IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

AMAPG: advanced mobile authentication protocol for GLOMONET

AMIR MASOUD RAHMANI[1], MOKHTAR MOHAMMADI [2], JAN LANSKY [3], STANISLAVA MILDEOVA [4], MASOUMEH SAFKHANI[5], SARU KUMARI[6], SARKHEL H.TAHER KARIM [7], MEHDI HOSSEINZADEH[8]

[1] Future Technology Research Center, National Yunlin University of Science and Technology, Yunlin, Taiwan (e-mail: rahmania@yuntech.edu.tw)
[2]Department of Information Technology, Lebanese French University, Erbil, Kurdistan Region, Iraq. (e-mail: Mukhtar@lfu.edu.krd)
[3]Department of Computer Science and Mathematics, Faculty of Economic Studies, University of Finance and Administration, Prague, Czech Republic (e-mail: lansky@mail.vsfs.cz)
[4]Department of Computer Science and Mathematics, Faculty of Economic Studies, University of Finance and Administration, Prague, Czech Republic(e-mail: mildeova@mail.vsfs.cz)
[5]Computer Engineering Department, Shahid Rajaee Teacher Training University, Tehran, Iran, Postal code: 16788-15811, (e-mail:Safkhani@sru.ac.ir)
[6]Department of Mathematics, Chaudhary Charan Singh University, Meerut 250004, India, (e-mail: Saryusiirohi@gmail.com)
[7]Computer Department, College of Science, University of Halabja, Halabja, Iraq (e-mail:Sarkhel.kareem@uoh.edu.iq)
[8]Pattern Recognition and Machine Learning Lab, Gachon University, 1342 Seongnamdaero, Sujeonggu, Seongnam 13120, Republic of Korea (e-mail: mehdi@gachon.ac.kr)

Corresponding authors: Mehdi Hosseinzadeh (e-mail: mehdi@gachon.ac.kr).

The result was created in solving the standard project no. 7429/2020/02 "System approach to selected ICT trends" using institutional support for long-term conceptual development of research of the University of Finance and Administration.

ABSTRACT Roaming is when the mobile user goes out of his/her home agent network coverage and loses its signal. Loss of coverage and signals may be limited to a remote area or may occur when mobile user leaves the country and moves to a country where his/her mobile carrier network is not available. In this case, the mobile device is in roaming mode. In this mode, mobile user through connection to a Foreign Agent can still use its home agent services if his/her authentication be successful. In such situations, the authentication mechanism plays a key and important role, where the mobile user often needs to integrate and secure roaming service over multiple foreign agents. Designing a secure mechanism in Global Mobility Network (GLOMONET) is a difficult and complex task due to the computational and processing limitations of most mobile devices, as well as the wireless nature of communication environment. Unfortunately, most of the authentication schemes that have been proposed so far to meet this goal have failed to achieve their goal. In this line, Shashidhara *et al.* recently reported security vulnerabilities of Xu *et al.*'s mobile authentication scheme, and also presented an amended version of it. This paper shows that this proposed scheme has security flaws against impersonation, traceability, forward secrecy contradiction, and stolen smart card attacks, which implies that this protocol may not be a proper choice to be used on GLOMONET. On the other hand, we propose AMAPG, as a cost-efficient remedy version of the protocol which provides desired security against various attacks and also prove its security using BAN logic. We also evaluate AMAPG's security using Scyther as a widely used formal tool to evaluate the security correctness of the cryptographic protocols.

INDEX TERMS Global Mobility Network; Roaming; Stolen Smart Card Attack; Traceability Attack; Impersonation Attack; Scyther, BAN logic.

I. INTRODUCTION

Wireless communication is the transmission of information without a wire interface by electromagnetic waves. The distance at which information is transmitted can be short or long. The term wireless was coined after the invention of the wireless telegraph as opposed to "wired communication". There are many types of wireless in different media, industrial, military, entertainment, frequency bands, transmissions and applications such as cell phone, global positioning system (GPS), remote control, wireless keyboard and satellite TV. One of the benefits of wireless communication is its mobility. The mobility service means that the mobile user i.e. MU can still use the wireless service when traveling to another country that is provided through roaming. Precisely, Global

Mobility Network (GLOMONET) comprises three roles: Mobile users (MU), Home Agents (HA) and Foreign Agents (FA). A mobile user MU first registers with the Home Agent (HA). After leaving the scope of coverage of the HA, in order to be able to continue using wireless services through the roaming system it connects to a Foreign Agent (FA) at its geographic place. The FA subsequently checks whether MU is allowed through HA or not, therefore, a strong authentication process must be held between MU, HA and FA in order to maintain security and privacy.

Whether or not authentication protocols for employing in Global Mobility Network (GLOMONET) are based on smart cards must have the following properties:

- All three parties to the protocol must be synchronized with each other.
- The freshness and aliveness of the protocol parties must be guaranteed.
- Anonymity and untraceability of the mobile user i.e. MU must be addressed even if his/her smart card is stolen (in smart card based authentication protocols).
- All secret values used in the protocol must be kept confidential.
- If the attacker accesses the secret keys of the current session, s/he should not be able to access the secret keys used in the past/future, which is referred to as the forward/backward secrecy.

Due to the importance of roaming security, many protocols have been designed and developed for this purpose. One recent effort in this regard is Xu *et al.*'s protocol. It was not long before that Shashidhara *et al.* [1] showed that Xu *et al.*'s protocol is not able to verify the local password and also suffers from the problem of clock synchronization. To address these issues, they developed a secure protocol for mobile networks. However, in this paper, we show that unfortunately, Shashidhara *et al.*'s protocol is also vulnerable to stolen smart cards and traceability attacks. In addition, we have modified Shashidhara *et al.*'s protocol so that it can be protected against all attacks, especially the ones presented in this paper.

A. PAPER CONTRIBUTION

The contributions of this paper are as follows:

- Design of effective and efficient traceability, user impersonation and stolen smart card attacks against Shashidhara *et al.*'s protocol;
- Strengthening the protocol against user impersonation, stolen smart card and traceability attacks which led to propose a new one called AMAPG (Advanced Mobile Authentication Protocol for GLOMONET);
- Proving the security of AMAPG informally and formally through BAN logic and Scyther;
- Comparing AMAPG in terms of security, required memory, computational and communication costs with other similar recent hash-based authentication protocols presented for GLOMONET.

B. PAPER ORGANIZATION

The remainder of this paper is structured as follows: Section II reviews related work in this field. The description of the protocol in question, Shashidhara *et al.*'s, is given in Section III. Section IV describes the user impersonation, the stolen smart card and the traceability attacks against Shashidhara *et al.*'s protocol. Protocol reinforcement solutions that lead to an advanced mobile authentication protocol (AMAPG) are presented in Section V. Sections VI and VII prove informally and formally the security of the proposed protocol and compares its security and performance, respectively. Finally, the paper ends in Section VIII with suggestions for further work.

II. RELATED WORK

These days, research on mobile authentication has attracted a lot of attention. In 1997, Suzuki *et al.* [2] presented a remote authentication scheme of a home agent through a foreign agent on GLOMONET. Zhu *et al.* in 2005 [3], proposed two-factor authentication protocol based on smart card for roaming's security in wireless environments. However, Lee *et al.* [4] presented that their scheme cannot provide security properties such as mutual authentication and backward secrecy and resistance against all kinds of impersonation attacks. Lee *et al.* [4] also remedied Zhu *et al.*'s scheme and claimed that their protocol resists against all active and passive attacks which are common in GLOMONET. Thereafter, their protocol's vulnerabilities against providing anonymity and the backward secrecy was found by Wu *et al.* [5]. They also presented a new authentication scheme. In [6], Mun *et al.* presented security pitfalls of Wu *et al.*'s scheme [5] such as lack of anonymity and perfect forward secrecy, and vulnerability against legitimate user's password's disclosure. They also presented an amended version using Elliptic Curve Diffie–Hellman (ECDH). Zhao *et al.* [7] reported that [6]'s scheme cannot provide mutual authentication, user-friendliness and local password verification and also suffers from all kinds of impersonation attacks. In 2011, in order to address the security pitfalls of different protocols, Yoon *et al.* presented another authentication protocol and claimed that their scheme preserves user anonymity [8]. However, it was not long before Li *et al.* [9] found its security vulnerabilities such as having unsuccessful key agreement and user traceability. Li *et al.* [9] also presented another GLOMONET security protocol. He *et al.* [10] presented a lightweight authentication protocol for wireless communications using XOR operation and hash functions. However, their protocol's vulnerabilities such as user traceability and weakness against replay and impersonation attacks are reported by Li and Lee [11]. Jiang *et al.* [12] proposed another anonymous scheme to provide privacy preserving in GLOMONET. Thereafter, it is proved by, Wen *et al.* [13] that Jiang *et al.*'s protocol suffers from spoofing and replay attacks. Wen *et al.* [13] also proposed an improved scheme. Gope and Hwang [14] presented a lightweight protocol for mobile networks. Thereafter, Wu *et al.* [15] showed that the protocol of [14] is vulnerable against de-synchronization attacks, unfair key agreement, and being impracticality due to the time delay. Moreover, they combat with proposing an improved mobile user authentication scheme.

Almuhaideb *et al.* [16], introduced the use of Passport/Visa instead of a roaming agreement that enables MUs to authenticate themselves directly with FA. In their proposal, MU receives the Passport as an authentication token from HA and in order to obtain the required Visa, the authentication mechanism can be started with the FA. Therefore, in their scheme, FAs have complete control over the authentication mechanism. They also in [17] presented two passport or visa protocols using their designed hybrid authentication model. In their protocols, passport stamps are used to provide FN with an effective way to solve the problem of checking the user revocation status.

In 2014, Niu *et al.* once again proved that Yoon *et al.*'s scheme cannot provide user anonymity and its key management system is also vulnerable [18]. Niu *et al.* also presented another elliptic curve cryptography (ECC) based authentication protocol. Thereafter, in 2017, authentication schemes based on ECC were independently presented by Li *et al.* [19] and by Chen and Peng [20]. Chang *et al.* and Mun *et al.* independently [21], [6] proposed lightweight schemes that do not use any symmetric or public key encryption/decryption and use only hash function and concatenation operations. It did not take long Gope *et al.* showed that they are highly insecure [22]. Likewise, Lee *et al.* in 2017, [23] showed the Mun *et al.* 's scheme [6] is vulnerable against man-in-the-middle and impersonation attacks, and does not provide perfect forward secrecy. Lee *et al.* also in [23] introduced another scheme, but they emphasized that their protocol suffers from logical errors and denial-of-service attacks of the registration phase. In 2018, Baig *et al.* proposed a new lightweight scheme to solve these issues [24]. However, in [25] have been shown the Baig *et al.*'s scheme cannot provide user privacy. They also proposed a new lightweight scheme and claimed their scheme provides user untraceability and privacy and resistance against identity/password guessing attacks. They also verified the security of their proposed scheme using ProVerif and AVISPA.

Later on, some new blockchain based authentication schemes have been proposed [26], [27], [28], [29], [30]. Besides, the protocols of [31], [32], [33], [34], [35], [36], [37], [38], [39], [40] have more computational overhead. Xu *et al.* [41] examined the security of proposed protocol of [31] and reported its vulnerability to replay attack, de-synchronization attack and having a large storage burden. Xu *et al.* also presented a new mutual authentication scheme. Thereafter, Shashidhara *et al.* [1] proved that the Xu *et al.*'s protocol does not resist against stolen verifier, denial of service, privileged insider, and impersonation attacks. Besides, they showed that the Xu *et al.*'s protocol is unable to provide local password verification and also suffers from clock synchronization problem. They also as a remedy, proposed a secure scheme for mobility networks. However, in this paper, we show that Shashidhara *et al.*'s protocol suffers from user impersonation, stolen smart card and traceability attacks. Moreover, we revised Shashidhara *et al.*'s protocol in such a way that it can be safe against all attacks, especially the ones presented in this paper.

TABLE 1: Notations

Symbol	Description
MU	The mobile user
HA	The home agent
FA	The foreign agent
ID_X	The identifier of entity X
PSW_M	The password of mobile user
K_{MU}	The counter of mobile user
SK	The session key
S_X	The secret value of X
SC	The smart card
R_N	The random number which is constantly stored in MU's smart card
N_M	Random number
$h(.)$	Hash Function
$\oplus$	Bit-wise exclusive-or (XOR) operation
$\|$	Concatenation operation
A	The adversary
Pr	The probability

III. SHASHIDHARA *ET AL.*'S PROTOCOL

The proposed protocol of Shashidhara *et al.* [1] to remedy Xu *et al.*'s protocol runs using notations represented in Table 1 as below in three phases including registration phase, login and authentication phase, and arbitrary password change phase.

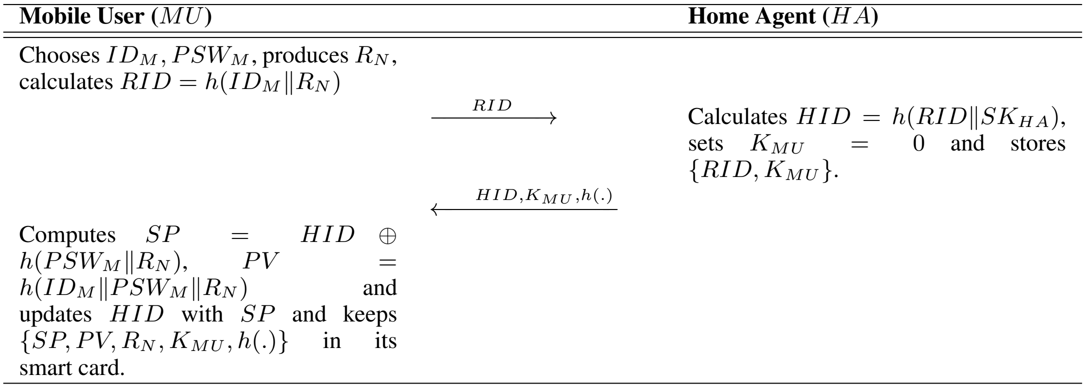
A. REGISTRATION PHASE

In this phase, the mobile user MU, gets registered with the home agent HA as below:(see Figure 1)

1) MU chooses its identity and password i.e. ID_M, PSW_M, produces a new random number R_N and using that computes $RID = h(ID_M \| R_N)$ and through a secure channel transmits RID to HA.
2) Once receives the message, HA calculates $HID = h(RID \| SK_{HA})$. Thereafter, HA sets MU's counter $K_{MU} = 0$ and stores $\{RID, K_{MU}\}$ in its database. At last, HA sends $\{HID, K_{MU}, h(.)\}$ to MU.
3) As soon as received the message, MU computes $SP = HID \oplus h(PSW_M \| R_N)$, $PV = h(ID_M \| PSW_M \| R_N)$, and updates HID with SP in the smart card. At last, MU keeps $\{SP, PV, R_N, K_{MU}, h(.)\}$ in the smart card.

B. LOGIN AND AUTHENTICATION PHASE

The login and authentication phase of Shashidhara *et al.*'s protocol as depicted in Figure 2, runs as follows:



Mobile User (MU)

Home Agent (HA)

Chooses ID_M, PSW_M, produces R_N, calculates $RID = h(ID_M\|R_N)$

$\xrightarrow{RID}$

Calculates $HID = h(RID\|SK_{HA})$, sets $K_{MU} = 0$ and stores $\{RID, K_{MU}\}$.

$\xleftarrow{HID, K_{MU}, h(.)}$

Computes $SP = HID \oplus h(PSW_M\|R_N)$, $PV = h(ID_M\|PSW_M\|R_N)$ and updates HID with SP and keeps $\{SP, PV, R_N, K_{MU}, h(.)\}$ in its smart card.

FIGURE 1: Registration phase of Shashidhara *et al.*'s protocol [1]

1) The mobile user MU puts the smart card in to the reader terminal and inputs his/her identity and password information i.e. ID_M and PSW_M.
2) Reader terminal calculates $PV^* = h(ID_M\|PSW_M\|R_N)$ and then checks whether $PV^* \overset{?}{=} PV$ is or not. If it does not hold, the reader stops the process, otherwise it verifies the mobile user MU is legitimate.
3) MU device generates a new random number N_M and calculates $HID = SP \oplus h(PSW_M\|R_N)$, $A_M = h(ID_M\|R_N)\oplus N_M$, $V_1 = h(HID\|K_{MU})\oplus N_M$, and transmits a login request $M_{MF} = \{A_M, V_1, ID_H\}$ to FA.
4) When FA receives M_{MF}, generates another random number N_F and calculates $A_F = h(A_M\|SK_{FA}) \oplus N_F$,$V_2 = h(A_F\|SK_{FA}\|V_1)$, stores them, and transmits an authentication request $M_{FH} = \{ID_F, A_F, V_1, V_2\}$ to HA.
5) Once received the message, HA at first searches for ID_F. If it exists, HA corresponding to ID_F, finds a secret key $SK_{FA} = h(ID_F\|SK_{HA})$. Then it calculates $V_2^* = h(A_F\|SK_{FA}\|V_1)$ and checks whether $V_2^* \overset{?}{=} V_2$ is or not. If so, HA authenticates FA and extracts $\{RID, K_{MU}\}$ from its database and calculates $HID^* = h(RID\|SK_{HA})$, $N_M^* = h(HID^*\|K_{MU})\oplus V_1$, $V_1^* = h(HID^*\|K_{MU})\oplus N_M^*$, and checks whether $V_1^* \overset{?}{=} V_1$. If they do not hold, HA stops the process otherwise successfully authenticates MA, and calculates $A_M^* = h(ID_M\|R_N) \oplus N_M^*$, $N_F = h(A_M^*\|SK_{FA})\oplus A_F$, $N_M' = h(HID^*\|N_M^*)\oplus N_F$, $V_3 = h(ID_H\|A_M^*\|SK_{FA})$, and $V_4 = h(HID^*\|ID_F\|K_{MU})$. Then it updates the counter as $K_{MU} = K_{MU} + 1$, and sends authentication response i.e. $M_{HF} = \{N_M', V_3, V_4\}$ to FA.
6) When receives the message, FA calculates $V_3^* = h(ID_H\|A_M\|SK_{FA})$ and checks whether $V_3^* \overset{?}{=} V_3$. If it is not, FA stops the process otherwise successfully authenticates MA and HA. Then FA calculates the session key as $SK = h(N_F\|A_M\|ID_H)$ and sends $M_{FM} = \{N_M', V_4\}$ to MU.
7) Once receipt of the message, MU computes $V_4^* = h(HID\|ID_F\|K_{MU})$, and checks whether $V_4^* \overset{?}{=} V_4$ is or not. If it does not hold, MU stops the process, otherwise, successfully authenticates FA and HA and extracts $N_F = N_M' \oplus h(HID\|N_M)$ and using that computes the secret key as $SK = h(N_F\|A_M\|ID_H)$. At last, MU updates its smart card's counter as $K_{MU} = K_{MU} + 1$.

C. PASSWORD CHANGE PHASE

In Shashidhara *et al.*'s protocol, it is possible that MU changes his default password without HA's assistance as below:

- MU puts on his/her identity ID_M and password PSW_M and submits the password change request in the reader terminal.
- The smart card of MU calculates $PV^* = h(ID_M\|PSW_M\|R_N)$ and then checks whether $PV^* \overset{?}{=} PV$ is or not. If it does not hold, the request is rejected. Otherwise, it is proved that MU is legitimate. Then smart card derives $HID = SP \oplus h(PSW_M\|R_N)$.
- MU enters its new password i.e. PSW_M^* and calculates $PV_N = h(ID_M\|PSW_M^*\|R_N)$, $SP_N = HID \oplus h(PSW_M^*\|R_N)$ and then updates the old $\{PV, SP\}$ with new values of $\{PV_N, SP_N\}$ respectively. At last, the smart card contains $\{PV_N, SP_N, R_N, K_{MU}\}$.

IV. ATTACKS ON SHASHIDHARA *ET AL.*'S PROTOCOL

In this section, used adversary model and scenarios of user impersonation, stolen smart card and traceability attacks are presented in detail to show the security vulnerabilities of Shashidhara *et al.*'s protocol.

A. ADVERSARY MODEL

The used adversary model in this paper is based on Dolev–Yao [42] adversary model in which all protocol parties communicate each other over insecure channels. An adversary in this model has below abilities:

Mobile User MU	**Foreign Agent** FA	**Home Agent** HA
MU inputs ID_M, PSW_M. Reader terminal computes $PV^* = h(ID_M\|PSW_M\|R_N)$. If PV^*=PV, authenticates MU. MU generates N_M, calculates $HID = SP \oplus h(PSW_M\|R_N)$, $A_M = h(ID_M\|R_N) \oplus N_M$, $V_1 = h(HID\|K_{MU}) \oplus N_M$ $\xrightarrow{\{A_M,V_1,ID_H\}}$		
	Generates N_F, calculates $A_F = h(A_M\|SK_{FA}) \oplus N_F$,$V_2 = h(A_F\|SK_{FA}\|V_1)$ $\xrightarrow{\{ID_F,A_F,V_1,V_2\}}$	
		Searches for ID_F. If it exists, based on ID_F, finds $SK_{FA} = h(ID_F\|SK_{HA})$, computes $V_2^* = h(A_F\|SK_{FA}\|V_1)$. If V_2^*=V_2, authenticates FA, extracts $\{RID, K_{MU}\}$, calculates $HID^* = h(RID\|SK_{HA})$,$N_M^* = h(HID^*\|K_{MU}) \oplus V_1$, $V_1^* = h(HID^*\|K_{MU})\oplus N_M^*$. If V_1^*=V_1, authenticates MU, calculates $A_M^* = h(ID_M\|R_N) \oplus N_M^*$, $N_F = h(A_M^*\|SK_{FA}) \oplus A_F$, $N_M' = h(HID^*\|N_M^*) \oplus N_F$, $V_3 = h(ID_H\|A_M^*\|SK_{FA})$ and $V_4 = h(HID^*\|ID_F\|K_{MU})$, $K_{MU} = K_{MU} + 1$ $\xleftarrow{\{N_M',V_3,V_4\}}$
	Computes $V_3^* = h(ID_H\|A_M\|SK_{FA})$. If V_3^*=V_3, authenticates MU and HA, calculates $SK = h(N_F\|A_M\|ID_H)$ $\xleftarrow{\{N_M',V_4\}}$	
Computes $V_4^* = h(HID\|ID_F\|K_{MU})$. If V_4^*=V_4 , authenticates FA and extracts $N_F = N_M' \oplus h(HID\|N_M)$ and computes $SK = h(N_F\|A_M\|ID_H)$, $K_{MU} = K_{MU} + 1$.		

FIGURE 2: Login and authentication phase of Shashidhara *et al.*'s protocol [1]

- can eavesdrop all the exchanged messages over the insecure channel;
- can modify, delete or replay the exchanged messages;
- can extract the stored important secret information from the smart card's memory by monitoring the smart card's power consumption [43];
- can be a legitimate insider user or an outsider [44].

B. USER IMPERSONATION ATTACK

In Step 5 of the login and authentication phase of Shashidhara *et al.*'s protocol, once received the message, after FA authentication, HA extracts $\{RID, K_{MU}\}$ from its database and calculates $HID^* = h(RID\|SK_{HA})$, $N_M^* = h(HID^*\|K_{MU}) \oplus V_1$, $V_1^* = h(HID^*\|K_{MU}) \oplus N_M^*$ and checks whether $V_1^* \overset{?}{=} V_1$ to authenticate the user. It is clear, replacing V_1 by any random string of the same length will pass the above verification. In addition, the received A_M

is not verified by HA. Hence, to impersonate MU, it is enough to respect ID_H and send any value as V_1 and A_M to the foreign agent. FA will forward it to HA and it will authenticate the user. It should be noted the protocol flaw comes the fact that the random nonce is extracted from V_1 and then its correctness is also verified based on V_1. However, it was better to use the received $A_M = h(ID_M \| R_N) \oplus N_M$ to verify the correctness of the extracted N_M and authenticating the user.

C. TRACEABILITY ATTACK

Our proposed traceability attack is presented as a game G in which the adversary has access to the following queries:

- $Execute(MU_i, FA, HA)$ query: With this query, the adversary executes the protocol once between different protocol participants and receives exchanged messages.
- $Test(MU_0, MU_1, FA, HA)$ query: In this query, the adversary must express his conjecture i.e. $b \in \{0, 1\}$ that which mobile user i.e. MU_0 or MU_1 participates in the protocol. The adversary's advantage i.e. Adv_A is defined as follows:
  $Adv_A = Pr(b\ is\ correct) - Pr(b\ is\ random) = Pr(b\ is\ correct) - 1/2 > \epsilon$
  where ϵ is a negligible function. If the adversary's advantage is much greater than ϵ, it means that the protocol in question is vulnerable to a traceability attack.

Here, we show that how the adversary can retrieve constant information related to mobile user MU which is usable to trace it. For our proposed traceability attack, it is enough the adversary plays the game G as below:

- runs $Execute(MU_0, FA, HA)$ query on Shashidhara *et al.*'s protocol and stores messages including A_M and V_1.
- computes $A_M \oplus V_1 = h((ID_M)_0 \| (R_N)_0) \oplus N_M \oplus h(HID_0 \| K_{MU_0}) \oplus N_M = h((ID_M)_0 \| (R_N)_0) \oplus h(HID_0 \| K_{MU_0})$ which is a constant value related to a specific mobile user MU_0.
- runs $Test(MU_0, MU_1, FA, HA)$ and in response to it, computes $A_M \oplus V_1 = h(ID_M \| R_N) \oplus N_M \oplus h(HID \| K_{MU}) \oplus N_M = h(ID_M \| R_N) \oplus h(HID \| K_{MU})$. Then s/he compares the result with $h((ID_M)_0 \| (R_N)_0) \oplus h(HID_0 \| K_{MU_0})$. If they are equal, s/he determines MU_0 participates in the protocol otherwise determines MU_1 is in the protocol.

D. STOLEN SMART CARD ATTACK

Stolen smart card attack is an attack in which the adversary is assumed to have access to the smart card and the values stored in it. S/he then uses that information to obtain other important secret values of the protocol such as secret session key i.e. SK. The adversary to apply our proposed stolen smart card attack scenario against Shashidhara *et al.*'s protocol, it is enough to proceed as follows:

1) Eavesdrop one authentication phase of Shashidhara *et al.*'s protocol and store exchanged messages including A_M, ID_H, V_1, N'_M, V_4 and ID_F.
2) Steal the mobile user MU's smart card and getting the values stored in it i.e. $\{SP, PV, R_N, K_{MU}, h(.)\}$.
3) Using stolen SP and R_N from MU's smart card and guessing MU's password i.e. PSW_M, the adversary computes $HID' = SP \oplus h(PSW_M \| R_N)$.
4) Using stolen K_{MU} from MU's smart card and retrieved HID' from Step 3, the adversary computes $V'_4 = h(HID \| ID_F \| K_{MU})$ and if V'_4 equals with eavesdropped V_4, means that the retrieved HID' is the same as the original HID, otherwise, it returns to Step 3.
5) Using stolen K_{MU} from MU's smart card and original HID which s/he retrieved in Step 4 and using eavesdropped V_1, the adversary extracts N_M as $V_1 \oplus h(HID \| K_{MU})$.
6) Using eavesdropped N'_M and N_M which extracted in Step 5, the adversary computes N_F as $N'_M \oplus h(HID \| N_M)$.
7) Finally, the adversary using retrieved N_F from Step 6, and the eavesdropped A_M and ID_H computes the secret session key i.e. SK as $h(N_F \| A_M \| ID_H)$ which is shared between mobile user MU and foreign agent FA. Using this key, the adversary can decrypt all communications encrypted with this key between MU and FA, thus violating the confidentiality property of communications. The success probability of the attack is equal to the success probability of the adversary in guessing the MU's password i.e. PSW_M, which is selected from a limited set.

Although Shashidhara *et al.* [[1], Table 4] also claimed to provide perfect forward secrecy. However, the above attack also violates the forward secrecy of the protocol.

V. AMAPG: THE PROPOSED PROTOCOL

To remedy the weaknesses of Shashidhara *et al.*'s protocol, in this section we propose an enhanced protocol and for the sake of simplicity we name it AMAPG, stands for advanced mobile authentication protocol for GLOMONET. We keep the protocol phases of AMAPG identical to those of Shashidhara *et al.*'s protocol, i.e. registration phase, login and authentication phase and arbitrary password change phase. In addition, we only modify login and authentication phase and keep the other two phases as it is, exclude that in the registration phase $RID = h(ID_M \| R_N)$ is replaced by $RID = h(ID_M \| (PSW_M \oplus R_N))$ and $SP = HID \oplus h(PSW_M \| R_N)$ is replaced by $SP = HID \oplus h(PSW_M \| (ID_M \oplus R_N))$. Hence, as it is depicted in Figure 3, the registration phase of AMAPG runs as follows:

1) MU chooses its identity and password i.e. ID_M, PSW_M, produces a new random number R_N and using that computes $RID = h(ID_M \| (PSW_M \oplus R_N))$ and through a secure channel transmits RID to HA.
2) Upon receipt of the message, HA calculates $HID = h(RID \| SK_{HA})$. Thereafter, HA stores $\{RID\}$ in its

database. At last, HA sends a smart card SC which includes $\{HID, h(.)\}$ to MU.

3) As soon as received SC, MU computes $SP = HID \oplus h(PSW_M \| (ID_M \oplus R_N))$, $PV = h(ID_M \| PSW_M \| R_N)$, and updates HID with SP in the received SC and also stores $\{SP, PV, R_N, h(.)\}$ in it.

The login and authentication phase of AMAPG is depicted in Figure 4. In the revised version, we replace the counter K_{MU} by the timestamp T_M and also the timestamp of the foreign agent, T_F, and home agent, T_H. This modification provides security against relay and replay attacks also. The login and authentication phase of AMAPG proceeds as follows:

A. LOGIN AND AUTHENTICATION PHASE

1) The mobile user MU puts the smart card in to the reader terminal and inputs his/her identity and password information i.e. ID_M and PSW_M.
2) Reader terminal calculates $PV^* = h(ID_M \| PSW_M \| R_N)$ and then checks whether $PV^* \overset{?}{=} PV$. If the equality does not hold, it stops the process, otherwise it accepts the mobile user as the legitimate user.
3) MU device generates a new random number N_M and calculates $HID = SP \oplus h(PSW_M \| (ID_M \oplus R_N))$, $A_M = h((HID \oplus N_M) \| T_M)$, $V_1 = h(HID \| T_M) \oplus N_M$, and transmits a login request $M_{MF} = \{A_M, V_1, ID_H, T_M\}$ to FA.
4) When FA receives M_{MF}, verifies T_M, generates another random number N_F and calculates $A_F = h(A_M \| T_F \| SK_{FA}) \oplus N_F$,$V_2 = h(A_F \| (T_F \oplus N_F) \| SK_{FA} \| (V_1 \oplus A_M))$, stores them and transmits an authentication request $M_{FH} = \{T_F, ID_F, A_F, V_1, V_2\}$ to HA.
5) Once received the message, HA at first verifies the timestamps T_M and T_F and then searches for ID_F. If it exists, HA finds a secret key $SK_{FA} = h(ID_F \| SK_{HA})$. Then it calculates $N_F^* = A_F \oplus h(A_M \| T_F \| SK_{FA})$ and extracts a $\{RID^*\}$ from its database and calculates $HID^* = h(RID^* \| SK_{HA})$, $N_M^* = h(HID \| T_M) \oplus V_1$ and $A_M^* = h((HID \oplus N_M) \| T_M)$. Then HA checks whether $V_2 \overset{?}{=} h(A_F \| (T_F \oplus N_F) \| SK_{FA} \| (V_1 \oplus A_M^*))$. If so, HA authenticates FA and MU. Once they have been authenticated, HA computes $A_H = A_F \oplus N_F^* \oplus N_M^*$, $V_3 = h((ID_H \oplus N_H) \| (N_F^* \oplus A_H) \| SK_{FA} \| T_H)$ and $V_4 = h((HID^* \oplus N_F^*) \| (ID_H \oplus N_M^*) \| N_H \| T_H)$ and sends authentication response, i.e. $M_{HF} = \{T_H, A_H, N_H, V_3, V_4\}$ to FA.
6) When receives the message, FA verifies T_H, calculates $V_3^* = h((ID_H \oplus N_H) \| (N_F \oplus A_H) \| SK_{FA} \| T_H)$ and checks whether $V_3^* \overset{?}{=} V_3$. If it is not, FA stops the process otherwise successfully authenticates MA and HA. Then, FA extracts $N_M = A_H \oplus A_F \oplus N_F$, calculates $A'_F = A_M \oplus N_M \oplus N_F$ and the session key as $SK = h(N_F \| N_M \| N_H)$ and sends $M_{FM} = \{N_H, A'_F, T_H, V_4\}$ to MU.
7) Once received the message, MU verifies T_H, extracts $N_F = A'_F \oplus A_M \oplus N_M$, computes $V_4 = h((HID \oplus N_F) \| (ID_H \oplus N_M) \| N_H \| T_H)$ and checks whether $V_4^* \overset{?}{=} V_4$. If it does not hold, MU stops the process, otherwise, successfully authenticates FA and HA and computes the secret key as $SK = h(N_F \| N_M \| N_H)$.

B. PASSWORD CHANGE PHASE

In AMAPG, we revise the password change phase as follows, which takes place over a secure channel:

- MU puts on his/her identity ID_M and password PSW_M and submits the password change request in the reader terminal.
- The smart card of MU calculates $PV^* = h(ID_M \| PSW_M \| R_N)$ and then checks whether $PV^* \overset{?}{=} PV$ is or not. If it does not hold, the request is rejected. Otherwise, it is proved that MU is legitimate. Then smart card derives $HID = SP \oplus h(PSW_M \| (ID_M \oplus R_N))$.
- MU enters its new password i.e. PSW_M^* and calculates $PV_N = h(ID_M \| PSW_M^* \| R_N)$, $SP_N = HID \oplus h(PSW_M^* \| (ID_M \oplus R_N))$ and then updates the old $\{PV, SP\}$ with new values of $\{PV_N, SP_N\}$ respectively. At last, the smart card contains $\{PV_N, SP_N, R_N\}$.

VI. SECURITY PROOF OF AMAPG

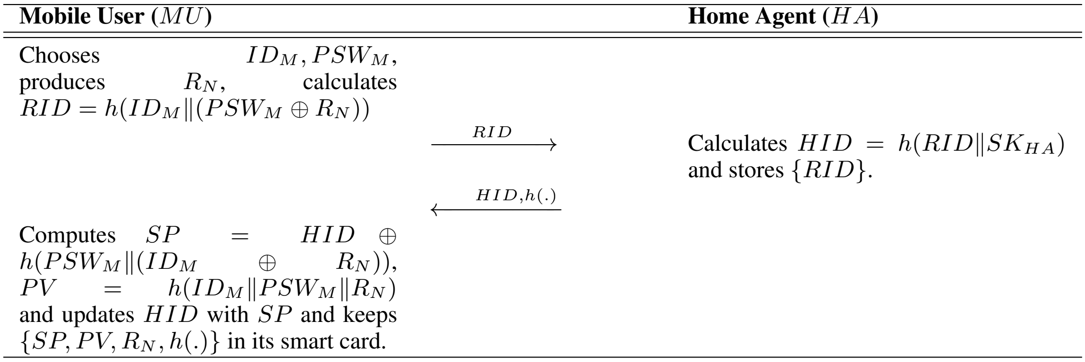
Here, we provide informal and formal security arguments of AMAPG against various attacks, including replay attack, impersonation attack, desynchronization attack and etc.

A. INFORMAL SECURITY ANALYSIS

Informal security proof methods are ones that are used using the knowledge and reasoning of the analyst to prove that the security protocol is weak or lacks security pitfalls and resists against the attack in question.

1) Replay attack

To do a replay attack, the adversary tries to impersonate a protocol party by eavesdropping a session of the protocol between legitimate parties and later broadcasting the stored messages. In AMAPG, the adversary has no significant chance to do replay attack because any session is randomized by the fresh nonces and also time stamps. For example, MU sends $A_M = h((HID \oplus N_M) \| T_M)$ and $V_1 = h(HID \| T_M) \oplus N_M$ to FA in which T_M is the timestamp and N_M is a fresh nonce and they prevent the adversary to use it later successfully. Similarly, FA sends $A_F = h(A_M \| T_F \| SK_{FA}) \oplus N_F$ and $V_2 = h(A_F \| (T_F \oplus N_F) \| SK_{FA} \| (V_1 \oplus A_M))$ to HA and HA sends $A_H = A_F \oplus N_F \oplus N_M$, $V_3 = h((ID_H \oplus N_H) \| (N_F \oplus A_H) \| SK_{FA} \| T_H)$ and $V_4 = h((HID \oplus N_F) \| (ID_H \oplus N_M) \| N_H \| T_H)$ to FA, where T_F and T_H are timestamps and N_F and N_H



Mobile User (MU)		**Home Agent** (HA)
Chooses ID_M, PSW_M, produces R_N, calculates $RID = h(ID_M \| (PSW_M \oplus R_N))$		
	$\xrightarrow{RID}$	Calculates $HID = h(RID \| SK_{HA})$ and stores $\{RID\}$.
	$\xleftarrow{HID, h(.)}$	
Computes $SP = HID \oplus h(PSW_M \| (ID_M \oplus R_N))$, $PV = h(ID_M \| PSW_M \| R_N)$ and updates HID with SP and keeps $\{SP, PV, R_N, h(.)\}$ in its smart card.		

FIGURE 3: Registration phase of AMAPG

are fresh nonces. Hence, a re-broadcasted message will be rejected by the received due to the timestamp verification. If the adversary changes the time stamp to an acceptable time, then the session will be rejected due to the lack of integrity.

2) Impersonation attack

To impersonate a protocol party, the adversary either should do a replay attack or generate valid messages to be accepted by a protocol party. However, in the case of AMAPG, in sub-subsection VI-A1, we have argued that it is not feasible to do replay attack. On the other hand, the adversary cannot produce valid messages because:

- $A_M = h((HID \oplus N_M) \| T_M)$ and $V_1 = h(HID \| T_M) \oplus N_M$ are dependent on HID which is secret;
- $A_F = h(A_M \| T_F \| SK_{FA}) \oplus N_F$ and $V_2 = h(A_F \| (T_F \oplus N_F) \| SK_{FA} \| (V_1 \oplus A_M))$ are factors of SK_{FA} which is a shared secret between the foreign agent and the home agent;
- $V_3 = h((ID_H \oplus N_H) \| (N_F \oplus A_H) \| SK_{FA} \| T_H)$ and $V_4 = h((HID \oplus N_F) \| (ID_H \oplus N_M) \| N_H \| T_H)$ are respectively factors of SK_{FA} and HID.

Therefore, AMAPG is secure against impersonation attacks.

3) Traceability and anonymity

It is possible to trace a protocol party if the adversary can find a correlation between its responses in different sessions which is specific for that entity. However, exclude timestamps which do not provide any information regarding the mobile user, any transferred message by MU in AMAPG, i.e. A_M and V_1, are randomized by nonce/timestamp through a one-way hash function. Hence, assuming the used hash function is enough secure, AMAPG is secure against MU traceability attack. A protocol which is secure against user traceability is also preserves the mobile user anonymity as well. It is worth noting that we do not aim to provide FA or HA anonymity/traceability.

4) Secret disclosure attack

Exclude time stamps, the identity of FA and HA and the nonce N_H, the rest of the transferred messages over the channel are produced/masked by one-way hash functions and the input of hash functions are including secret parameters. Given that it is not feasible to invert a secure hash function, AMAPG does not reveal any secret parameters. In addition, the session key is computed as $SK = h(N_F \| N_M \| N_H)$ and N_M and N_F have respectively been masked by $h(HID \| T_M)$ and $h(A_M \| T_F \| SK_{FA})$, in which HID and SK_{FA} are secrets and T_M and T_F are fresh session-dependent timestamps. Hence, AMAPG provides desired security against secret disclosure attacks.

5) Permanent de-synchronization attack

To de-synchronize a protocol party permanently, the adversary could force them to update their shared values differently, for example see [45]. However, in the login and authentication phase of AMAPG are not updated any shared values. In addition, the integrity of the transferred messages has been guaranteed by one-way hash functions and the adversary cannot impersonate any entity. Hence, it cannot also force them to come up with different session keys. On the other hand, in the password change phase, to change the password, the adversary should choose a pair of ID'_M and password PSW'_M such that they satisfy $PV = h(ID'_M \| PSW'_M \| R_N)$ which is not feasible without the knowledge of the user ID_M and PSW_M. Hence, AMAPG provides desired security against any permanent de-synchronization attack. However, similar to any other protocol, an active adversary can terminate the messages to prevent secret sharing, which is applicable to any other protocol which is run over a public channel.

6) Man-in-the-middle attack

Given that the integrity of all messages are guaranteed by hash functions and the session time is also controlled by timestamps, any message manipulation or unexpected delay by a man-in-the-middle adversary will be detected with a high probability. Hence, AMAPG is secure against man-in-the-middle attacks.

Mobile User MU	**Foreign Agent** FA	**Home Agent** HA
MU inputs ID_M, PSW_M. Reader terminal computes $PV^* = h(ID_M \Vert PSW_M \Vert R_N)$. If $PV^*{=}PV$, authenticates MU, generates N_M, calculates $HID = SP \oplus h(PSW_M \Vert (ID_M \oplus R_N))$, $A_M = h((HID \oplus N_M) \Vert T_M)$ and $V_1 = h(HID \Vert T_M) \oplus N_M$ $\xrightarrow{\{A_M, V_1, ID_H, T_M\}}$		
	Verifies T_M, generates N_F, computes $A_F = h(A_M \Vert T_F \Vert SK_{FA}) \oplus N_F$ and $V_2 = h(A_F \Vert (T_F \oplus N_F) \Vert SK_{FA} \Vert (V_1 \oplus A_M))$ $\xrightarrow{\{T_F, ID_F, A_F, V_1, V_2\}}$	
		Verifies T_M and T_F, searches for ID_F and finds $SK_{FA} = h(ID_F \Vert SK_{HA})$, computes $N_F^* = A_F \oplus h(A_M \Vert T_F \Vert SK_{FA})$ and extracts a $\{RID^*\}$ from its database and calculates $HID^* = h(RID^* \Vert SK_{HA})$, $N_M^* = h(HID^* \Vert T_M) \oplus V_1$ and $A_M^* = h((HID^* \oplus N_M^*) \Vert T_M)$, checks $V_2 \overset{?}{=} h(A_F \Vert (T_F \oplus N_F) \Vert SK_{FA} \Vert (V_1 \oplus A_M^*))$ and computes $A_H = A_F \oplus N_F^* \oplus N_M^*$, $V_3 = h((ID_H \oplus N_H) \Vert (N_F^* \oplus A_H) \Vert SK_{FA} \Vert T_H)$ and $V_4 = h((HID^* \oplus N_F^*) \Vert (ID_H \oplus N_M^*) \Vert N_H \Vert T_H)$ $\xleftarrow{\{T_H, A_H, N_H, V_3, V_4\}}$
	Computes $V_3^* = h((ID_H \oplus N_H) \Vert (N_F \oplus A_H) \Vert SK_{FA} \Vert T_H)$ and checks $V_3^* \overset{?}{=} V_3$ to authenticate MA and HA, extracts $N_M = A_H \oplus A_F \oplus N_F$, calculates $A'_F = A_M \oplus N_M \oplus N_F$ and the session key $SK = h(N_F \Vert N_M \Vert N_H)$ $\xleftarrow{\{N_H, A'_F, V_4\}}$	
Extracts $N_F = A'_F \oplus A_M \oplus N_M$, checks whether $V_4 \overset{?}{=} h((HID \oplus N_F) \Vert (ID_H \oplus N_M) \Vert N_H \Vert T_H)$ to authenticate FA and HA and then computes the session key as $SK = h(N_F \Vert N_M \Vert N_H)$.		

FIGURE 4: Login and Authentication phase of AMAPG

7) Insider adversary

Besides the transferred messages over a public channel, an insider adversary could access the transferred messages over a secure channel in the registration phase also. The target of such adversary could be extracting the user password PSW_M. However, the only information that an insider gets in this way, compared to any other adversary which has no access to the secure channel, are $RID = h(ID_M \| (PSW_M \oplus R_N))$ and $HID = h(RID \| SK_{HA})$. Given that R_N is a fresh nonce, even if PSW_M has low entropy, it will not be feasible for the insider attacker to guess the user's password. Even assuming that the adversary also gets access to the user smart card SC and therefore knows R_N, yet the complexity of guessing PSW_M will be $2^{|PSW_M + ID_M|}$, where $|PSW_M + ID_M|$ is the joint entropy of PSW_M and ID_M and could be enough large to make it infeasible to be guessed in polynomial time.

8) Stolen smart card attack

The ability of any adversary with access to the user's smart card, is not more than an insider adversary with access to smart card. Hence, for such an adversary, the complexity of guessing PSW_M correct will be $2^{|PSW_M + ID_M|}$.

9) Forward secrecy

Given that the proposed protocol i.e. AMAPG shares session key only using symmetric key-cryptography, i.e. hash function, and also we do not update the shared parameters per session, hence, similar to any other protocol in this context it is not possible to provide this property. It should be noted it is possible to easily provide this property when the protocol uses a public key primitive such as elliptic curve cryptography (ECC). However, such component will be much costlier than hash function. However, if forward secrecy is vital for a user, then we suggest to not use AMAPG.

B. FORMAL SECURITY ANALYSIS

Here, we formally prove the security of AMAPG using BAN logic and Scyther tool.

1) Security proof through BAN logic

In 1990, Burrows, Abadi, and Needham [46] presented a logic-based approach to verify the security of protocols named BAN logic. In BAN logic, the protocol and its security goals were described using BAN logic notations and using its logic rules it is deduced whether the the protocol participants believe the protocol's objectives. Security proof is done by BAN logic method as follows:

1) Writing the protocol using BAN logic notations.
2) Writing an idealized version of the protocol. In the idealized version of the protocol, plain parameters of the protocol are ignored.
3) Specify the assumptions as well as the security objectives of the protocol.
4) The rules in BAN logic are written as fractions such as $\frac{A}{B}$ and these rules are used in such a way that using protocol messages and assumptions, an attempt is made to make a rule numerator i.e. A. In this case, it is inferred that the denominator of the rule i.e. B is also deduced. In this step, using the protocol messages and assumption and based on BAN logic rules efforts are being made to achieve the security objectives set out in the protocol.

TABLE 2: Notations used in AMAPG's security proof through BAN logic

Notation	Description
$P \mid\equiv X$	P believes X
$P \triangleleft X$	P receives X
$P \mid\sim X$	P once said X
$P \Rightarrow X$	P controls X
$\#(X)$	X is fresh
$\langle X \rangle_Y$	Combination of X and Y
$\{X\}_Y$	Encryption of X with Y
$P \overset{K}{\leftrightarrow} Q$	K is a shared secret between P and Q
$Y = (X)_h$	Y is hash of X

TABLE 3: BAN logic postulates used in this paper

Rule's name	Rule description
P_1	$\frac{A \mid\equiv (A \overset{K}{\leftrightarrow} B), A \triangleleft \{X\}_K}{A \mid\equiv B \mid\sim X}$
P_2	$\frac{A \mid\equiv \#(X)}{A \mid\equiv \#(X, Y)}$
P_3	$\frac{A \mid\equiv B \mid\sim X, A \mid\equiv \#(X)}{A \mid\equiv B \mid\equiv X}$
P_4	$\frac{A \mid\equiv (X, Y)}{A \mid\equiv (X)}$
P_5	$\frac{A \mid\equiv X, A \mid\equiv Y}{A \mid\equiv (X, Y)}$
P_6	$\frac{A \mid\equiv (X)}{A \mid\equiv (X)_h}$
P_7	$\frac{A \mid\equiv B \mid\equiv X, A \mid\equiv B \Rightarrow X}{A \mid\equiv X}$

Here, we prove AMAPG's security through BAN logic using notations and some BAN logic rules represented in Table 2 and Table 3 respectively. Precisely, we prove that the protocol's parties i.e. MU and FA can retrieve the mutuality belief in their shared key i.e. SK.

AMAPG using BAN logic format

Since the registration phase of AMAPG is done in a secure channel, here, we only prove the security of AMAPG's login and authentication phase.

- $M_1 : FA \triangleleft T_M, ID_H, AM = \{T_M, N_M\}_{HID}, V_1 = \{T_M, N_M\}_{HID}$
- $M_2 : HA \triangleleft T_F, ID_F, A_F = \{A_M, T_F, N_F\}_{SK_{FA}}, V_1 = \{T_M, N_M\}_{HID}, V_2 = \{A_F, T_F, N_F, V_1, A_M\}_{SK_{FA}}$
- $M_3 : FA \triangleleft T_H, A_H = \{N_F, N_M, A_M, T_F\}_{SK_{FA}}, N_H, V_3 = \{ID_H, N_H, N_F, A_H, T_H\}_{SK_{FA}}, V_4 = \{N_F, ID_H, N_M, N_H, T_H\}_{HID}$
- $M_4 : MU \triangleleft N_H, A'_F, V_4 = \{N_F, ID_H, N_M, N_H, T_H\}_{HID}$

Idealization of AMAPG

- $IM_1 : FA \lhd AM = \{T_M, N_M\}_{HID}, V_1 = \{T_M, N_M\}_{HID}$
- $IM_2 : HA \lhd A_F = \{A_M, T_F, N_F\}_{SK_{FA}}, V_1 = \{T_M, N_M\}_{HID}, V_2 = \{A_F, T_F, N_F, V_1, A_M\}_{SK_{FA}}$
- $IM_3 : FA \lhd A_H = \{N_F, N_M, A_M, T_F\}_{SK_{FA}}$, $V_3 = \{ID_H, N_H, N_F, A_H, T_H\}_{SK_{FA}}$, $V_4 = \{N_F, ID_H, N_M, N_H, T_H\}_{HID}$
- $IM_4 : MU \lhd A'_F, V_4 = \{N_F, ID_H, N_M, N_H, T_H\}_{HID}$

AMAPG assumptions and security objectives

AMAPG's assumptions and security objectives are as follows:

- A_1: $MU \mid\equiv \#(N_M)$
- A_2: $MU \mid\equiv \#(T_M)$
- A_3: $FA \mid\equiv \#(N_F)$
- A_4: $FA \mid\equiv \#(T_F)$
- A_5: $HA \mid\equiv \#(N_H)$
- A_6: $HA \mid\equiv \#(T_H)$
- A_7: $MU \mid\equiv (MU \overset{HID}{\longleftrightarrow} HA)$
- A_8: $HA \mid\equiv (HA \overset{HID}{\longleftrightarrow} MU)$
- A_9: $FA \mid\equiv (FA \xleftrightarrow{SK_{FA}=h(ID_F \| SK_{HA})} HA)$
- A_{10}: $HA \mid\equiv (HA \xleftrightarrow{SK_{FA}=h(ID_F \| SK_{HA})} FA)$
- A_{11}: $MU \mid\equiv HA \Rightarrow SK$
- A_{12}: $FA \mid\equiv HA \Rightarrow SK$

To prove the security of AMAPG, the following security objectives must be satisfied.

- O_1: $FA \mid\equiv SK$
- O_2: $MU \mid\equiv SK$

To deduce the security objectives of AMAPG, we do as follows:

2) Retrieving security objective O_1

Given IM_3 which is $FA \lhd \{ID_H, N_H, N_F, A_H, T_H\}_{SK_{FA}}$ and $A9$ and based on postulate P_1 we get:
D_1: $FA \mid\equiv HA \mid\sim \{ID_H, N_H, N_F, A_H, T_H\}$.
From A_3 and based on P_2, we deduce $D_2 : FA \mid\equiv \#(\{ID_H, N_H, N_F, A_H, T_H\})$. From D_1 and D_2 and based on P_3 we get:
D_3: $FA \mid\equiv HA \mid\equiv \{ID_H, N_H, N_F, A_H, T_H\}$.
Given D_3 based on P_4, D_4 and D_5 is concluded as below:
D_4: $FA \mid\equiv HA \mid\equiv N_F$.
D_5: $FA \mid\equiv HA \mid\equiv N_H$.
Given IM_3 which is $FA \lhd \{N_F, N_M, A_M, T_F\}_{SK_{FA}}$ and $A9$ and based on postulate P_1 we get:
D_6: $FA \mid\equiv HA \mid\sim \{N_F, N_M, A_M, T_F\}$.
From A_3 and based on P_2, we deduce $D_7 : FA \mid\equiv \#(\{N_F, N_M, A_M, T_F\})$. From D_6 and D_7 and based on P_3 we get:
D_8: $FA \mid\equiv HA \mid\equiv \{N_F, N_M, A_M, T_F\}$.
Given D_8 based on P_4, D_9 is concluded as below:
D_9: $FA \mid\equiv HA \mid\equiv N_M$.
Using D_4, D_5 and D_9 based on P_5, we retrieve D_{10} as $D_{10} : FA \mid\equiv HA \mid\equiv (N_M, N_H, N_F)$. Given D_{10} based on P_6, we get $D_{11} = FA \mid\equiv HA \mid\equiv (N_M, N_H, N_F)_h = SK$. Considering D_{11}, A_{12} based on P_7, we deduce $D_{12} : FA \mid\equiv SK$ which is same O_1. Security objective O_1 indicates that FA believes in a shared key i.e. SK.

3) Retrieving security objective O_2

Given IM_4 which is $MU \lhd \{N_F, ID_H, N_M, N_H, T_H\}_{HID}$ and $A7$ and based on postulate P_1 we get:
D_{13}: $MU \mid\equiv HA \mid\sim \{N_F, ID_H, N_M, N_H, T_H\}$.
From A_1 and based on P_2, we deduce $D_{14} : MU \mid\equiv \#(\{N_F, ID_H, N_M, N_H, T_H\})$. From D_{13} and D_{14} and based on P_3 we get:
D_{15}: $MA \mid\equiv HA \mid\equiv \{N_F, ID_H, N_M, N_H, T_H\}$.
Given D_{15} based on P_4, D_{16}, D_{17} and D_{18} is concluded as below:
D_{16}: $MU \mid\equiv HA \mid\equiv N_F$.
D_{17}: $MU \mid\equiv HA \mid\equiv N_M$.
D_{18}: $MU \mid\equiv HA \mid\equiv N_H$.
Using D_{16}, D_{17} and D_{18} based on P_5, we retrieve D_{19} as $D_{19} : MU \mid\equiv HA \mid\equiv (N_M, N_H, N_F)$. Given D_{19} based on P_6, we get $D_{20} : MU \mid\equiv HA \mid\equiv (N_M, N_H, N_F)_h = SK$. Considering D_{20} and A_{11} based on P_7, we deduce $D_{21} : MU \mid\equiv SK$ which is same O_2. Security objective O_2 indicates that MU believes in a shared key i.e. SK.

4) Security proof using Scuther

Scyther [47] is a security tool written in the Python language that is used to check the correctness and security of protocols. The protocol modeling language in this tool is Security Protocol Description Language (SPDL). SPDL allows the protocol designer to examine the security features of the protocol. The protocol designer can examine the security objectives set in the protocol, such as maintaining the confidentiality of a secret value. If the designed protocol does not set any security goals for it, Scyther automatically adds security goals to it. Table 4 represents some of the security claims that can be made with the Scyther tool.

To model the proposed protocol, it is sufficient to state the three parties participating in the protocol i.e. MU, FA and HA in different roles, to express the messages that are sent and received between them in SPDL respectively, and to make security claims for each role. Thereafter, Scyther tool executes the written code.

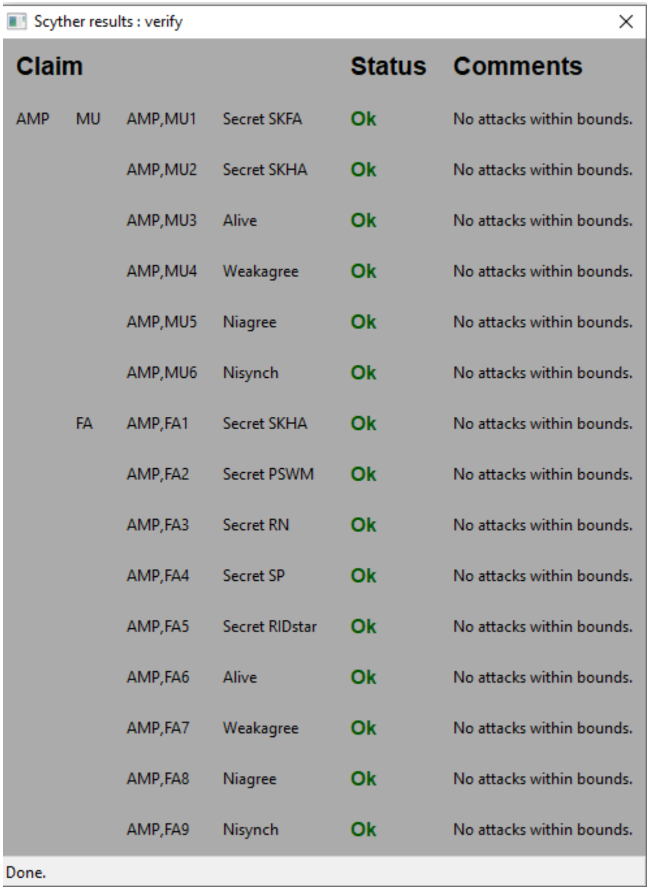
As can be seen in Figures 5 and 6, Scyther tool cannot find any security pitfalls in AMAPG.

VII. SECURITY AND PERFORMANCE COMPARISON

Table 5, compares our proposed protocol with its predecessor and also other recent hash-based GLOMONET authentication protocols. From the security point of view, we have shown that Shashidhara *et al.*'s protocol suffers from several important drawbacks including traceability, impersonation, stolen smart card and the lack of forward secrecy. On the other hand, the detailed security analysis of AMAPG and its formal security verification using Scyther tool confirms that it provides desired security against different attacks. To keep

TABLE 4: Scyther tool's security claims

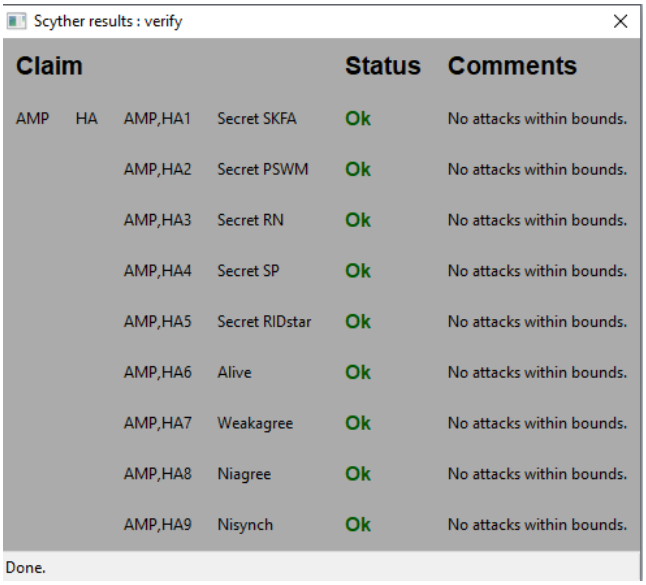
Claim	Description
Secret	means that the protocol keeps the secret value safe and its value is not accessible to others
Niagree	means that the sender and receiver agree on the secret values exchanged and the results of the analysis justify the validity of this claim
Nisynch	means that the sending and receiving events are executed by the roles in order and with the main content in question
Alive	means that if one role has finished one run of protocol, the other role has already started to play
Weakagree	When one role completes a run, the other role has already started, and the first role is apparently related to the second role



Claim				Status	Comments
AMP	MU	AMP,MU1	Secret SKFA	Ok	No attacks within bounds.
		AMP,MU2	Secret SKHA	Ok	No attacks within bounds.
		AMP,MU3	Alive	Ok	No attacks within bounds.
		AMP,MU4	Weakagree	Ok	No attacks within bounds.
		AMP,MU5	Niagree	Ok	No attacks within bounds.
		AMP,MU6	Nisynch	Ok	No attacks within bounds.
	FA	AMP,FA1	Secret SKHA	Ok	No attacks within bounds.
		AMP,FA2	Secret PSWM	Ok	No attacks within bounds.
		AMP,FA3	Secret RN	Ok	No attacks within bounds.
		AMP,FA4	Secret SP	Ok	No attacks within bounds.
		AMP,FA5	Secret RIDstar	Ok	No attacks within bounds.
		AMP,FA6	Alive	Ok	No attacks within bounds.
		AMP,FA7	Weakagree	Ok	No attacks within bounds.
		AMP,FA8	Niagree	Ok	No attacks within bounds.
		AMP,FA9	Nisynch	Ok	No attacks within bounds.

Done.

FIGURE 5: Security evaluation of AMAPG via Scyther



Claim				Status	Comments
AMP	HA	AMP,HA1	Secret SKFA	Ok	No attacks within bounds.
		AMP,HA2	Secret PSWM	Ok	No attacks within bounds.
		AMP,HA3	Secret RN	Ok	No attacks within bounds.
		AMP,HA4	Secret SP	Ok	No attacks within bounds.
		AMP,HA5	Secret RIDstar	Ok	No attacks within bounds.
		AMP,HA6	Alive	Ok	No attacks within bounds.
		AMP,HA7	Weakagree	Ok	No attacks within bounds.
		AMP,HA8	Niagree	Ok	No attacks within bounds.
		AMP,HA9	Nisynch	Ok	No attacks within bounds.

Done.

FIGURE 6: Continuation of security evaluation of AMAPG via Scyther

AMAPG as much as possible similar to its predecessor protocol, i.e. Shashidhara *et al.*'s protocol, from the security point of view, we kept the used component identical which is one-way hash function as the main primitive to provide desired security. Hence, in the term of the required area to implement the cryptographic primitive all of protocols compared in Table 5 are identical. However, in the term of required memory as depicted in Table 6 and Figure 7, Lee *et al.*, Kang *et al.* and AMAPG schemes requires 320, 480 and 480 bits memory capacity respectively. As shown in this table, AMAPG is better than its predecessor because Shashidhara *et al.*'s protocol stores SP, PV, R_N, K_{MU} while AMAPG stores SP, PV, R_N.

In the term of computational costs, as depicted in Table 7 and Figure 8, the Baig *et al.* [24] and AMAPG schemes require the least amount of time for calculations, respectively. Focusing on the MU computation analysis as it is the resource constrain device, it can easily seen in Table 7, the Baig *et al.* [24] and AMAPG schemes in their MU side require $6T_h$ and $9T_h$, respectively which are the fastest. The time of the hash function i.e. T_h is considered to be 0.038 milliseconds using [25]. Comparing AMAPG with its predecessor i.e. Sashidhara *et al.* shows the mobile user does 7 calls to $h(.)$, the foreign agent does 4 calls to $h(.)$ and the home agent does 10 calls to $h(.)$. On the other hand, in AMAPG the mobile user, the foreign agent and the home agent respectively does 6, 4 and 8 calls to $h(.)$ which shows that AMAPG outperforms Shashidhara *et al.*'s protocol in the term of computational costs.

Assuming that the output length of the hash function $h(.)$ and random numbers is 160 bits, the length of identifier is 128 bits and the timestamp is 64 bits, as can be seen in

Table 8 and Figure 9, Shashidhara *et al.* [1] and AMAPG enforce lower computational costs, respectively. Focusing on the MU communication costs as it is the resource constrain device, it can easily seen in Table 8, MU in Shashidhara *et al.*'s protocol and AMAPG in login and authentication phase sends 448 and 512 bits respectively. The 64 bits that MU used in the proposed protocol more than its predecessor is due to its improved security. Precisely, in Shashidhara *et al.*'s protocol, MU transfers 448 bits to FA, FA transfers 608 bits to HA, HA transfers 480 bits to FA and finally FA transfers 320 bits to MU. On the other hand, in AMAPG, MU transfers 512 bits to FA, FA transfers 672 bits to HA, HA transfers 704 bits to FA and finally FA transfers 480 bits to MU. Although AMAPG has slightly increased communication costs, it has been able to reduce computational costs on the MU and HA. Also, as shown in Table 5, it has been able to provide complete security.

A. SCALABILITY ANALYSIS

AMAPG is a symmetric cryptography based protocol and in this class of protocols, to respect the users privacy the user should send its credentials masked, otherwise it will be traced by the adversary. To identify the user, the server needs to search over the stored records which may not be very efficient for a large scale protocol. However, in the proposed protocol the search is done by the home agent which is less constrained compared to the end users. To reduce the search time to $\mathcal{O}(1)$, it is possible to use dynamic identifier or use asymmetric cryptography, however each of them has its own pros and cons also.

VIII. CONCLUSION

In this paper, Shashidhara *et al.*'s protocol, which was proposed for GLObal MObility NETwork (GLOMONET), was evaluated in the term of security against various attacks. These security assessments demonstrated the protocol's vulnerabilities to impersonation, stolen smart card attacks, the lack of forward secrecy and traceability attacks. Then, to remedy the protocol and strengthen its security against the attacks described in this paper and other known attacks, we proposed an enhanced protocol named AMAPG. Our detailed security analysis and conducted performance analysis shows that AMAPG is superior to Shashidhara *et al.*'s protocol in the term of security which is very important and even in computational cost, although Shashidhara *et al.* requires lower communication cost comparatively.

To provide security, similar to Shashidhara *et al.*'s protocol, AMAPG also only uses one-way hash functions as the core of the security. Hence, it could be very lightweight and applicable in many applications that are targeting constrained environments. However, a drawback of such a protocol, which is only uses symmetric encryption and in the same time aiming to provide user anonymity, is the problem of scalability in the server side (HA in these protocols), because the server should search whole database to find the target user. A solution could be sending dynamic identifier which has its own pros and cons. Another solution is to use public key approaches such as Elliptic Curve Cryptography (ECC). However, such solutions are also very resource consuming and may not be suitable for many applications. Hence, we leave it to the user to choose the proper protocol for his/her application.

On the other hand, any new protocol should be extensively analysed by independent researchers and we also invite to analyse AMAPG as a future work. Besides, in the AMAPG we considered the foreign agent to be honest. Hence, the session key is shared between the user, the foreign agent and the home agent. However, in some applications the user should not trust the foreign agent. In such applications, it could be better to revise the protocol such that the foreign agent can not identify the shared key. We leave this as another opportunity for a future work. At last but not at least, given that the proposed protocol mainly uses hash function through its computations and any transferred data is masked, the home agent should search over whole its records to identify the user. Although the proposed protocol guarantees the user's privacy in this way but violates the protocol's scalability. Hence, it may be better to investigate a solution to provide a trade-off between security and scalability in a future work, although AMAPG could be a proper solution for any applications for which the anonymity is important but scalability is not matter.

REFERENCES

[1] 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 Netw. Appl., vol. 13, no. 6, pp. 1943–1966, 2020.

[2] S. Suzuki and K. Nakada, "An authentication technique based on distributed security management for the global mobility network," IEEE Journal on Selected Areas in Communications, vol. 15, no. 8, pp. 1608–1617, 1997.

[3] 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, 2004.

[4] 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, 2006.

[5] 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, 2008.

[6] 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, 2012.

[7] 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, 2014.

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

[9] C.-T. Li and C.-C. Lee, "A novel user authentication and privacy preserving scheme with smart cards for wireless communications," Mathematical and Computer Modelling, vol. 55, no. 1-2, pp. 35–44, 2012.

[10] 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. 3, pp. 367–374, 2011.

[11] 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, 2013.

TABLE 5: Security properties comparison of the improved protocol and related hash-based GLOMONET authentication protocols where ✓ and × represent Resistant/Yes and Vulnerable/No respectively

Security properties	[23]	[24]	[25]	[1]	AMPAG
Impersonation and replay attack resistance	×	×	✓	×	✓
Traceability and anonymity contradiction attack resistance	×	×	✓	×	✓
Stolen smart card attack resistance	✓	✓	✓	×	✓
De-synchronization attack resistance	×	×	✓	✓	✓
Secret disclosure attack resistance	✓	✓	✓	✓	✓
Insider attacks resistance	✓	✓	✓	✓	✓
Mutual authentication property	×	×	✓	✓	✓

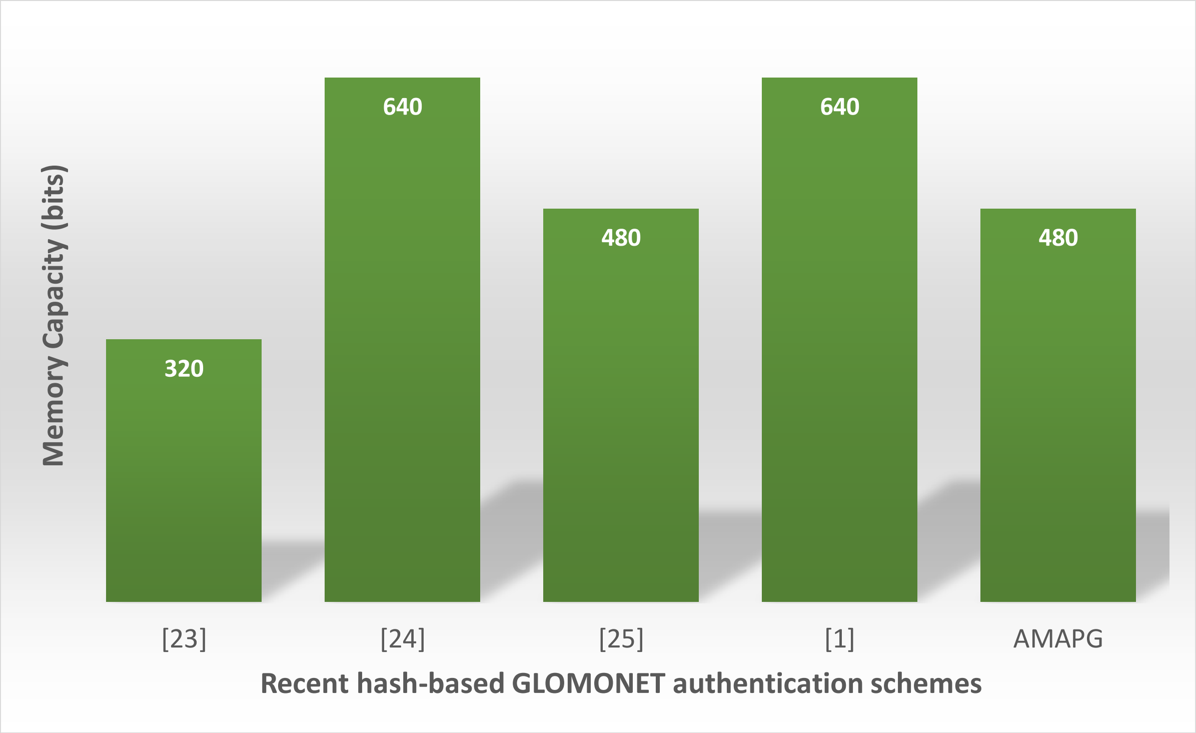


FIGURE 7: The memory capacity comparison of AMAPG with recent hash-based GLOMONET authentication protocols.

TABLE 6: Memory capacity comparison of the improved protocol and related hash-based GLOMONET authentication protocols

Protocol	[23]	[24]	[25]	[1]	AMAPG
Memory capacity(bits)	320	640	480	640	480

[12] 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, 2013.

[13] 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, 2013.

[14] 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, 2015.

[15] F. Wu, L. Xu, S. Kumari, X. Li, A. K. Das, M. K. Khan, M. Karuppiah, and R. Baliyan, "A novel and provably secure authentication and key agreement scheme with user anonymity for global mobility networks," Security and Communication Networks, vol. 9, no. 16, pp. 3527–3542, 2016.

[16] A. Almuhaideb, P. D. Le, and B. Srinivasan, "Passport/Visa: authentication and authorisation tokens for ubiquitous wireless communications," in International Conference on Mobile and Ubiquitous Systems: Computing, Networking, and Services, pp. 224–236, Springer, 2010.

[17] A. Almuhaideb, B. Srinivasan, P. D. Le, M. Alhabeeb, and W. Alfehaid, "A hybrid mobile authentication model for ubiquitous networking," in 2015 IEEE Trustcom/BigDataSE/ISPA, vol. 1, pp. 360–367, IEEE, 2015.

[18] 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, 2014.

[19] 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

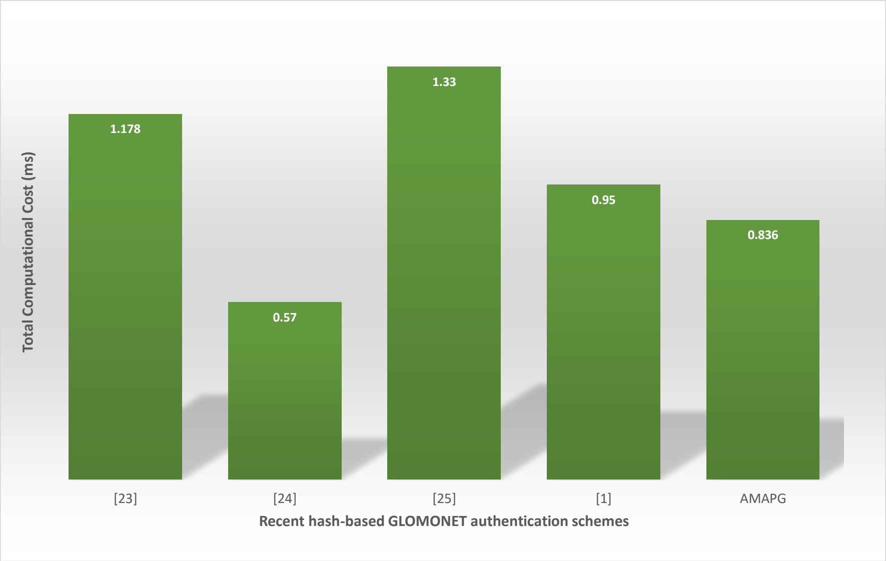


FIGURE 8: The computational cost comparison of AMAPG with recent hash-based GLOMONET authentication protocols.

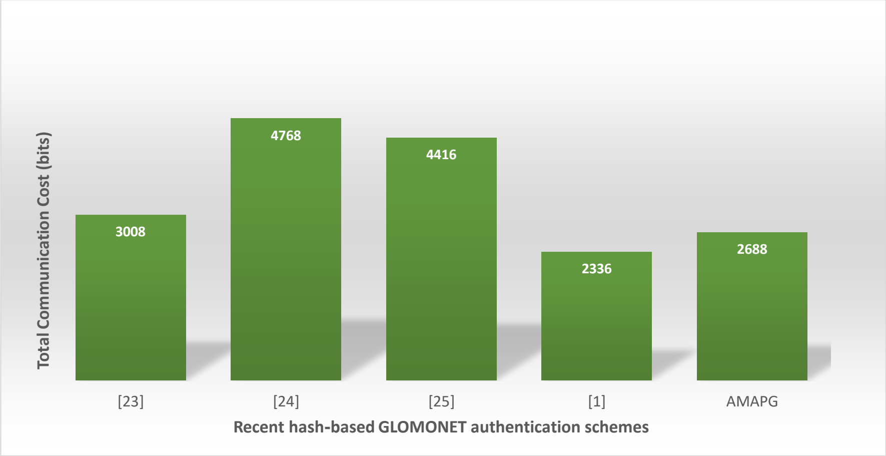


FIGURE 9: The communication cost comparison of AMAPG with recent hash-based GLOMONET authentication protocols.

for roaming service in smart city," Personal and Ubiquitous Computing, vol. 21, no. 5, pp. 791–805, 2017.

[20] 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, 2017.

[21] 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, 2009.

[22] P. Gope, R.-H. Hsu, J. Lee, and T. Q. Quek, "Energy efficient mutual authentication and key agreement scheme with strong anonymity support for secure ubiquitous roaming services," in 2016 11th International Conference on Availability, Reliability and Security (ARES), pp. 247–252, IEEE, 2016.

[23] 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, 2017.

[24] 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, p. e0196061, 2018.

[25] 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, p. e0247441, 2021.

[26] W. Al Amiri, M. Baza, K. Banawan, M. Mahmoud, W. Alasmary, and K. Akkaya, "Towards secure smart parking system using blockchain technology," in 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), pp. 1–2, IEEE, 2020.

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

[28] 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 2019 IEEE International Conference on Blockchain (Blockchain), pp. 504–509, IEEE, 2019.

[29] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," ACM Computing Surveys (CSUR), vol. 52, no. 3, pp. 1–34, 2019.

[30] 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 Transactions on Dependable and

TABLE 7: Computational comparison of the improved protocol and related hash-based GLOMONET authentication protocols, where C., R., L.A. and T.T. respectively denote Component, Registration phase, Login & Authentication phase and Total Time (ms). In this table $T_h = 0.038(ms)$ based on [25]

Protocol	C.	R.	L.A.	T.T.(ms)
Lee *et al.* [23]	MU	$2T_h$	$10T_h$	$31T_h = 1.178$
	FA	-	$8T_h$	
	HA	$2T_h$	$9T_h$	
Baig *et al.* [24]	MU	T_h	$5T_h$	$15T_h = 0.57$
	FA	-	$2T_h$	
	HA	$2T_h$	$5T_h$	
Kang *et al.* [25]	MU	$3T_h$	$13T_h$	$35T_h = 1.33$
	FA	-	$5T_h$	
	HA	$2T_h$	$12T_h$	
Shashidhara [1]	MU	$3T_h$	$7T_h$	$25T_h = 0.95$
	FA	-	$4T_h$	
	HA	T_h	$10T_h$	
AMAPG	MU	$3T_h$	$6T_h$	$22T_h = 0.836$
	FA	-	$4T_h$	
	HA	T_h	$8T_h$	

TABLE 8: Communication comparison of the improved protocol and related hash-based GLOMONET authentication protocols, where C., R. and L.A. respectively denote Component, Registration phase and Login & Authentication pahse

Protocol	C.	R.	L.A.	Total(bits)
Lee *et al.* [23]	MU	160	800	3008
	FA	-	1408	
	HA	160	480	
Baig *et al.* [24]	MU	288	672	4768
	FA	-	2304	
	HA	480	1024	
Kang *et al.* [25]	MU	320	704	4416
	FA	-	2208	
	HA	160	1024	
Shashidhara *et al.* [1]	MU	160	448	2336
	FA	-	928	
	HA	320	480	
AMAPG	MU	160	512	2688
	FA	-	1152	
	HA	160	704	

Secure Computing, 2020.

[31] 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, 2016.

[32] D. Guo and F. Wen, "A more robust authentication scheme for roaming service in global mobility networks using ECC," IJ Network Security, vol. 18, no. 2, pp. 217–223, 2016.

[33] R. Madhusudhan, "An efficient and secure authentication scheme with user anonymity for roaming service in global mobile networks," in Proceedings of the 6th International Conference on Communication and Network Security, pp. 119–126, 2016.

[34] 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, 2017.

[35] S. Bojjagani and V. Sastry, "A secure end-to-end SMS-based mobile banking protocol," International journal of communication systems, vol. 30, no. 15, p. e3302, 2017.

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

[37] 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, 2017.

[38] 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, p. e3361, 2017.

[39] 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, pp. 2185–2212, 2020.

[40] R. Madhusudhan and R. Shashidhara, "A secure anonymous authentication protocol for roaming service in resource-constrained mobility environments," Arabian Journal for Science and Engineering, pp. 1–22, 2019.

[41] G. Xu, J. Liu, Y. Lu, X. Zeng, Y. Zhang, and X. Li, "A novel efficient MAKA protocol with desynchronization for anonymous roaming service in global mobility networks," Journal of Network and Computer Applications, vol. 107, pp. 83–92, 2018.

[42] D. Dolev and A. Yao, "On the security of public key protocols," IEEE Transactions on information theory, vol. 29, no. 2, pp. 198–208, 1983.

[43] S. Rana, M. S. Obaidat, D. Mishra, S. Mukhopadhyay, and B. Sadoun, "Computational efficient authenticated digital content distribution frameworks for DRM systems: Review and outlook," IEEE Systems Journal, 2020.

[44] A. Chaturvedi, D. Mishra, S. Jangirala, and S. Mukhopadhyay, "A privacy preserving biometric-based three-factor remote user authenticated key agreement scheme," Journal of Information Security and Applications, vol. 32, pp. 15–26, 2017.

[45] M. Safkhani and N. Bagheri, "Generalized desynchronization attack on UMAP: application to rcia, kmap, SLAP and sasi$^+$ protocols," IACR Cryptol. ePrint Arch., vol. 2016, p. 905, 2016.

[46] M. Burrows, M. Abadi, and R. M. Needham, "A logic of authentication," Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences, vol. 426, no. 1871, pp. 233–271, 1989.

[47] C. J. Cremers, "The scyther tool: Verification, falsification, and analysis of security protocols," in International conference on computer aided verification, pp. 414–418, Springer, 2008.

AMIR MASOUD RAHMANI received his B.Sc. in Computer Engineering from Amir Kabir University, Tehran, in 1996, the M.Sc. in Computer Engineering from Sharif University of Technology, Tehran, in 1998 and the Ph.D. degree in Computer Engineering from IAU University, Tehran, in 2005. Currently, he is a Professor in the Department of Computer Engineering at the IAU University. He is the author/co-author of more than 200 publications in technical journals and conferences. His research interests are in the areas of distributed systems, Internet of things and evolutionary computing.

MOKHTAR MOHAMMADI received the B.Sc. degree in computer engineering from Shahed University, Tehran, Iran, in 2003, the M.Sc. degree in computer engineering from Shahid Beheshti University, Tehran, Iran, in 2012, and the Ph.D. degree in computer engineering from Shahrood University of Technology, Shahrood, Iran, in 2018. His current research interests include signal processing, time-frequency analysis, and machine learning. He is currently with the Department of Information Technology, Lebanese French University-Erbil, Iraq.

JAN LANSKY received the M.Sc. degree and the Ph.D. degree in computer science: software systems from Charles University, Prague, Czech Republic, in 2005 and 2009, respectively. He has been a Professor with Department of Computer Science and Mathematics, Faculty of Economic Studies, University of Finance and Administration, Prague, Czech Republic, since March 2009. He has been a Head of the department since September 2014. His research interests include cryptocurrencies, text compression, and databases.

STANISLAVA MILDEOVA graduated from the University of Economics in Prague. She is associate professor and deputy head of the Department of Informatics and Mathematics at the Faculty of Economic Studies at the University of Finance and Administration Prague, Czech Republic, since 2017. In her work, she focuses on applied informatics and systems science with a focus on systems dynamics. She has been the editor in chief of the Scopus journal Acta Informatica Pragensia.

MASOUMEH SAFKHANI received the Ph.D. degree in Electrical Engineering from the Iran University of Science and Technology, in 2012, with the security analysis of RFID protocols as her major field. She is currently an Associate Professor with the Computer Engineering Department, Shahid Rajaee Teacher Training University, Tehran, Iran. Her current research interests include the security analysis of lightweight and ultra-lightweight protocols, targeting constrained environments, such as RFID, the IoT, VANET, and WSN. She is the author/co-author of over 70 technical articles in information security and cryptology in major international journals and conferences.

SARU KUMARI received the Ph.D. degree in mathematics from Chaudhary Charan Singh University, Meerut, India, in 2012. She is currently an Assistant Professor with the Department of Mathematics, Chaudhary Charan Singh University. She has published more than 133 research articles in reputed International journals and conferences, including 115 publications in SCI-indexed journals. Her current research interests include information security and applied cryptography. She is a Technical Program Committee member for many International conferences. She has served as a Lead/Guest Editor of four special issues in SCI journals of Elsevier, Springer, and Wiley. She is on the Editorial Board of more than 12 journals of international repute, including seven SCI journals.

SARKHEL H.TAHER KARIM received his B.Sc. degree in Computer Science from the University of Sulaimani, Sulaymaniyah, Iraq, in 2007, 3rd out of twenty graduated. He started working at the University of Sulaimani 2007-2009. He did his master degree 2011 in Computer Science, Faculty of Management and Information Technology, Jamia Hamdard University, New Delhi, India. Lecturer at University of Sulaimani, College of Science, Computer Department 2011-2016. Currently, he is Head of Computer Department College of Science, University of Halabja, Halabja, Iraq since 2016. His current research interests include Recommender Systems, Social Network Analysis, Speech, Dialogue and Natural Language Processing, Neural Network, Deep Learning and Internet of Things.

MEHDI HOSSEINZADEH received his B.Sc. degree in computer hardware engineering, from Islamic Azad University, Dezfol branch, Iran in 2003. He also received his M.Sc. and the Ph.D. degrees in computer system architecture from the Science and Research Branch, Islamic Azad University, Tehran, Iran in 2005 and 2008, respectively. He is currently an Associate professor in Iran University of Medical Sciences (IUMS), Tehran, Iran. He is the author/co-author of more than 120 publications in technical journals and conferences, and his research interests include SDN, Information Technology, Data Mining, Big data analytics, E-Commerce, E-Marketing, and Social Networks.