section, it will be shown that Ryu et al. scheme [15] is not forward secure and also it is not secure against known session-specific temporary information attack. Furthermore, we show that if known session-specific temporary information attack is done, the protocol is not secure against mobile user impersonation attack, where details of these attacks are given in the following.

A. FORWARD SECURITY

If long-term secret key of HA, SK_H is compromised, an adversary can compute long-term secret key

of FA, $SK_F = h(ID_F, SK_H)$. Next, it can obtain x_F from the relation $x_F = B_2 \oplus h(B_1, ID_H, T_M, T_{F1}, SK_F)$, and it can attain x_H and x_M from $x_H = B_4 \oplus x_F$ and $x_M = B_7 \oplus x_H$, respectively. Hence, the adversary can compute the session key, $SK = h(x_M, x_F, x_H)$. As a consequence, an adversary can extract session key SK with having long-term secret key of HA and other parameters (B_2, B_4, B_7, T_M, T_F) used in the attack have been obtained by eavesdropping public channel. Therefore, this protocol is not forward secure.

B. KNOWN SESSION-SPECIFIC TEMPORARY INFORMATION ATTACK

The proposed protocol is not secure against known session-specific temporary information attack in a way that if x_M, x_F and x_H are known by the adversary, not only session key is obtained, but also an adversary can find HID_M from the relation $B_1 \oplus x_M = h(HID_M, T_M)$ since HID_M is fixed in all sessions and is not changed. Hence, an adversary with the following steps can obtain HID_M

- ◇ Step I. The adversary with having x_M and eavesdropping B_1 and T_M from public channel can find $x = B_1 \oplus x_M$.
- ◇ Step II. Then, the adversary chooses HID_M^A, and computes $x^A = h(HID_M^A, T_M)$.
- ◇ Step III. Next, the adversary checks if x^A is equal to x. If the equality holds, it finds correct HID_M^A; otherwise, it repeats Step 2 and Step 3.

In this attack, it is required to compute one hash value, so the time-complexity can be reduced by use of trade-off methods such as rainbow table [52]. It should be noted that this attack will be successful since the value of HID_M is fixed in different sessions.

C. MOBILE USER IMPERSONATION ATTACK

In this attack, an adversary can impersonate a mobile user with having HID_M which is obtained by known session-specific temporary attack IV. For this purpose, it as to generate message m_1 in form of $\{B_1, ID_{HA}, T_M\}$, where $B_1 = h(HID_M, T_M) \oplus x'_M$ and x'_M is selected randomly by the adversary. Consequently, Ryu et al.'s scheme loes not have security against impersonation attack, and the main reason for this attack is that the value of HID_M is not changed in all sessions.

V. OUR PROPOSED PROTOCOL

In this section, a modified scheme for SMASG [15] named as m-SMASG is given, where its details are given.

A. MOBILE USER REGISTRATION PHASE: THIS PHASE IS THE SAME AS THE ONE IN RYU ET AL.'S SCHEME.

- ◇ Step I. This step is the same as Step 1 of Ryu et al.'s scheme.

◇ Step II. The HA chooses w_M, and calculates $HID_M = h(w_M, SK_H)$, and $Ew_M = (w_M, PID_M) \oplus (h(SK_{H1}))$, $h(SK_{H2})$, and stores (Ew_M, PID_M) in its database, and sends HID_M to MU.

◇ Step III. This step is the same as Step 3 of Ryu et al.'s scheme.

B. LOGIN AND AUTHENTICATION PHASE: THE AUTHENTICATION BETWEEN MU, FA AND HA IS DONE, WHERE THE DETAILS ARE DESCRIBED IN WHAT FOLLOWS.

◇ Step I. A mobile user MU enters ID_M, PW_M and Bio_M into its smart card. Then, it calculates $P = REP(B_M, Q)$, $L_1 = h(ID_M, PW_M, P)$, $RID_M^* = h(ID_M, P), PID_M^* = h(ID_M, PW_M), HID_M^* = = TID_M \oplus RID_M$ and $g_M^* = h(L_1^*, HID_M^*)$, and checks if Tag_M^* is equal to Tag_M. If the equality holds, the smart card retrieves a time stamp T_1, and generates two random numbers r_M and v, and computes $A_1 = h(HID_M, T_1) \oplus (r_M, C_1)$ and $C_1 = vP$, and sends $m_1 = \{A_1, ID_H, T_1\}$ to FA.

◇ Step II. The FA checks freshness of T_1. If it is not fresh, FA rejects the message m_1; otherwise, FA extracts timestamp T_2, and generates random numbers r_F and u, and it calculates $C_2 = uP$, and $A_2 = h(A_1, ID_H, T_1, T_2, SK_F, C_2) \oplus r_F$ and $A_3 = \mathrm{h}(A_2, r_F)$, and sends $m_2 = \{A_1, A_2, A_3, T_1, T_2, C_1, C_2\}$ to HA.

◇ Step III. The HA checks freshness of T_2. If T_2 is not fresh, it rejects m_2; otherwise, it computes $SK_F = h(ID_F, SK_H)$, $r_F = A_2 \oplus h(A_1, ID_H, T_1, T_2, SK_F, C_1, C_2)$, and checks if $A_3^* = h(A_2, r_F)$ is equal to A_3. If so, HA computes $HID_M = h(w_M, SK_H)$, and then $(r_M, C_1) = A_1 \oplus h(HID_M, T_1)$. Next, HA extracts a timestamp T_3, and generates three random numbers r_H, z and w_M^{new}, calculates $(w_M, PID_M) = Ew_M \oplus (h(SK_{H1}), h(SK_{H2}))$, and computes $C_3 = zP$, $HID_M^{\mathrm{new}} = h(w_M^{\mathrm{new}}, SK_H)$, $SK = h(r_M, r_H, HID_M, zC_1)$, $A_4 = (SK, ID_H) \oplus h(SK_F, zC_2, r_F, T_3)$, $A_5 = h(A_4, r_M, r_H, HID_M)$, A_5^' = $A_5 \oplus (HID_M^{\mathrm{new}}, C_3)$, $A_6 = r_H \oplus r_M$, $A_7 = h(r_F, SK_F, T_3, A_6, A_5'$, A_4, SK) and $A_8 = h(HID_i^{\mathrm{new}}, SK, r_H, r_M, A_5', C_3, HID_M)$, and sends $m_3 = \{C_3, A_5', A_4, A_6, A_7, A_8, T_3\}$ to FA.

◇ Step IV. The FA examines the validity of T_3. If it is valid, it computes $(SK, ID_H) = A_4 \oplus h(SK_F, uC_3, r_F, T_3)$, and checks if $A_7^* = h(r_F, SK_F, T_3, A_6, A_5', A_4, SK)$ is equal to A_7. If so, it retrieves T_4, and sends $m_4 = \{A_4, A_5', A_6, A_8, T_4\}$ to MU.

◇ Step V. The MU checks the validity of T_4. If it is valid, it calculates $r_H = A_6 \oplus r_M$, $A_5 = h(A_4, r_M, r_H, HID_M)$, and then computes $(HID_M^{\mathrm{new}}, C_3) = A_5 \oplus A_5'$, $SK^* = h(r_M, r_H, HID_M, vC_3)$. If $A_8^* = h(HID_M^{\mathrm{new}}, SK^*, r_H, r_M, A_5', C_3, HID_M)$ is equal to A_8. If so, it accepts SK and updates HID_M to HID_M^{new}.

C. PASSWORD CHANGE PHASE: THE MOBILE USER CAN UPDATE ITS PASSWORD TO PROVIDE ITS SECURITY THROUGH THE FOLLOWING STEPS AS DESCRIBED IN WHAT FOLLOWS.

◇ Step I. The mobile user MU inputs ID_M, PW_M and its Bio_M into its smart card. Then, it calculates

$P = REP(Bio_M, Q)$, $L_1 = h(ID_M, PW_M, P)$, $RID_M^* = h(ID_M, P), PID_M^* = h(ID_M, PW_M), HID_M^* = h(ID_M, PW_M)$, $HID_M^* = TID_M \oplus RID_M$ and $g_M^* = h(L_1^*, HID_M^*)$, and checks if Tag_M^* is equal to Tag_M. If the equality holds, the smart card allows the user go the next Step.

◇ Step II. The MU enters its new password PW_M^{new}.

◇ Step III. The smart card computes $L_1^{new} = h(ID_M, PW_M^{new}, P)$, $\mathrm{PID}_M^{new} = h(ID_M, PW_M^{new})$ and $Tag_M = h(L_1, HID_M)$, and replaces Tag_M with Tag_M^{new}. Then, it sends (PID_M, PID_M^{new}) to HA through a secure channel.

VI. INFORMAL SECURITY ANALYSIS

In this subsection, we show that the proposal is secure as defined in Section II.

◇ Forward security. A protocol is forward secure if long term secret keys of entities are compromised, the session key cannot be obtained. In our protocol, the value $zC_1 = vC_3$ is used in session key generation, and so with compromising SK_H and SK_F, the session key SK cannot be computed by the adversary. As a consequence, our protocol provides forward security.

◇ Authentication table leakage attack and privileged user attack. In this attack, an adversary with having access to HA database violates security of the protocol. In our protocol, (Ew_M, PID_M) is stored into HA database, where $Ew_M = (w_M, PID_M) \oplus (h(SK_{H1})), h(SK_{H2}))$ is the encryption of w_M, and so an adversary cannot attain w_M from Ew_M and also ID_M from PID_M. As a consequence, the proposal is secure against authentication table leakage attack and privileged user attack.

◇ Identity guessing attack. In this attack, an adversary can find mobile user identity by offline or online guessing attack. In our protocol, ID_M is used in registration phase in form of encrypted one in RID_M, PID_M and L_1. Therefore, the adversary cannot be aware of ID_M, and it guessing is difficult.

◇ Replay attack. In this attack, the adversary resends previous messages as a new one without being detected by FA and HA, and can generate session key SK. In our protocol, for instance, HID_M is updated in each session, so resending old messages can be detected by HA, and also the adversary cannot compute the session key since it does not have HID_M. Therefore, the proposed protocol has security against replay attack.

◇ Stolen smart card attack. In this attack, an adversary can extract all information stored in U_i's smart card, $\{B_2, B_3, w_i, RTS_i, RTC_i\}$, but it cannot get parameters such as TC_i since it is protected by PW_i and ID_i. Also, guessing these two parameters simultaneously is not possible. In addition, ID_i is protected by a hash function. Hence, the adversary cannot generate message m_1. As a consequence, our protocol is secure against stolen smart card attack.

◇ Home agent impersonation attack. In this attack, an adversary produces a valid message m_3 to

Table 2. Login and authentication phase of our protocol

MU (U_M) **step I**

Inputs ID_M, PW_M, Bio_M, and computes

$P = REP(Bio_M, Q)$

$L_1 = h(ID_M, PW_M, P)$

$RID_M^* = h(ID_M, P)$

$PID_M^* = h(ID_M, PW_M)$ (h)

$HID_M^* = TID_M \oplus RID_M$

$Tag_M^* = h(L_1^*, HID_M^*)$

$Checks\, Tag_M^* \stackrel{?}{=} Tag_M$

Generates random numbers v and r_M

Retrieves timestamp T_1 and computes

$C_1 = vP$

$A_1 = h(HID_M, T_1) \oplus (r_M \oplus ID_H, C_1)$

$m_1 = \{A_1, ID_H, T_1\}$ → FA

Foreign Agent (FA) **step II**

Checks freshness of T_1

Retrieves timestamp T_2, and computes

$C_2 = uP$

$A_2 = h(A_1, ID_H, T_1, T_2, SK_F, C_2) \oplus r_F$

$A_3 = h(A_2, r_F)$

$m_2 = \{A_1, A_2, A_3, T_1, T_2, C_2\}$ → HA

Home Agent (HA) **step III**

Checks freshness of T_2, and computes

$SK_F = h(ID_F, SK_H)$

$r_F = A_2 \oplus h(A_1, ID_H, T_1, T_2, SK_F, C_2)$

$A_3^* = h(A_2, r_F)$

$A_3^* \stackrel{?}{=} A_3$

Computes

$HID_M = h(w_M, SK_H)$

$(r_M \oplus ID_H, C_1) = A_1 \oplus h(HID_M, T_1)$

Retrieves timestamp T_3

Generates three random numbers r_H, z and w_M^{new}

Computes

$C_3 = zP$

$HID_M^{\text{new}} = h(w_M^{\text{new}}, SK_H)$

$SK = h(r_M, r_H, HID_M, ID_F, ID_H, zC_1)$

$A_4 = (SK, ID_H) \oplus h(SK_F, zC_2, r_F, T_3)$

$A_5 = h(A_4, r_M, r_H, HID_M)$

$A_5' = A_5 \oplus HID_M^{\text{new}}$

$A_6 = r_H \oplus r_M$

$A_7 = h(r_F, SK_F, T_3, A_6, A_5', A_4, SK)$

$A_8 = h(HID_M^{new}, SK, r_H, r_M, A_5', C_3, HID_M)$

$m_3 = \{C_3, A_5', A_4, A_6, A_7, A_8, T_3\}$ → FA

Foreign Agent (FA) **step IV**

checks freshness of T_3

Computes

$(SK, ID_H) = A_4 \oplus h(SK_F, uC_3, r_F, T_3)$

$A_7^* = h(r_F, SK_F, T_3, A_6, A_5', A_4, SK)$

$A_7^* \stackrel{?}{=} A_7$

$m_4 = \{A_4, A_5', A_6, A_8, T_4\}$ → MU

MU(U_M) **step V**

Checks freshness of T_4, and computes

$r_H = A_6 \oplus r_M$

$A_5 = h(A_4, r_M, r_H, HID_M)$

$(HID_M^{new}, C_3, ID_H) = A_5 \oplus A_5'$

$SK^* = h(r_M, r_H, HID_M, ID_F, ID_H, vC_3)$

$A_8^* = h(HID_M^{\text{new}}, SK, r_H, r_M, A_5', C_3, HID_M)$

$A_8^* \stackrel{?}{=} A_8$

Updates HID_M to HID_M^{new}

be accepted by FA. In our protocol, for instance, it has to know SK_H to compute SK_F to generate A_4 and also it has to compute HID_M to produce SK and also A_8. Therefore, the proposed protocol is secure against home agent impersonation attack.

◇ Mobile user impersonation attack. In this attack, an adversary produces a valid message m_1 to be accepted by HA. In our protocol, it has to compute a valid A_1, where without having HID_M is not possible. In addition, this value is updated in each session. Therefore, the protocol is secure against mobile user impersonation attack.

VII. FORMAL SECURTY ANALYS

A. BAN LOGIC

By using Burrows–Abadi–Needham logic (BAN logic) that is used in [53] and the following roles we provide the proof. It should be noted that BAN logic is a set of rules for defining and analyzing information exchange protocols. Specifically, BAN logic helps its users determine whether exchanged information is trustworthy, secured against eavesdropping or both. BAN logic starts with the assumption that all information exchanges happen on media vulnerable to tampering and public monitoring. The notations of BAN logic are given in Table 3.

R_1. Nonce verification rule: $\frac{P|\equiv\#(X),P|\equiv Q|\sim X}{P|\equiv Q|\equiv X}$ (1)

R_2. Freshness conjuncatenation rule (2)

(R_2): $\frac{P|\equiv\#(X)}{P|\equiv\#(X,Y)}$

R_3. Seeing rule: $\frac{P◁(X,Y)}{P◁X}$ (3)

R_4. Message meaning rule: $\frac{P|\equiv P\overset{K}{\leftrightarrow}Q,P◁\{X\}_k}{P|\equiv Q|\sim X}$ (4)

R_5. Belief 1: $\frac{P|\equiv Q|\equiv(X,Y)}{P|\equiv Q|\equiv X}$ (5)

R_6. Belief 2: $\frac{P|\equiv Q|\sim(X,Y)}{P|\equiv Q|\sim X}$ (6)

R_7. Jurisdiction rule: $\frac{P|\equiv Q\Rightarrow X,P|\equiv Q|\equiv X}{P|\equiv X}$ (7)

B. SECURITY GOALS

The security goals we need to prove are defined as follows.

Goal 1. $FA \mid\equiv SK$ (8)

Goal 2. $MU \mid\equiv \{SK, HID_M^{\text{new}}\}$ (9)

Table 3. Notations of BAN logic

Notation	Description
$P \mid\equiv X$	*P* believes *X*
$P \mid\sim X$	*P* once said *X* or *P* had sent message *X*
$P \triangleleft X$	*P* sees or receives *X*
$P \overset{K}{\rightleftharpoons} X$	The *K* is a secret formula which, can be used by *P* and *X* to prove their identity to another, because only *P* and *X* know the *K*
$P \Rightarrow X$	*P* has jurisdiction over *X*
$\#(X)$	*X* is fresh
$\langle X \rangle_N$	*X* is encrypted with *N*
$P \overset{K}{\leftrightarrow} Q$	*K* is a shared secret key between *P* and *Q*

C. SUPPOSITIONS

The following suppositions used in the proof are listed in what follows.

$$\mathbf{s_1}: MU \mid\equiv \#(T_1, r_M) \tag{10}$$

$$\mathbf{s_2}: FA \mid\equiv \#(T_2, T_4, r_F) \tag{11}$$

$$\mathbf{s_3}: HA \mid\equiv \#(T_3, r_H) \tag{12}$$

$$\mathbf{s_4}: MU \mid\equiv MU \overset{HID_M}{\longleftrightarrow} HA \tag{13}$$

$$\mathbf{s_5}: HA \mid\equiv HA \overset{HID_M}{\longleftrightarrow} MU \tag{14}$$

$$\mathbf{s_6}: FA \mid\equiv FA \overset{SK_5}{\longleftrightarrow} HA \tag{15}$$

$$\mathbf{s_7}: HA \mid\equiv HA \overset{SK_F}{\longleftrightarrow} FA \tag{16}$$

$$\mathbf{s_8}: MU \mid\equiv HA \Rightarrow SK \tag{17}$$

$$\mathbf{s_9}: FA \mid\equiv HA \Rightarrow SK \tag{18}$$

D. IDEALIZATION

In this section we present an idealized form of our protocol as follows.

$$MU \rightarrow FA: M_1 = \{l_1\} \tag{19}$$

$$l_1: \{\langle r_M, C_1, T_1 \rangle_{HID_M}\} \tag{20}$$

$$FA \rightarrow HA: M_2 = \{l_2, l_3\} \tag{21}$$

$$l_2: \{\langle r_M, C_1, T_1 \rangle_{HID_M}\} \tag{22}$$

$$l_3: \{\langle r_F, C_2, T_2, l_2 \rangle_{SK_F}\} \tag{23}$$

$$HA \rightarrow FAM_3 = \{l_4, l_5\} \quad (24)$$

$$l_4: \{\langle SK, ID_H, T_3\rangle_{h(SK_F, C_3^u, r_F)}\} \quad (25)$$

$$l_5: \{\langle r_M, r_H, HID_M^{\text{new}}, SK\rangle_{HID_M}\} \quad (26)$$

$$FA \rightarrow MU: M_4 = \{l_6\} \quad (27)$$

$$l_6: \{\langle r_H, r_M, HID_M^{\text{new}}, C_3\rangle_{HID_M}\} \quad (28)$$

E. PROOF

In this subsection, the idealized version of our protocol, suppositions, and BAN logic rules are used to prove the aforementioned security goals.

According to l_4, s_6 and R_4 we have:

Based on s_2 and R_2 we have:

$$P_1: FA| \equiv HA| \sim \{SK, ID_H, T_3\} \quad (29)$$

$$P_2: FA \mid\equiv \#SK \quad (30)$$

According to P_1, P_2 and R_1 we have:

$$P_3: FA| \equiv HA| \equiv SK \quad (31)$$

$P_4: FA \mid\equiv SK$ (Goal 1) (32)

Based on and we have:

$$P_3: FA| \equiv HA| \equiv SK \quad (33)$$

$$l_5: \{\langle r_M, r_H, HID_M^{\text{new}}, SK\rangle_{HID_M}\} \quad (34)$$

$$l_5: \{\langle r_M, r_H, HID_M^{\text{new}}, SK\rangle_{HID_M}\} \quad (32)$$

According to l_6, s_4 and R_4 we have:

$$P_5: MU| \equiv HA| \sim \{r_M, r_H, HID_M^{\text{new}}, C_3, T_4\} \quad (33)$$

Based on P_5, s_1 and R_1 we have:

$$P_6: MU| \equiv HA| \equiv \{r_M, r_H, HID_M^{new}, C_3\} \quad (34)$$

According to P_6, s_8 and R_7 we have:

$P_7: MU \mid\equiv \{SK, HID_M^{new}\}$ *(Goal 2)* (34)

VIII. PERFORMACE ANALYS

A. COMPUTATIONAL OVERHEAD

Comparison of m-SMASG, SMASG [15] and AMAPG [11] in terms of computational cost at the MU side, FA side and HA side for logging and authentication phase is summarized in Table 4. In addition, communication overhead of the aforementioned protocols is given in Table 4. In Table 4, T_H, T_R and T_m denote the required time for hash computation, Rep(.) computation and multiplicative operation in the elliptic curve cryptography (ECC). As given in Table 6, the computational time of MU in m-SMASG contains 8 hash computations, one Rep(.) computation and two multiplicative operations as specified in Steps I and V which are done by MU in Subsection V, while this time at MU side is $7T_H + T_R$ and $6T_H$ in SMASG [15] and AMAPG [11], respectively. Similarly, the computation time of FA in m-SMASG includes IV hash function operations and II multiplicative operations as given in Steps II and IV as specified in Subsection V. Hence, computation cost of FA in m-SMASG is $4T_H + 2T_m$, while this value is $4T_H$ and the same for SMASG [15] and AMAPG [11]. The computation time at HA side is composed of 11 hash computations and III multiplicative operations as given in Step III of Subsection V. As a consequence, the time for computation costs in m-SMASG is $11T_H + 3T_m$ and the computation time for SMASG [15] and AMAPG [11] is $7T_H$ and $8T_H$, respectively.

B. COMMUNICATION OVERHEAD

The communication cost of m-SMASG includes the size of messages m_1, m_2, m_3 and m_4, where $m_1 = \{A_1, ID_H, T_1\}$, $m_2 = \{A_1, A_2, A_3, T_1, T_2, C_2\}$, $m_3 = \{C_3, A'_5, A_4, A_6, A_7, A_8, T_3\}$ *and* $m_4 = \{A_4, A'_5, A_6, A_8, T_4\}$. Hence, we have $|m_1| = |A_1| + |ID_H| + |T_1| = |H(.)| + |ID_H| + |T|$, $|m_2| = |A_1| + |A_2| + |A_3| + |T_1| + |T_2| + |C_2| = 3|H(.)| + |\mathbb{Z}_q| + 2|T|$, $|m_3| = |C_3| + |A'_5| + |A_4| + |A_6| + |A_7| + |A_8| + |T_3| = 5|H(.)| + |\mathbb{Z}_q| + |T|$ and $|m_4| = |A_4| + |A'_5| + |A_6| + |A_8| + |T_4| = 4|H(.)| + |T|$ As a consequence, the communication cost is $13|H(.)| + |ID_H| + 5|T| + 2|\mathbb{Z}_q|$ since its size is the summation of the length of these messages. The communication overhead in SMASG [15] and AMAPG [11] is $4|\mathbb{Z}_q| + 6|H(.)| + 5|T|$ and $3|\mathbb{Z}_q| + 9|H(.)| + |T|$, respectively.

C. SECURITY FEATURES COMPARISON

In Table 5, the security features of the proposed protocol are compared with other protocols [10, 11, 15]. According to the results of Table 5 the existing protocols cannot resist various attacks, and they cannot provide mobile user impersonation attack and forward secrecy. Therefore, the proposed protocol can provide more security features in comparison with them.

Table 4. Computation and communication overhead comparison

Metric \ Protocols	AMAPG [11]	SMASG [15]	m-SMASG
MU computational overhead	$6T_H$	$7T_H + T_R$	$8T_H + 2T_m + T_R$
FA computational overhead	$4T_H$	$4T_H$	$4T_H + 2T_m$
HA computational overhead	$8T_H$	$7T_H$	$11T_H + 3T_m$
Communication overhead	$3\|\mathbb{Z}_q\| + 9\|H(.)\| + \|T\|$	$4\|Z_q\| + 6\|H(.)\| + 5\|T\|$	$13\|H(.)\| + \|ID_H\| + 5\|T\| + 2\|\mathbb{Z}_q\|$

D. EXPERIMENTAL RESULTS

In this part, the efficiency of m-SMASG is evaluated and a comparison with SMASG [15] and AMAPG [11] is made. These protocols are implemented on a personal computer (Intel (R) Core (TM) 2 Quad CPU Q8300 2.50 GHz processor, 2 GB memory and Windows 7 Professional system) using MIRACL library [54], SHA-256 for hash function, AES encryption. It is assumed that $|\mathbb{Z}_q| = 160$ bits, $|H(.)| = 256$ bits, $|ID_H| = 40$ bits and $|T| = 32$ bits, T_H =0.5 ms, T_m =50.3 ms and $T_{Rep} = 0.5$ ms.

The computation time at MU side of m-SMASG is $8T_H + 2T_m + T_R = 8 \times 0.5 + 100.6 + 0.5 = 105.1$ ms, while it in SMASG [15] is $7T_H + T_R = 7 \times 0.5 + 0.5 = 4$ ms and in AMAPG [11] is $6T_H = 6 \times 0.5 = 3$ ms. In addition, the computational time at FA side of m-SMASG is $4T_H + 2T_m = 4 \times 0.5 + 2 \times 50.3 = 108.6$ ms, in SMASG [15] is $4T_H = 4 \times 0.5 = 2$ ms and in AMAPG [11] is $4T_H = 4 \times 0.5 = 2$ ms. Furthermore, the computational time at HA side of m-SMASG is $11T_H + 3T_m = 11 \times 0.5 + 3 \times 50.3 = 150.9$ ms, while this value in SMASG [15] is $7T_H = 7 \times 0.5 = 3.5$ ms and in AMAPG [11] is $8T_H = 8 \times 0.5 = 4$ ms. As a consequence, the total computation cost in m-SMASG is 364.9 ms, and also it is 9.5 ms and 9 ms in SMASG [15] and AMAPG [11], respectively. However, the computation cost of m- SMASG is increased, m-SMASG is the first authentication protocol for GLOMONET which satisfies forward secrecy in a way that if long-term secret keys of entities are derived, security of session keys are preserved. As presented in Table 4, the communication overhead of m-SMASG, SMASG [15] and AMAPG [11] is $13|H(.)| + |ID_H| + 5|T| + 2|\mathbb{Z}_q| = 13 \times 250 + 40 + 5 \times 32 + 2 \times 160 = 3770$ bits, $4|\mathbb{Z}_q| + 6|H(.)| + 5|T| = 4 \times 160 + 6 \times 250 + 5 \times 32 = 2300$ ms and $3|\mathbb{Z}_q| + 9|H(.)| + 5|T| = 3 \times 160 + 9 \times 256 + 5 \times 32 = 2944$ bits.

IX. CONCLUSION

In this paper, we showed that SMASG [15] presented by Ryu et al. has some security drawbacks. In fact, it does not have forward security which means that if an adversary obtains long-term secret keys of entities, it can all extract session keys. In addition, SMASG protocol is not secure

Table 5. comparison of security features

Security features	Shashidhara et al. [10]	AMAPG [11]	SMASG [15]	m-SMASG
Resistant to the replay attack	Y	Y	Y	Y
Resistant to the mobile user impersonation attack	N	N	N	Y
Resistant to the home agent impersonation attack	Y	Y	Y	Y
Resistant to the offline password guessing attack	Y	Y	N	Y
Resistant to the stolen smart card attack	N	Y	Y	Y
Resistant to the Identity guessing attack	Y	N	Y	Y
Resistant to the known session-specific temporary information attack	N	N	N	Y
Provide forward secrecy	N	N	N	Y

Note: Y and N denote yes and no, respectively.

against known session-specific temporary information attack since some important information related to the mobile user have not been updated during the protocol, and consequently it does not provide security against mobile user impersonation attack. Then, a forward-secure protocol was presented to address these vulnerabilities, and its security have been discussed. It should be highlighted that m-SMASG not only has forward secrecy and is secure against aforementioned attacks but also its performance evaluation demonstrates that the proposal has a reasonable computation and communication overhead.

REFERENCES

[1] H. Lee, D. Kang, J. Ryu, D. Won, H. Kim, and Y. Lee, "A three-factor anonymous user authentication scheme for internet of things environments," *Journal of Information Security and Applications,* vol.52, (102494), pp.1-15, June 2020.

[2] C. Shi, J. Liu, H. Liu, Y. Chen, "Smart user authentication through actuation of daily activities leveraging Wi-Fi-enabled IoT," *In: Proc. of the 18th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, pp. 1-10. ACM, Chennai, India, July 2017.

[3] G. Horn and B. Preneel, "Authentication and payment in future mobile systems," *In: Proc. of the 5th European Symposium on Research in Computer Security (ESORICS 98),* pp. 277-293. Springer, Louvain-la-Neuve, Belgium, Sept. 1998.

[4] J. Zhu and J. Ma," A new authentication scheme with anonymity for wireless environments," *IEEE Trans. Consumer Electronics,* vol.50, no.1, pp. 231-235, Feb. 2004.

[5] C.-C. Lee, M.-S. Hwang, and I.-E. Lino, "Security enhancement on a new authentication scheme with anonymity for wireless environments," *IEEE Trans. Industrial Electronics,* vol.53, no. 5, pp.1683-1687, Oct. 2006.

[6] 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, March 2009.

[7] 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.

[8] P. Gope and T. Hwang, "Lightweight and energy-efficient mutual authentication and key agreement scheme with

A_5' $\mathbb{Z}$

user anonymity for secure communication in global mobility networks," *IEEE Systems Journal*, vol.10, no.4, pp.1370-1379, April 2016.

[9] G. Q. Xu, J. Liu, Y. R. Lu, X. J. Zeng, Y. Zhang, and X. M. Li, "A novel efficient maki protocol with desynchronization for anonymous roaming service in global mobility networks," *Journal of Network and Computer Applications*, vol.107, pp.8392, April 2018.

[10] R. Shashidhara, S. Bojjagani, A. K. Maurya, S. Kumari, and H. Xiong, "A robust user authentication protocol with privacy-preserving for roaming service in mobility environments," *Peer-Peer Networking and Applications*, vol.13, no. 6, pp.1943-1966, Nov. 2020.

[11] A. M. Rahmani, M. Mohammadi, J. Lansky, S. Mildeova, M. Safkhani, S. Kumari, S. H. T. Karim, and M. Hosseinzadeh, "AMAPG: Advanced mobile authentication protocol for GLOMONET," *IEEE Access*, vol. 9, pp.88256-88271, June 2021.

[12] D. Kang, H. Lee, Y. Lee, and D. Won, "Lightweight user authentication scheme for roaming service in GLOMONET with privacy preserving," *PLOS ONE*, vol. 16, no. 2, 10-13710247441, Feb. 2021

[13] R. Madhusudhan, "Mobile user authentication protocol with privacy preserving for roaming service in GLOMONET," *Peer-Peer Networking and Applications*, vol. 13, no. 1, pp. 82-103, Jan. 2020.

[14] M. Nikooghadam, H. Amintoosi, and S. Kumari, "A provably secure ECC-based roaming authentication scheme for global mobility networks," *Journal of Information Security and Applications,* vol.54, no.2, pp. 102588, Oct. 2020.

[15] J. Ryu, H. Lee, D. Wang: SMASG, "Secure mobile authentication scheme for global mobility network," *IEEE Access*, vol. 10, pp.26907-26919, March 2022.

[16] S. Suzuki and K. Nakada, "An authentication technique based on distributed security management for the global mobility network," *IEEE Journal of Selected Areas in Communications*, vol. , Oct. 1997.

[17] C.-C. Wu, W.-B. Lee, and W.-J. Tsaur, "A secure authentication scheme with anonymity for wireless communications," *IEEE Communications Letters*, vol. 12, no. 10, pp. 722-723, Oct. 2008.

[18] 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.

[19] D. Zhao, H. Peng, L. Li, and Y. Yang, "A secure and effective anonymous authentication scheme for roaming service in global mobility networks," *Wireless Personal Communications*, vol. 78, no. 1, pp. 247-269, Sept. 2014.

[20] E.-J. Yoon, K.-Y. Yoo, and K.-S. Ha, "A user friendly authentication scheme with anonymity for wireless communications," *Computers and Electrical Engineering*, vol. 37, no. 3, pp. 356-364, May 2011.

[21] D. He, M. Ma, Y. Zhang C. Chen, and J. Bu, "A strong user authentication scheme with smart cards for wireless communications," Computer Communications, vol. 34, no. 12, pp. 367-374, March 2011.

[22] X. Li, J. Niu, M. K. Khan, and J. Liao, "An enhanced smart card based remote user password authentication scheme," *Journal of Network and Computer Applications*, vol. 36, no. 5, pp. 1365-1371, Sept. 2013.

[23] 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.

[24] F. Wen, W. Susilo, and G. Yang, "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, Dec. 2013.

[25] P. Gope and T. Hwang, "Lightweight and energy-efficient mutual authentication and key agreement scheme with user anonymity for secure communication in global mobility networks," *IEEE Systems Journal*, vol.10, no.4, pp.1370-1379, April 2016.

[26] J. Niu and X. Li, "A novel user authentication scheme with anonymity for wireless communications," *Security*

and Communication Networks, vol. 7, no. 10, pp. 1467-1476, Oct. 2014.

[27] X. Li, A. K. Sangaiah, S. Kumari, F. Wu, J. Shen, and M. K. Khan, "An efficient authentication and key agreement scheme with user anonymity for roaming service in smart city," *Personal and Ubiquitous Computing*, vol. 21, no. 5, pp.791-805, Oct. 2017.

[28] R. Chen and D. Peng, "An anonymous authentication scheme with the enhanced security for wireless communications," *Wireless personal communications*, vol. 97, no. 2, pp.2665-2682, Nov. 2017.

[29] 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, March 2009.

[30] P. Gope, R.-H. Hsu, J. Lee, and T. Q. S. Quek, "Energy efficient mutual authentication and kay agreement scheme with strong anonymity support for secure ubiquitous roaming services," *In: Proc. of the 11-th International Conference on Availability, Reliability and Security* (ARES 2016), pp. 247-252. IEEE, Salzburg, Austria, Aug. 2016.

[31] C.-C. Lee, Y.-M. Lai, C.-T. Chen, and S.-D. Chen, "Advanced secure anonymous authentication scheme for roaming service in global mobility networks," *Wireless personal communications*, vol. 94, no. 3, pp.1281-1296, June 2017.

[32] A. F. Baig, K. M. U. Hassan, A. Ghani, S. A. Chaudhry, I. Khan, and M. U. Ashraf, "A lightweight and secure two factor anonymous authentication protocol for global mobility networks," *PLOS ONE,* vol. 13, no. 4, 10-13710196061, April 2018.

[33] D. Kang, H. Lee, Y. Lee, and D. Won, "Lightweight user authentication scheme for roaming service in GLOMONET with privacy preserving," *PLoS ONE*, vol. 16, no. 2, e0247441, Feb. 2021.

[34] W. A. Amiri, M. Baza, K. Banawan, M. Mahmoud, W. Alasmary, and K. Akkaya, "Towards secure smart parking system using blockchain technology," *In: Proc. of the 17-th Annual Consumer Communications & Networking Conference (CCNC)*, pp. 10-11094610820209045674. IEEE, NV, USA, Jan2020 ..

[35] W. Al Amiri, M. Baza, K. Banawan, M. Mahmoud, W. Alasmary, K. Akkaya, "Privacy-preserving smart parking system using blockchain and private information retrieval," *IEEE. In: 2019 International Conference on Smart Applications, Communications and Networking (SmartNets*), pp. 1-6, Dec. 2019.

[36] M. Baza, M. Nabil, M. M. E. A. Mahmoud, N. Bewermeier, K. Fidan, W. Alasmary, and M. Abdallah, "Detecting sybil attacks using proofs of work and location in Vanets," *IEEE Trans. Dependable and Secure Computing,* vol. 19, no. 1, pp. 39-53, May 2020.

[37] R. Zhang, R. Xie, and L. Liu, "Security and privacy on blockchain," *ACM Computing Surveys*, vol. 52, no. 3, pp.1-34, July 2019.

[38] M. Baza, M. Nabil, M. Ismail, M. Mahmoud, E. Serpedin, and M. A. Rahman, "Blockchain-based charging coordination mechanism for smart grid energy storage units," *In: Proc. of the 2019 International Conference on Blockchain (Blockchain)*, pp. 504-509. IEEE, Atlanta, GA, USA, July 2019.

[39] P. Gope and T. Hwang, "An efficient mutual authentication and key agreement scheme preserving strong anonymity of the mobile user in global mobility networks," *Journal of Network and Computer Applications*, vol. 62, pp.1-8, Feb. 2016.

[40] D. Guo and F. Wen, "A more robust authentication scheme for roaming service in global mobility networks using ECC," *International Journal of Network Security*, vol. 18, no. 2, pp. 217-223, March 2016.

[41] R. Madhusudhan and Shashidhara, "An efficient and secure authentication scheme with user anonymity for roaming service in global mobile networks," *In: Proc. of the 6th International Conference on Communication and Network Security*, pp. 119-126. ACM, NY, USA, Nov. 2016.

[42] F. Wu, L. Xu, S. Kumari, X. Li, M. K. Khan, and A. K. Das, "An enhanced mutual authentication and key agreement scheme for mobile user roaming service in global mobility networks," *Annals of Telecommunications*, vol. 72, no. 3-4, pp.131-144, April 2017.

[43] S. Bojjagani and V. N. Sastry" A secure end-to-end SMS-based mobile banking protocol, "*International Journal of Communication System*s, vol. 30, no. 15, pp. 10023302, Oct. 2017.

[44] S. Bojjagani and V. N. Sastry "A secure end-to-end proximity NFC-based mobile payment protocol," *Computer Standards & Interfaces*, vol. 66, p.103348, Oct. 2019.

[45] M. Karuppiah, S. Kumari, X. Li, F. Wu, A. K. Das, M. K. Khan, R. Saravanan, and S. Basu, "A dynamic id-based generic framework for anonymous authentication scheme for roaming service in global mobility networks," *Wireless Personal Communications*, vol. 93, no. 2, pp. 383-407, March 2017.

[46] H. Arshad and A. Rasoolzadegan, "A secure authentication and key agreement scheme for roaming service with user anonymity," *International Journal of Communication Systems*, vol. 30, no. 18, pp.10023361, Dec. 2017.

[47] R. Madhusudhan and R. Shashidhara, "A novel DNA- based password authentication system for global roaming in resource-limited mobile environments," *Multimedia Tools and Applications*, vol. 79, no. 3-4, pp. 2185-2212, Jan. 2020.

[48] R. Madhusudhan and R. Shashidhara, "A secure anonymous authentication protocol for roaming service in resource-constrained mobility environments," *Arabian Journal for Science and Engineering*, vol. 45, pp.2993-3014, April 2020.

[49] K. Roy and A. Bhattacharya, "An anonymity-preserving mobile user authentication protocol for global roaming services," *Computer Networks*, vol. 221, pp. 109532, Feb. 2023.

[50] D. Sadhukhan, S. Ray, M. Dasgupta and M.K. Khan, "Development of a provably secure and privacy-preserving lightweight authentication scheme for roaming services in global mobility network," *Journal of Network and Computer Applications*, vol. 224, pp.103831, April 2024.

[51] E.H. Nurkifli, "Provably secure biometric and PUF-based authentication for roaming service in global mobility network," *Alexandria Engineering Journal*, vol. 113, pp. 414-430, Feb. 2025.

[52] P. Oechslin, "Making a faster cryptanalytic time-memory trade-off," *in Proc. of the 23rd Annual International Cryptology Conference on Advances in Cryptology-CRYPTO* 2003, pp. 617-630. Springer, Santa Barbara, California, USA, Aug. 2003.

[53] M. Burrows M, M. Abadi, R.M. Needham," A logic of authentication," *ACM Trans. Computer Systems*, vol.8, no. 1, pp. 18-36, Feb. 1990.

[54] MIRACL Cryptographic Library: Multiprocessing Integer and Rational Arithmetic C/C + + Library. Available at https://www shamus.ie.