Lightweight and Energy-Efficient Mutual Authentication and Key Agreement Scheme With User Anonymity for...

Article *in* IEEE Systems Journal · April 2015

DOI: 10.1109/JSYST.2015.2416396

Prosanta Gope
National University of Singapore

Lightweight and Energy-Efficient Mutual Authentication and Key Agreement Scheme With User Anonymity for Secure Communication in Global Mobility Networks

Prosanta Gope and Tzonelih Hwang

***Abstract*—User authentication is an imperative security mechanism for recognizing legal roaming users. However, designing an expeditious anonymous-user authentication scheme in the global mobility networking (GLOMONET) environment is always a challenging task. Because, due to the broadcast nature of the wireless channels, wireless networks are often susceptible to various attacks and mobile devices powered by batteries that have limited communication, processing, and storage capabilities. In this paper, we propose a lightweight, secure, and an expeditious authentication scheme, which can preserve the user anonymity for roaming services in GLOMONET. In this regard, we use the low-cost cryptographic primitives such as one-way hash functions and EXCLUSIVE-OR operations to accomplish goals, which is more suitable for battery-powered mobile devices. Although some authentication protocols for GLOMONET security have already been proposed, however, they are unable to achieve the desired imperative security properties, such as anonymity, privacy against eavesdroppers, communication security, etc. As a consequence of that, they are vulnerable to various security issues. Security and performance analyses show that our proposed scheme is secure and even more efficient, as compared with other related authentication schemes in GLOMONET.**

***Index Terms*—Anonymity, authentication, global mobility networks (GLOMONETs), privacy, smart card.**

I. Introduction

GLOBAL mobility network (GLOMONET) provides global roaming service that permits a legitimate mobile user to use ubiquitous services provided by the home agent (HA) in a foreign agent (FA). However, in the rapid development of such environment, many security problems, such as user's privacy, have predominantly brought to researchers' attention. Hence, mutual authentication with anonymity in GLOMONET is an imperative issue. In order to resolve this issue, cryptographers around the world often like to come up with computationally complex ideas based on symmetric/asymmetric encryption/decryption or even would like to use modular operation during their design of the authentication protocol. However, these ideas are often considered to be incompetent in some cases, where the authentication entities such as mobile devices cannot afford higher computation, but at the same time demand for a secure and even expeditious authentication environment by preserving the user anonymity [1] in GLOMONET. Therefore, it is greatly desirable to have a mutual authentication and key agreement (MAKA) scheme for GLOMONETs, which can deal with various security issues, such as forgery attack, known session key attack, backward and forward secrecy, smart card loss problem, etc. Besides, the protocol should also encompass limited computational burden with the lower execution time and reasonable communication overhead (number of data flows or message exchanges during the authentication process).

A. Related Work

Over the past few years, some interesting authentication and key agreement protocols for GLOMONETs have been proposed [2]–[16]. Particularly, in 2004, Zhu and Ma proposed a wireless security protocol based on smart card and featuring user anonymity [2]. Unfortunately, Lee *et al.* [3] pointed out, in 2006, that the protocol by Zhu and Ma [2] does not achieve mutual authentication and is also subjected to the forgery attack. Lee *et al.* also proposed a slightly modified version of the protocol by Zhu and Ma to remedy the identified shortcomings. However, in [4], it was shown that the scheme by Zhu and Ma and the scheme by Lee *et al.* fail to provide user anonymity, and Wu *et al.* proposed an enhanced scheme by providing an effective remedy. Independently, in [5], Chang *et al.* showed that the scheme in [3] cannot provide user anonymity, under the forgery attack, and also proposed an enhanced lightweight authentication scheme based on the hash function and EXCLUSIVE-OR operation. Unfortunately, Youn *et al.* found that the scheme in [5] fails to achieve user anonymity under four attack strategies [6]. Besides, the protocol even cannot resist several important security attacks, such as forgery attack, known session key attack, forward and backward secrecy, etc. Furthermore, if the smart card is lost or stolen, the attacker can always recover all the secrets, including the identity of the subscriber. In 2008, Tang and Wu proposed

Manuscript received April 24, 2014; revised July 22, 2014, November 9, 2014, and January 12, 2015; accepted March 22, 2015. This work was supported by the National Science Council of Taiwan under Contract NSC MOST 103-2221-E-006-177.

The authors are with the Department of Computer Science and Information Engineering, National Cheng Kung University, Tainan 701, Taiwan (e-mail: prosanta.nitdgp@gmail.com; hwangtl@ismail.csie.ncku.edu.tw).

Digital Object Identifier 10.1109/JSYST.2015.2416396

an authentication protocol for mobile networks [7], and they claimed that their scheme is immune to all known types of attacks. However, Lu and Zhou [8] showed that the scheme in [7] suffers from replication attack. Now, at the end of 2011, Zhou and Xu independently proposed a MAKA scheme [9], based on the decisional Diffie–Hellman (DDH) assumption. However, due to inclusion of the exponential operation, the protocol also encompasses higher computational cost and even requires higher execution time similar to [2]–[5] and [7]. Certainly, having limited battery power and computational capability, it is not suitable particularly for the mobile equipment. Besides, after a thorough inspection, we found that the proposed scheme in [9] cannot even resist several attacks, such as replay attacks, forgery attacks, etc. (shown in Section II-B). On the other hand, few more interesting roaming authentication protocols have been proposed [10]–[16]. In particular, the protocols in [10] and [11], which are basically two-party authentication schemes, build upon the elliptic curve discrete logarithm problem. Certainly, these protocols cause the similar computational overhead as in [9]. In addition, according to [12] and [13], the protocol discussed in [11] consists of some security weaknesses as well. In 2012, Mun *et al.* proposed an anonymous authentication scheme [14] for roaming services in GLOMONET. However, Kim and Kwak [15] pointed out that the scheme proposed by Mun *et al.* cannot withstand replay attacks, man-in-the-middle attacks, and insider attacks. Recently, in 2013, Jiang *et al.* have proposed an anonymous-user authentication scheme [16], but Wen *et al.* [17], Gope and Hwang [33], and independently He *et al.* [18] showed that the protocol is vulnerable to several attacks, such as spoofing attacks, replay attacks, etc.

B. Cryptanalysis of the Scheme by Zhou and Xu

Here, we present the several weaknesses of the protocol in [9], which have not been revealed yet, and these are the attacks that certainly cause an insecure mobile communication.

a) Unsuccessful key agreement (Forgery attacks): Assume, in phase II of the scheme by Zhou and Xu, a malicious adversary $\mathcal{A}$, who does not want that the FA and the mobile station (MS) should successfully establish the session key SK between them. In this regard, $\mathcal{A}$ just eavesdrops the communication between the FA and the MS (intercepts m_4) and replaces the nonce n_F generated by FA with n'_F. Unfortunately, the MS does not verify it and, accordingly, cannot comprehend that alternation, which eventually generates a wrong session key $SK' = h(D\|ID_M\|n_M\|n'_F\|ID_F)$, where n_M denotes the nonce generated by the MS, and ID_F signifies the identity of the FA. Therefore, we can argue that the scheme proposed by Zhou and Xu is undoubtedly an unsuccessful key agreement scheme and that also indicates a successful forgery attempt against the user.

b) Vulnerable to replay attacks: The replay attack works if the system cannot check whether the received messages for authentication are fresh or not. The attackers can retransmit the authentication messages that are transmitted during any previous session of communication. Once the system has no ability to deal with the problem, the attackers will obtain the authorization of the system or the user. Unfortunately, the scheme by Zhou and Xu cannot resist replay attacks. In phase II of this scheme, if $m_2 = \{n_M, A, SID, V_1, n_F, ID_F, S_1\}$ is repeatedly sent several times to the system, the HA cannot comprehend that; as a result, it may keep the system busy and eventually degrades the performance of the system.

c) Vulnerable to insider attack: During the execution of the registration phase of the scheme by Zhou and Xu, a user discloses his/her password to the HA; in that case, a privileged insider of the HA can get the information about a registered user's password, which may eventually cause the insider attacks.

In this paper, we present an innovative, lightweight, and efficient mutual authentication and fair key agreement scheme preserving the anonymity for roaming services in GLOMONET. In order to do that, the proposed scheme only employs the hash function and bitwise EXCLUSIVE-OR operation similar to [5]. However, performance analysis shows that our scheme is greatly secure and even more expeditious, as compared to [5] and other state-of-the-art contributions in GLOMONET. Therefore, the remainder of this paper is organized as follows: In Section II, we present our lightweight and efficient mobile communication environment. We analyze the security properties of the proposed scheme in Section III. A relevant discussion based on the performance benchmarking of the proposed scheme is given in Section IV. The formal analysis of the proposed scheme is presented in Section V. Finally, a concluding remark is given in Section VI. The abbreviations and cryptographic functions used in this paper are defined in Table I.

TABLE I
NOTATIONS AND CRYPTOGRAPHIC FUNCTIONS

Symbol	Definition
MS	Mobile Station
FA	Foreign Agent
HA	Home Agent
ID_M	Identity of the mobile user
AID_M	One-time-alias identity of the MS
PID	Pseudo Identity of MS
ID_h	Identity of the HA
ID_f	Identity of the FA
PSW_M	Password of the mobile user
N_m	Random number generated by the MS
N_f	Random number generated by the FA
SK	Session key between FA and MS
K_{uh}	Shared key between MS and HA
K_{em}	Shared emergency key between MS and HA
K_{fh}	Secret Key shared between the FA and HA
Ts_{uh}	Transaction sequence number (maintain both MS and HA)
$h(.)$	One-way hash function
$\oplus$	Exclusive-OR operation
$\|\|$	Concatenation operation

This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

II. PROPOSED SCHEME

Here, we will present our lightweight and efficient user authentication scheme for GLOMONET security. The proposed scheme consists of three phases. In phase I, the HA issues a smart card to a mobile user MS through a secure channel; this phase is called registration phase. The next phase of our proposed scheme (phase II) is the lightweight and secure MAKA phase, where both the MS and the FA can authenticate themselves under the supervision of the HA and, eventually, can establish a session key between them. In phase III, the MS can renew his/her password. Therefore, this phase is denoted as the password renewal phase. Hence, the design goals of our proposed scheme are described as follows:

1) to achieve mutual authentication by preserving the feature of user anonymity;
2) to establish a session key with fairness;
3) privacy against eavesdropper (PAE);
4) to defeat forgery attack and known session key attack along with the forward/backward secrecy support;
5) to achieve perfect forward secrecy (PFS) with the resistance of denial-of-service (DoS) attack;
6) to reduce computation and communication cost.

A. Phase I: Registration Phase

A new mobile user MS submits his/her identity ID_M to a particular HA in a secure manner. After receiving the request from the MS, the HA generates a random number n_h and then computes $K_{uh} = h(ID_M \| n_h) \oplus ID_h$. Subsequently, the HA generates a set of unlinkable pseudo-IDs $PID = \{pid_1, pid_2, \ldots\}$, where for each $pid_j \in PID$, the HA computes $pid_j = h(ID_M \| r_j \| K_{uh})$. Then, the HA also generates a set of emergency keys $K_{\text{em}} = \{k_{\text{em}_1}, k_{\text{em}_2}, \ldots.\}$, i.e., each corresponds to a particular $pid_j \in PID$, where for each $k_{\text{em}_j} \in K_{\text{em}}$, the HA computes $k_{\text{em}_j} = h(ID_M \| pid_j \| r'_j)$. Here, the parameters r_j, r'_j denote the random numbers used for deriving the pseudo-ID pid_j and the corresponding emergency key k_{em_j}, respectively. Hereafter, the HA generates a transaction sequence number Ts_{uh} [19], which is basically a sequence number of 64 bits. This sequence number is computed based on the number of requests (m) handled by the HA, including the present request of the current MS, where, for each request of any subscriber, the system (HA) will increment the value of m by one and then sets $Ts_{uh} = m$ and subsequently sends Ts_{uh} to the subscriber by keeping a copy in its database, in which HA can see the most recent Ts_{uh} for each subscriber. This sequence number can be used to speed up the authentication process, as well as to prevent any replay attempt from any adversary, where by seeing the Ts_{uh} and comparing it with the stored value of its database, the HA can comprehend exactly who the subscriber is, and based on Ts_{uh}, the HA can even decide that whether the user request is valid or not. Precisely, during the execution of the MAKA phase, if the Ts_{uh} provided by the subscriber does not match with the stored value of the HA's database, then the HA will immediately terminate the connection. In that case, the MS will be asked to use his/her one of the unused $pid_j \in PID$ and its corresponding emergency key $k_{\text{em}_j} \in K_{\text{em}}$. Once a pair of pseudo-ID pid_j and the emergency key k_{em_j} is used up from the list of pair of (PID and K_{em}), then the pair of $(pid_j,\ k_{\text{em}_j})$ must be deleted from the list by both the MS and the HA. Now, the HA personalizes a smart card with $\{K_{uh}, (PID, K_{\text{em}}), Ts_{uh} h(.)\}$ and issues it to MS through the secure channel, and then, the HA stores a copy of ID_M, K_{uh}, (PID, K_{em}), and Ts_{uh} in its own database for further communication. After that, the MS chooses a password PSW_M and then computes $K^*_{uh} = K_{uh} \oplus h(ID_M \| PSW_M)$, $PID^* = PID \oplus h(ID_M \| PSW_M), K^*_{\text{em}} = K_{\text{em}} \oplus h(ID_M \| PSW_M)$. Finally, the MS replaces K_{uh} with K^*_{uh}, PID with PID^*, and K_{em} with K^*_{em}; then, the smart card contains $\{K^*_{uh}, (PID^*, K^*_{\text{em}}), Ts_{uh}, h(.)\}$.

B. Phase II: MAKA Phase

When a mobile user MS with a smart card wants to roam over an FA and tries to access services, before providing services, the FA needs to authenticate the MS with the assistance of the HA and establishes a session key SK with the MS. This phase of the proposed scheme consists of the following steps.

Step 1 M_{A_1}—$\{AID_M, N_x, Ts_{uh}(\textit{if require}), ID_h\}$: The MS inserts his/her smart card into the device and submits his/her identity ID_M and password PSW_M. The smart card computes $K_{uh} = K^*_{uh} \oplus h(ID_M \| PSW_M)$. Hereafter, it generates a random number N_m and derives $AID_M = h(ID_M \| K_{uh} \| N_m \| Ts_{uh})$ and $N_x = h(ID_M \| K_{uh}) \oplus N_m$. Finally, the MS forms a request message M_{A_1} and then sends it to the FA, from whom he/she wants to acquire services. Here, Ts_{uh} denotes the most recent transaction sequence number received from the HA. Note that, in case of loss of synchronization, the MS needs to choose one of the unused pair of $(pid^*_j, k^*_{\text{em}_j})$ and then submits his/her identity ID_M and password PSW_M and computes $pid_j = pid^*_j \oplus h(ID_M \| PSW_M)$, $k_{\text{em}_j} = k^*_{\text{em}_j} \oplus h(ID_M \| PSW_M)$ and subsequently assigns the pid_j as AID_M, i.e., $AID_M = pid_j$, and then assigns k_{em_j} as K_{uh}. In that case, the MS need not to send any transaction sequence number Ts_{uh} in M_{A_1}.

Step 2 M_{A_2}—$\{AID_M, N_x, Ts_{uh}, ID_f, V_1, N_y\}$: After receiving the request message from the MS, the FA generates a secret random number N_f and computes $N_y = h(K_{fh}) \oplus N_f, V_1 = h(M_{A_1} \| N_y \| K_{fh} \| N_f)$. Hereafter, it requests the mobile user's HA to verify the legitimacy of the MS. In that case, the FA sends its claimed identity ID_f, and V_1, N_y, in addition to $\{AID_M, N_x, Ts_{uh}\}$ of the MS, to the HA.

Step 3 M_{A_3}—$\{N'_x, N'_y, V_2, V_3, Ts, x(\textit{if req.})\}$: Upon receiving the message from the FA, the HA checks whether the transaction sequence number Ts_{uh} is valid or not. If so, then the HA at first derives $N_m = h(ID_M \| K_{uh}) \oplus N_x$, $N_f = h(K_{fh}) \oplus N_y$ and then verifies V_1, AID_M. If the verification is successful, then the HA computes $N'_x = h(K_{uh} \| ID_M \| Ts_{uh}) \oplus N_f$, $N'_y = h(K_{fh} \| N_f) \oplus N_m$, and $V_2 = h(N'_y \| N_f) \oplus K_{fh}$. Subsequently, the HA checks the latest value of the transaction sequence parameter m and increments it by $m \leftarrow m + 1$ then stores $Ts_{uh_{\text{new}}} = m$ and computes $Ts = h(K_{uh} \| ID_M \|$

$N_m) \oplus Ts_{uh_{\rm new}}$, $V_3 = h(N'_x \| N_m \| Ts) \oplus K_{uh}$. Then, it forms a response message M_{A_3} and sends it to the FA. Finally, the HA computes $K_{uh_{\rm new}} = h(K_{uh} \| ID_M \| Ts_{uh_{\rm new}}), K_{fh_{\rm new}} = h(K_{fh} \| N_f \| ID_f)$ and updates its database with $K_{uh_{\rm new}}$, $K_{fh_{\rm new}}$, and $Ts_{uh_{\rm new}}$. Note that, in case if HA cannot find any Ts_{uh} in M_{A_2}, then the system (HA) will validate the AID_M first, where the system will try to recognize the pid_j in AID_M. If so, then only the system proceeds for any further computation, and at the end, it randomly generates a new shared key, i.e., $K_{uh_{\rm new}}$, and encodes it by using the emergency key $k_{{\rm em}_j}$ (used on that particular transaction) and the real identity of MS ID_M, i.e., $x = K_{uh_{\rm new}} \oplus h(ID_M \| k_{{\rm em}_j})$, and sends x with other response parameters in M_{A_3}. In that case, the response parameter V_3 will be computed in the following way: $V_3 = h(N'_x \| N_m \| Ts \| x) \oplus k_{{\rm em}_j}$. If the system cannot recognize the pid_j in AID_M, then it terminates the connection and requests the MS to try with a valid unused pair of $(pid_j, k_{{\rm em}_j})$.

Step 4 M_{A_4}—$\{N'_x, V_3, Ts, x(\textit{if req.})\}$: Upon receiving M_{A_3}, the FA at first checks whether V_2 is equal to $h(N'_y \| N_f) \oplus K_{fh}$ or not. If the verification is successful, then the FA computes $N_m = h(K_{fh} \| N_f) \oplus N'_y$ and derives the session key and subsequently forwards the other parameters $\{N'_x, V_3, Ts\}$ received from the HA in M_{A_3}, to the MS in M_{A_4}. Otherwise, the system (FA) terminates the connection immediately. Finally, the FA updates K_{fh} with $K_{fh_{\rm new}} = h(K_{fh} \| N_f \| ID_f)$. In case of loss of synchronization between the FA and the HA, which can be comprehended if the response message M_{A_3} has been interrupted, so that the FA cannot receive the message within a specific time period. Then, the FA needs to ask the HA for the new secret shared key, i.e., $K_{fh_{\rm new}}$, which will be securely sent to the FA. Now, after receiving the message M_{A_4} from the FA, the MS at first computes V_3 and verifies whether it is equal to $h(N'_x \| N_m \| Ts) \oplus K_{uh}$ or not. If so, then the smart card computes $N_f = h(K_{uh} \| ID_M \| Ts_{uh}) \oplus N'_x$ and derives the session key $SK = N_m \oplus N_f$. Hereafter, the MS decodes the new transaction number $Ts_{uh_{\rm new}} = h(K_{uh} \| ID_M \| N_m) \oplus Ts$ and computes $K_{uh_{\rm new}} = h(K_{uh} \| ID_M \| Ts_{uh_{\rm new}})$ and subsequently updates the value of K_{uh} with $K_{uh_{\rm new}}$ and Ts_{uh} with $Ts_{uh_{\rm new}}$. Now, if a pair of $(pid_j, k_{{\rm em}_j})$ is sent in M_{A_1}, then the MS will receive a new shared key, i.e., $K_{uh_{\rm new}}$, in the encoded parameter x of M_{A_4}, which will be decoded through his/her identity and the emergency key $k_{{\rm em}_j}$ (used on that particular transaction), and then the MS needs to store that for further communication.

Note that, in our proposed scheme, both the pseudoidentity with emergency key pair and one-time-alias identity with transaction sequence number can resolve the issues such as user anonymity and untraceability. However, since the usage of the (pseudo-ID, emergency key) pair in every transaction may cause excessive storage cost in both the MS and the HA. Therefore, we only use the concept of (pseudo-ID, emergency key) pair for dealing with the DoS attack [20], [21], which may occur because of the loss of synchronization between MS and HA. That can be comprehended if the response message M_{A_4} has been interrupted, so that the MS cannot receive the message within a specific time period. In that case, only a reasonable number of (pseudoidentities, emergency keys) pairs are required to be stored. Although the attackers can continuously interrupt the connections to destroy the unsinkability, it is the tradeoff problem. The system can limit the failure for updating the transaction sequence numbers. In the case when all the pairs have already been used up, then the HA will securely send a new set of pairs to the MS. In addition, it should also be noticed that our regular updating of the shared key K_{uh} and K_{fh}, after completion of each transaction, will resist an adversary from learning any previous session key, even if the secret shared key between the HA and the MS and/or the secret shared key between the HA and the FA is compromised by the adversary. Precisely, if the HA is compromised by the adversary, then he/she can manage $K_{uh_{\rm new}}$, $K_{fh_{\rm new}}$. However, since the hash function is one way, the adversary cannot acquire K_{uh} from $K_{uh_{\rm new}}$ and K_{fh} from the $K_{fh_{\rm new}}$. In this way, the protocol achieves PFS [22], [23] and eventually guarantees the security of any previous session key. However, it should be noted that our key updating approach cannot ensure the security of the future session key. Therefore, once the shared keys K_{uh} and K_{fh} are revealed, then the HA needs to securely send the new shared keys $K_{uh_{\rm new}}$ and $K_{fh_{\rm new}}$ to the MS and the FA, respectively.

On the other hand, apart from the reply attack, the concept of transaction sequence number used in our protocol can also be useful to resolve another imperative issue, where in most of the existing state-of-the-art protocols similar to [1]–[9], the HA needs to do more exercise or needs to have a back-end channel, in order to figure out exactly who the subscriber is, because, for ensuring anonymity, the MS needs to encode his/her original identity and none of the other requested parameters can help the HA to realize the identity of the user. In order to justify our point more clearly, here, we consider an example, in case of the protocol similar to [1], where we see that the mobile user sends a request message $\{n, (x_0)_{E_L}, ID_h, T_M\}$ to the FA, where $n = r \oplus PSW_M, r = h(N \| ID_h) \oplus h(N \| ID_M) \oplus ID_h \oplus ID_M$, x_0 represents the nonce, and T_M denotes the timestamp. Now, the FA forwards these parameters to the HA, in order to verify the user. Here, none of the parameters among $\{n, (x_0)_{E_L}, ID_h, T_M\}$ can straight away tell the HA exactly who the subscriber is. In this regard, the HA needs to put more effort or a back-end communication is required, only to comprehend the user's existence or to get some sense about the user and the service request, where T_M can easily be forged. Unfortunately, the similar problems can also be profound in many existing GLOMONET protocols. In our proposed scheme, the concept of transaction sequence number can easily resolve this problem, where for each communication, the HA always has to provide a new Ts_{uh}, i.e., $Ts_{uh_{\rm new}}$, to the MS, which will be used for communication next time; in other words, in order to help the HA to comprehend exactly who the subscriber is, and to respond quickly, the MS has to provide his/her most recent transaction sequence number $Ts_{uh_{\rm new}}$, which is also stored in the HA's database. However, the downside of this approach is that it causes some searching time and storage cost. Now, if there is any check in the aforementioned steps that is invalid, this phase of the proposed scheme will be aborted. On the other hand, successful completion of this phase indicates that both

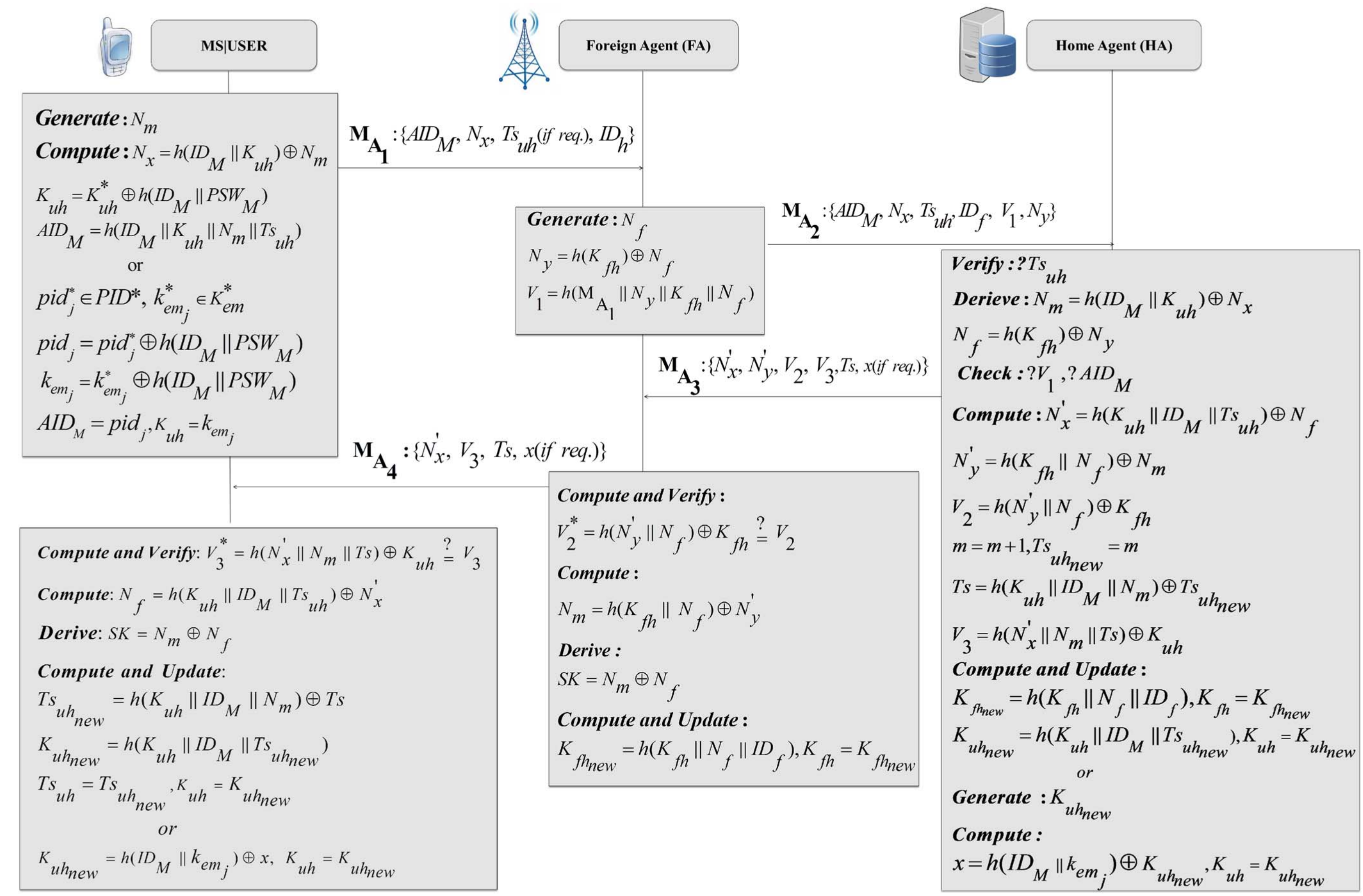

Fig. 1. User-anonymity-based lightweight and secure MAKA protocol.

the MS and the FA mutually authenticate each other, and at the same time, it also denotes the successful establishment of the session key. The details of the MAKA phase are also depicted in Fig. 1.

C. Phase III: Password Renewal Phase

In this scheme, a mobile user can freely change his/her password on the smart card, without any help of the HA. When a mobile user MS wants to renew a password, the MS needs to insert his identity ID_M, old password PSW_M, and the new password PSW_M^* to the smart card. Thereafter, the smart card will retrieve $K_{uh} = K_{uh}^* \oplus h(ID_M \| PSW_M)$, $PID = PID^* \oplus h(ID_M \| PSW_M)$, and $K_{\text{em}} = K_{\text{em}}^* \oplus h(ID_M \| PSW_M)$ and then derive $K_{uh}^{**} = K_{uh} \oplus h(ID_M \| PSW_M^*)$, $PID^{**} = PID^* \oplus h(ID_M \| PSW_M^*)$, and $K_{\text{em}}^{**} = K_{\text{em}} \oplus h(ID_M \| PSW_M^*)$. Finally, the device will replace K_{uh}^* with K_{uh}^{**}, PID^* with PID^{**}, and K_{em}^* with K_{em}^{**} and subsequently stores them for further communication.

III. Security Analysis

Here, we will demonstrate that our proposed scheme holds several imperative security properties, which are indeed essential to offer a secure mobile communication environment.

A. Accomplishment of the Mutual Authentication

In our MAKA phase of the proposed scheme, where the HA authenticates the mobile user MS by verifying the one-time-alias AID_M in the message M_{A_2}, the HA authenticates the FA using the value of the parameter V_1 in the message M_{A_2}. The FA authenticates the HA by using V_2 in the message M_{A_3}, and the MS authenticates the HA and FA by verifying the parameter V_3 in M_{A_4}.

B. Accomplishment of the Fair Key Agreement

A fair key agreement protocol is such a protocol that the agreed key contains some contribution from each participant; hence, nobody has the unfair advantage in controlling the session key. Now, in our proposed scheme, during the establishment of the session key SK, each participant (MS, FA) has contributed equally. Precisely, in our proposed scheme, the session key $SK = N_m \oplus N_f$, where N_m and N_f are the random numbers produced by the MS and FA, respectively, and that clearly denotes the equal contribution of both the MS and the FA.

C. PAE With User Anonymity and Untraceability

An orthogonal security arising as a result of mobility is the confidentiality of the mobile subscriber's identity and movements. For obvious reasons, it is desirable to keep this information secret. In other words, passive eavesdroppers and active intruders should not be able to identify or keep track of the user. In fact, it can be argued that even the visited locations should not be privy to the user's real identity. In case of 3GPP-AKA, the subscriber identity [international mobile subscriber identity (IMSI)] is forced to be directly exposed, as it is sent unencrypted, particularly when synchronization is lost. Therefore, the Universal Mobile Telecommunications System (UMTS) [24], [25] is unable to assure location privacy or user anonymity. In contrast, to ensure good anonymity to the mobile user during his/her migration, the proposed scheme has maintained the one-time-alias feature (using AID_M), where there is no direct relationship between aliases. In addition, here, we also maintain the domain separation that means even when assuming a conspiracy of all the visited domains, the real identity of the user cannot be figured out. Apart from the mobile user himself/herself, only the HA is aware with the mobile user's real identity ID_M. Furthermore, in our proposed scheme, if the same MS requests for service to a particular FA several times, then also it will be very difficult for the foreign domain authority to keep track of the user. Since, almost all of the parameters that the FA receives in M_{A_1} are one time. This approach of the proposed scheme is quite effective for PAE to achieve, along with the features of user anonymity and untraceability.

D. Resistance to Forgery Attack

In our proposed scheme, only the legitimate MS can form a valid AID_M. Because, in order to do that, an adversary must have prior knowledge of the user's real identity ID_M and password PSW_M. After inserting the correct pair of (ID_M, PSW_M) only, a user can compute $K_{uh} = K^*_{uh} \oplus h(ID_M \| PSW_M)$, and subsequently $AID_M = h(ID_M \| K_{uh} \| N_m \| Ts_{uh})$. This seems to be difficult for any attacker to guess this pair. On the other hand, legitimacy of both the systems (HA and FA) can easily be verified through the message M_{A_4}. Besides, if someone tries to alter M_{A_4} in order to cheat against the user, this can easily be detected by checking the parameter V_3. On the other hand, if the attacker tries to modify the M_{A_3}, particularly, the parameters N'_y and V_2 resist the FA to form a valid session key;. However, in that case, the attacker needs to have prior information on the secret key K_{fh} and the nonce N_f, which seems to be difficult for any polynomial time adversary.

E. Security Against Known Session Key Attack

It is clear that known session key attack is a serious threat against any session-key-establishing schemes. A protocol is called secure against known session key attacks if a revealed session key does not influence on the security of other session keys. In other words, if past session keys are compromised, it should not allow an adversary to reveal any future session key or even any other session keys earlier than that one. In this way, a protocol can also compromise its backward and forward secrecy. By backward secrecy, we mean that a compromise of any session key should not compromise any earlier key, whereas forward secrecy implies that a compromise of the current session key should not compromise any future key. Now, in our proposed scheme, if one of the session keys SK_i has been compromised, it never helps to recover any past or future session key (e.g., SK_{i-1} or SK_{i+1}) because there is no significant relationship between any SK_i, SK_{i-1}, SK_{i+1}. Precisely, the session key is generated based on the two random numbers, i.e., $SK = N_m \oplus N_f$, which are expected to be different each time. In addition, since these random numbers must not be transmitted through the encoded manner during authentication, it is indeed a difficult task to figure out or guess these random numbers, which is only possible if the adversary has some prior knowledge of the secret keys K_{uh} and K_{fh}. However, it seems to be hard, as none of the participants of our proposed scheme is allowed to share the long-term secrets. In this way, our proposed scheme can resist any known session key attack and can even assure the backward/forward secrecy.

F. Resistance to Insider Attack

In the real environment, it is very common that many users use the same password to access servers or applications for convenience. Now, if a privileged insider of the HA has learned the MS's password, he may try to impersonate the MS to access other servers where MS could be a registered user. In the registration phase of our proposed scheme, users need not to submit their passwords to the HA; thus, a privileged insider of the HA could not get any information about a registered user's password. Hence, insider attack is prevented.

G. Security Assurance in Case of Lost Smart Card

Usually, if the user's smart card is lost or an attacker steals the MS's smart card, then the attacker can easily get all the secret parameters stored [26] in it and, thereafter, can use it for illegal purposes. However, in our proposed scheme, if the smart card is lost or stolen, the attacker cannot obtain the MS's identity ID_M and password PSW_M. Besides, without knowing these parameters, the attackers cannot compute $K_{uh} = K^*_{uh} \oplus h(ID_M \| PSW_M), AID_M = h(ID_M \| K_{uh} \| N_m \| Ts_{uh})$ or $pid_j = pid^*_j \oplus h(ID_M \| PSW_M), k_{\mathrm{em}_j} = k^*_{\mathrm{em}_j} \oplus h(ID_M \| PSW_M)$, which are essential to convince the HA.

IV. Performance Analysis and Comparisons

The purpose of the proposed scheme is to resolve several security issues existing in the GLOMONET, and at the same time, it should also maintain the reasonable computational and communication overhead. Here, we compare our scheme with recently proposed schemes with user anonymity [3], [5], [9], [14], [16] to manifest the advantages of our scheme. We also demonstrate that our scheme is well suitable for low- power mobile devices. In order to analyze the performance of the proposed scheme, particularly on the security front, our scheme has been compared with the four state-of-the-art protocols [3], [5], [9], [14], [16] (shown in Table II). In Table II, it is clear that

This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

TABLE II
PERFORMANCE BENCHMARKING BASED ON SECURITY PROPERTIES

Scheme	SP1	SP2	SP3	SP4	SP5	SP6	SP7	SP8
Lee et al. [3]	No	Yes	No	No	No	No	No	No
Chang et al. [5]	No	No	No	No	No	No	No	No
Zhou et al. [9]	Yes	No	Yes	No	Yes	No	No	No
Mun et al.[14]	No	No	No	No	No	No	No	No
Jiang et al. [16]	Yes	No	Yes	No	No	No	No	No
Ours	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SP: Security Property; **SP1:** User Anonymity; **SP2:** Robustness Against Replay Attack; **SP3:** Privacy Against Eavesdroppers (PAE); **SP4:** Robustness Against Forgery Attacks ; **SP5:** Robustness Against Known Session Key Attack; **SP6:** Robustness Against Insider Attack; **SP7:** Robustness Against Lost Smart Card Problem; **SP8:** Perfect Forward Secrecy;								

TABLE III
PERFORMANCE BENCHMARKING BASED ON COMPUTATIONAL COST

Scheme	Mobile	Foreign Agent	Home Agent
Lee et al. [3]	$2t_{Sym} + 4t_{Hash}$	$t_{Sym} + 2t_{ASym} + 3t_{Hash}$	$t_{Sym} + 2t_{ASym} + 5t_{Hash}$
Chang et al. [5]	$7t_{Hash}$	$5t_{Hash}$	$8t_{Hash}$
Zhou et al. [9]	$2t_{Exp1} + 4t_{Hash}$	$3t_{Hash}$	$t_{Exp1} + 7t_{Hash}$
Mun et al.[14]	$t_{ASym} + 5t_{Hash}$	$t_{ASym} + 4t_{Hash}$	$5t_{Hash}$
Jiang et al. [16]	$t_{Exp2} + 3t_{Hash}$	$4t_{Hash}$	$t_{Exp2} + 5t_{Hash}$
Ours	$6t_{Hash}$	$5t_{Hash}$	$10t_{Hash}$
t_{Sym} **:** Execution time of a symmetric key operation; t_{ASym} **:** Execution time of a asymmetric key operation; t_{Hash} **:** Execution time of a one-way hash function; t_{Exp1} **:** Execution time of a modular exponential operation Using Using Diffie-Hellman; t_{Exp2} **:** Execution time of a modular exponential operation Using Chinese Remainder Theorem;			

the proposed scheme can resist several security threats existing in the GLOMONET environment. In contrast, the protocols presented in [3], [5], [9], [14], and [16] are vulnerable to various security attacks. In addition, the protocols presented in [3], [5], and [14] even cannot assure user anonymity as well. In the protocol in [9], once the HA is compromised, then the adversary can get the secret key K_{fh}, and by using that, he/she can accomplish all the previous session keys. Hence, although the protocol by Zhou and Xu is based on DDH, it cannot ensure PFS. Now, as far as the computational overhead is concerned, the performances of the scheme in [5] and the proposed scheme are significantly better than [3], [9], [14], and [16], precisely because there is no symmetric/asymmetric cryptosystem, or any exponential operation, that has been introduced in the proposed scheme, which certainly demands higher computational overhead. Instead, both the proposed scheme and the scheme by Chang *et al.* are based on the one-way noncollusion hash function, which causes reasonable computational overhead as compared to any encryption/decryption or any exponential operation. However, the performance of the proposed scheme is even better than the scheme by Chang *et al.* since our proposed scheme causes even less communication overhead during authentication, as compared with the scheme by Chang *et al.* (shown in Table III).

Now, in order to analyze the performance of the proposed scheme more comprehensively, here, we simulate several cryptographic operations used in the proposed scheme and the schemes presented in [3], [5], [9], [14], and [16], using a CryptoPP cryptographic library [25] on an Arm Cortex-A8 machine with the frequency of 0.72 GHz. In addition, we assume that the symmetric and asymmetric encryptions are implemented by the Advance Encryption Standard with Cipher Block Chaining (AES-CBC) [28]–[30] mode and the Elliptic Curve Integrated Encryption Scheme (ECIES), respectively,

TABLE IV
COMPUTATIONAL OVERHEAD OF THE VARIOUS CRYPTOGRAPHIC OPERATIONS

Cryptographic Operation	CPU Cycles	Execution Time
Hash operation (SHA-256)	5.63×10^{2} cpo	7.81×10^{-4} msec
Symmetric key encryption/decryption (AES-CBC)	7.56×10^{2} cpo	10.5×10^{-4} msec
Asymmetric encryption/decryption (ECIES)	12.42×10^{6} cpo	17.25 msec
Modular exponential operation (Diffie-Hellman)	9.52×10^{6} cpo	13.22 msec
Modular exponential operation (Chinese remainder theorem)	8.69×10^{6} cpo	12.06 msec
$t_{Hash} \approx 5.63\times10^{2}$ (Cycle per operation); $t_{Sym} \approx 7.56\times10^{2}$ (Cycle per operation); $t_{Exp1} \approx 9.52\times10^{6}$ (Cycle per operation); $t_{Exp2} \approx 8.69\times10^{6}$ (Cycle per operation); $t_{ASym} \approx 12.42\times10^{6}$ (Cycle per operation);		

since the protocol in [3] has used both the symmetric and asymmetric cryptosystem and the protocol presented in [14] is based on the asymmetric cryptosystem. On the other hand, since the protocols presented in [9] and [16] have used the modular exponential operations Diffie–Hellman and Chinese remainder theorem, respectively, we analyze the computational cost of the Diffie–Hellman public key solution and the Chinese remainder theorem, in terms of the CPU cycles and execution time. Now, to implement our proposed scheme and the scheme in [5], we adopt SHA-256 [31]. Therefore, the execution time and the related operations of the proposed scheme are summarized, as in Table IV. Now, based on Table IV, the proposed scheme takes 118.23×10^2 CPU cycles, in order to perform $21 * t_{\text{Hash}}$ operations in 0.016 ms, where a hash operation needs 5.63×10^2 CPU cycles, whereas the scheme by Chang *et al.* needs 112.6×10^2 CPU cycles, in order to perform $20 * t_{\text{Hash}}$ operations in 0.015 ms. It clearly denotes that the proposed scheme causes slightly more computational overhead and execution time, as compared with the scheme by Chang *et al.*. However, it should be noted that, during the authentication process, the proposed scheme causes only $17 * t_{\text{Hash}}$ operations, whereas in order to achieve PFS, all the participants need to update their secret keys, which eventually causes additional $4 * t_{\text{Hash}}$ operations. Moreover, the scheme by Chang *et al.* needs eight messages to exchange during the execution of the protocol; in addition, the scheme is highly insecure as well. In contrast, our proposed scheme requires only four messages to exchange between the participants (MS, FA, and HA) during authentication. Accordingly, the communication overhead of the scheme by Chang *et al.* is much higher than that of our proposed scheme and even higher than those in [3], [9], [14], and [16]. Now, the execution of the protocol in [16] causes 17.39×10^6 CPU cycles, with 24.15 ms of execution time, which shows that it causes less computational overhead as compared with [3], [9], and [14]. However, the computational overhead of the protocol by Jiang *et al.* is significantly higher, as compared with that of the proposed scheme and of the scheme in [5], where the Chinese remainder theorem used in [16] requires 8.69×10^6 CPU cycles to perform the exponential operation. The detailed analyses are shown in Figs. 2 and 3. Furthermore, in order

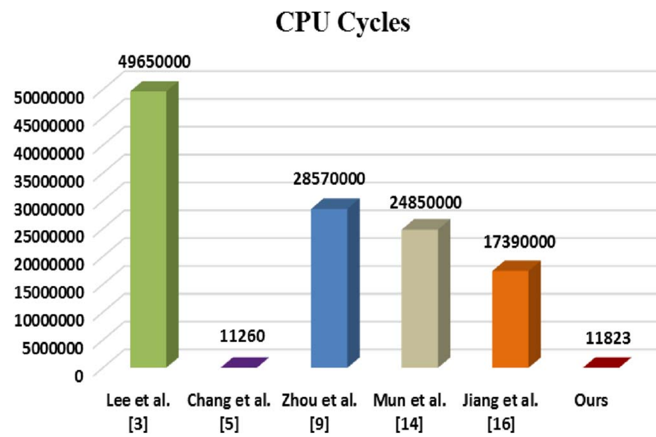

Fig. 2. Performance comparison based on the CPU cycles.

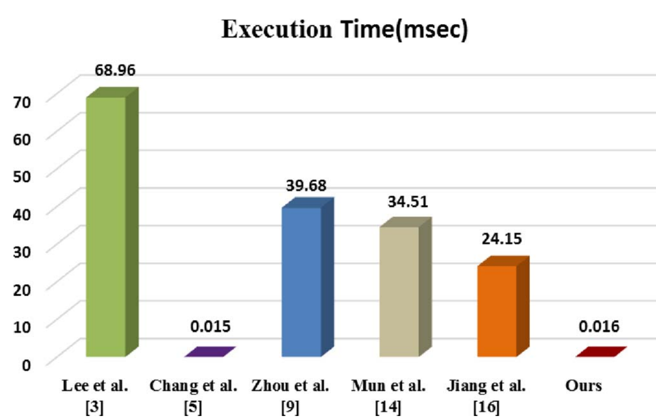

Fig. 3. Performance comparison based on the execution time.

to distinguish the computational performance of the proposed scheme and the protocol in [5] more precisely, here, we also simulate SHA-256 on the MSP430 family with a frequency of 8 MHz, where the execution time of a hash function is 0.065 ms. Based on that, the proposed scheme requires 13.65 ms to perform $21 * t_{\text{Hash}}$ operations, and the scheme by Chang *et al.* needs 13 ms to perform $20 * t_{\text{Hash}}$ operations.

This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

V. Protocol Analysis

In order to find out flaws in the proposed scheme, here, we introduce a formal analysis using the Burrows–Abadi–Needham (BAN) logic, which is basically a model logic with primitives that describe the belief of the principle involved in a cryptosystem. Using the inference rules of the BAN logic, authentication issues between the principles can be dealt with.

A. BAN Logic and Its Improvement

Three sorts of objects are included in BAN logic as follows [32]: principle, encryption keys, and logical formulas. The main construction of BAN logic is described as follows: $P| \equiv X$ denotes that P believes X; $P\Delta X$ denotes that P sees X; $P| \sim X$ denotes that P said X; $P| \Rightarrow X$ denotes that P has jurisdiction over X; # (X) denotes that the formula X is fresh, i.e., X has not been sent in a message at any time before the current execution of the protocol. $P \overset{K}{\longleftrightarrow} Q$ denotes that P and Q may use the shared K to communicate; $P \ni X$ denotes that P processes or is capable of processing formula X; $\{X\}_K$ denotes that the formula X is encrypted under the key K. The inference rules of BAN logic that are required in the analysis are described as follows:

1. Message-meaning rules R1: $((P| \equiv P \leftrightarrow Q, P\Delta\{X\}_K)(/P| \equiv Q| \sim X))$;
2. Nonce-verification rules R2: $((P| \equiv \#(X), P| \equiv Q| \sim X)/(P| \equiv Q| \equiv X))$;
3. Jurisdiction rules R3: $((P| \equiv Q| \Rightarrow X, P| \equiv Q| \equiv X)/(P| \equiv X))$;
4. Seeing rules R4: $((P\Delta(X,Y)/P\Delta X)$; $\mathrm{R5}: (P| \equiv P \overset{K}{\longleftrightarrow} Q, P\Delta\{X\}_K)/P\Delta X)$;
5. Fresh rules R6: $((P| \equiv \#(X))/(P| \equiv \#(X,Y)))$;
6. Belief rules R7: $((P| \equiv (X,Y))/(P| \equiv X))$.

Now, in order to analyze the properties of our proposed scheme, here, we need to extend the BAN logic with the following: ER1: $((P| \equiv Q \overset{K}{\longleftrightarrow} P, P\Delta f(X,Y))/(P| \equiv Q| \sim X))$, where the extension rule ER1 denotes that the key K is shared among P and Q; function f is used to verify the originality of the principles.

B. Formal Analysis of the Proposed Scheme

The initial security assumptions about the MS, FA, and HA are as follows:

$$1.\ \mathrm{MS}| \equiv \mathrm{MS} \overset{K_{uh}}{\longleftrightarrow} \mathrm{HA};\ 2.\ \mathrm{HA}| \equiv \mathrm{MS} \overset{K_{uh}}{\longleftrightarrow} \mathrm{HA};$$

$$3.\ \mathrm{FA}| \equiv \mathrm{FA} \overset{K_{fh}}{\longleftrightarrow} \mathrm{HA};\ 4.\ \mathrm{HA}| \equiv \mathrm{FA} \overset{K_{fh}}{\longleftrightarrow} \mathrm{HA}.$$

Now, applying R1–R7 with ER1 on our proposed scheme, we can write the following statements: $\mathrm{HA}| \equiv \mathrm{MS}| \sim \{AID_M\}$; more accurately, by using ER1, we can write

$$\frac{\mathrm{HA}| \equiv \mathrm{MS} \overset{K_{uh}}{\longleftrightarrow} \mathrm{HA}, \mathrm{HA}\Delta f(h(ID_M\|K_{uh}\|N_m\|Ts_{uh}), AID_M)}{\mathrm{HA}| \equiv \mathrm{MS}| \sim AID_M}$$

Hereafter, using R7 and R6, we can write the following statements: $((\mathrm{HA}| \equiv (N_m, AID_M))/(\mathrm{HA}| \equiv N_m))$; $((\mathrm{HA}| \equiv \#(Ts_{uh}))/(\mathrm{HA} \equiv \#(Ts_{uh}, AID_M)))$; and $((\mathrm{HA}| \equiv \#(Ts_{uh}))/(\mathrm{HA}| \equiv \#(Ts_{uh}, N_m)))$.

Similarly, $\mathrm{HA}| \equiv \mathrm{FA}| \sim \{V_1\}$; more accurately, by using ER1, we can write the following statement:

$$\frac{\mathrm{HA}| \equiv \mathrm{FA} \overset{K_{fh}}{\longleftrightarrow} \mathrm{HA}, \mathrm{HA}\Delta f(h(M_{A_1}\|N_y\|K_{fh}\|N_f), V_1)}{\mathrm{HA}| \equiv \mathrm{FA}| \sim V_1}$$

and based on that, we can write $((\mathrm{HA}| \equiv (M_{A_2}, V_1))/(\mathrm{HA}| \equiv M_{A_2}))$.

Now, $\mathrm{FA}| \equiv \mathrm{HA}| \sim M_{A_3}, \exists \mathrm{FA}| \equiv \#(V_2)$, and $((\mathrm{FA}| \equiv (M_{A_3}, V_2))/(\mathrm{FA}| \equiv M_{A_3}))$; more accurately, by using ER1, we can write $((\mathrm{FA}| \equiv \mathrm{HA} \overset{K_{fh}}{\longleftrightarrow} \mathrm{FA}, \mathrm{FA}\Delta f(h(N'_y\|N_f) \oplus K_{fh}), V_2))/(\mathrm{FA}| \equiv \mathrm{HA}| \sim V_2))$, and using R6 and R3, we have $((\mathrm{FA}| \equiv \#(N_f))/(\mathrm{FA}| \equiv \#(N_f, V_2)))$; $((\mathrm{FA}| \equiv \#(V_2))/(\mathrm{FA}| \equiv \#(V_2, M_{A_3})))$; $((\mathrm{FA}| \equiv \mathrm{HA}| \Rightarrow V_2, \mathrm{FA}| \equiv \mathrm{HA}| \equiv V_2)/(\mathrm{FA}| \equiv V_2))$.

Now, for MS, we can write $\mathrm{MS}| \equiv \mathrm{HA}| \sim M_{A_4}, \exists \mathrm{MS}| \equiv \#(V_3)$, and $((\mathrm{MS}| \equiv (M_{A_4}, V_3))/(\mathrm{MS}| \equiv M_{A_4}))$; precisely, using ER1, we can write

$$\frac{\mathrm{MS}| \equiv \mathrm{HA} \overset{K_{uh}}{\longleftrightarrow} \mathrm{MS}, \mathrm{MS}\Delta f(h(N'_x\|N_m\|Ts) \oplus K_{uh}), V_3)}{\mathrm{FA}| \equiv \mathrm{HA}| \sim V_3}.$$

Now, the MS can verify the nonce N_f, which is imperative for session key generation, since, in the case of wrong N_f, the MS will form the wrong session key. In this case, we can write the following statements: $((\mathrm{MS}| \equiv (N'_x, V_3))/(\mathrm{MS}| \equiv N'_x))$; $((\mathrm{MS}| \equiv (N_f, N'_x))/(\mathrm{MS}| \equiv N_f))$; and $((\mathrm{MS}| \equiv (SK, N_f))/(\mathrm{MS}| \equiv SK))$, where $SK = N_m \oplus N_f$. In this way, the MS, FA, and HA can authenticate themselves through the legitimate security capabilities. Now, from the aforementioned analysis using the BAN logic, we have proved that the protocol used in the proposed scheme is correct, where the legitimate participants (MS, FA, and HA) can authenticate each other by using the several security capabilities, if the executions of the protocols are successful.

VI. Conclusion

In this paper, at first, we have discussed several security weaknesses in the proposed scheme by Zhou and Xu. Subsequently, we have proposed a lightweight and secure MAKA scheme, which is based on the low-cost cryptographic primitives, such as one-way hash functions and EXCLUSIVE-OR operations. Our proposed scheme can resolve several security issues existing in the GLOMONET environment. In addition, based on the aforementioned analyses, we can clearly argue that the proposed scheme is more efficient, as compared with other recently proposed schemes in GLOMONET, and even much suitable for low-power mobile devices with roaming services of GLOMONET.

ACKNOWLEDGMENT

The authors would like to thank the Ministry of Science and Technology (MOST), Taiwan for their support and the editor and all the anonymous referees for their valuable comments and suggestions.

REFERENCES

[1] A. Herzberg, H. Krawczyk, and G. Tsudik, "On travelling incognito," in *Proc. IEEE Workshop Mobile Syst. Appl.*, 1994, pp. 205–211.

[2] J. Zhu and J. Ma, "A new authentication scheme with anonymity for wireless environments," *IEEE Trans. Consum. Electron.*, vol. 50, no. 1, pp. 231–235, Feb. 2004.

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

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

[5] C. C. Chang, C. Y. Lee, and Y. C. Chiu, "Enhance authentication scheme with anonymity for roaming service in global mobility networks," *Comput. Commun.*, vol. 32, no. 4, pp. 611–618, Mar. 2009.

[6] T. Y. Youn, T. H. Park, and Lim, "Weaknesses in an anonymous authentication scheme for roaming service in global mobile networks," *IEEE Commun. Lett.*, vol. 13, no. 7, pp. 471–473, Jul. 2009.

[7] C. Tang and D. O. Wu, "Mobile privacy in wireless networks revisited," *IEEE Trans. Wireless Commun.*, vol. 7, no. 3, pp. 1035–1042, Mar. 2008.

[8] J. Lu and J. Zhou, "On the security of an efficient mobile authentication scheme for wireless networks," in *Proc. 6th Int. Conf. WICOM*, Sep. 2010, pp. 23–25.

[9] T. Zhou and J. Xu, "Provable secure authentication protocol with anonymity for roaming service in global mobility networks," *Comput. Netw.*, vol. 55, no. 1, pp. 205–213, Jan. 2011.

[10] G. Yang, Q. Huang, W. S. Duncan, and X. Deng, "Universal authentication protocols for anonymous wireless communications," *IEEE Trans. Wireless Commun.*, vol. 9, no. 1, pp. 168–174, Jan. 2010.

[11] D. He, C. Chen, S. Chan, and J. Bu, "Secure and efficient handover authentication based on bilinear pairing functions," *IEEE Trans. Wireless Commun.*, vol. 11, no. 1, pp. 48–53, Jan. 2012.

[12] D. He, C. Chen, S. Chan, and J. Bu, "Analysis and improvement of a secure and efficient handover authentication for wireless networks," *IEEE Commun. Lett.*, vol. 16, no. 8, pp. 1270–1273, Aug. 2012.

[13] J. L. Tsai, N. W. Lo, and T. C. Wu, "Secure handover authentication protocol based on bilinear pairings," *Wireless Pers. Commun.*, vol. 73, no. 3, pp 1037–1047, Dec. 2013.

[14] H. Mun, K. Han, Y. Lee, C. Yeun, and H. Choi, "Enhanced secure anonymous authentication scheme for roaming service in global mobile network," *Math. Comput. Model.*, vol. 55, pp. 214–222, 2012.

[15] J. Kim and J. Kwak, "Improved secure anonymous authentication scheme for roaming service in global mobile network," *Int. J. Security Appl.*, vol. 6, no. 3, pp. 45–54, 2012.

[16] Q. Jiang, J. Ma, G. Li, and L. Yang, "An enhanced authentication scheme with privacy preservation for roaming services in global mobility networks," *Wireless Pers. Commun.*, vol. 68, no. 4, pp. 1477–1491, Feb. 2013.

[17] F. Wen, W. Susilo, and G. Yang, "A secure and effective user authentication scheme for roaming service in global mobility networks," *Wireless Pers. Commun.*, vol. 73, no. 3, pp. 993–1004, Dec. 2013.

[18] D. He, Y. Zhang, and J. Chen, "Cryptanalysis and improvement of an anonymous authentication protocol for wireless access networks," *Wireless Pers. Commun.*, vol. 74, no. 2, pp. 229–243, Jan. 2014.

[19] T. Hwang and P. Gope, "Provably secure mutual authentication and key exchange scheme for expeditious mobile communication through synchronously one-time secrets," *Wireless Pers. Commun.*, vol. 77, no. 1, pp. 197–224, Jul. 2014.

[20] C. H. Wang and C. Y. Lin, "An efficient delegation-based roaming payment, protocol against denial of service attacks," in *Proc. Int. Conf. Electron., Commun. Control*, pp. 4136–4140, Sep. 2011.

[21] J. L. Tsai, N. W. Lo, and T. C. Wu, "Secure delegation-based authentication protocol for wireless roaming service," *IEEE Commun. Lett.*, vol. 16, no. 7, Jul. 2012.

[22] W. Diffie, P. C. van Oorshot, and M. J. Wiener, "Authentication and Authenticated Key Exchanges," *Designs, Codes Cryptogr.*, vol. 2, no. 2, pp. 107–125, Jun. 1992.

[23] H. Krawczyk, "SKEME: A versatile secure key exchange mechanism for Internet," in *Proc. Symp. Netw. Distrib. Syst. Security*, Feb. 22–23, 1996, pp. 114–127.

[24] *Security Architecture, Version 4.2.0, Released 4*, 3GPP TS 33.102, 2001.

[25] *Formal Analysis of the 3G Authentication Protocol*, 3GPP-Authentication and Key Agreement (AKA) TR 33.902, 2000.

[26] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. CRYPTO*, 1999, vol. 1666 LNCS, pp. 388–397, Springer-Verlag.

[27] Crypto++ Library. [Online] Available: http://www.cryptopp.com

[28] National Bureau of Standards, "*NBS FIPS PUB 81: DES Modes of Operation*," U.S. Dept. of Commerce, 1980.

[29] C. H. Meyer and S. M. Matyas, *Cryptography. A New Dimension in Computer Data Security*. New York, NY, USA: Wiley, 1982.

[30] B. Schneier, *Applied Cryptography*. New York, NY, USA: Wiley, 1996.

[31] D. R. Stinson, "Universal hashing and authentication codes," *Des. Codes Cryptogr.*, vol. 4, no. 4, pp. 369–380, 1994.

[32] M. Burrows, M. Abadi, and R. Needham. "A logic of authentication," *ACM Trans. Comput. Syst. (TOCS)*, vol. 8, no. 1, pp. 18–36, 1990.

[33] P. Gope and T. Hwang, "Enhanced secure mutual authentication, and key agreement scheme preserving user anonymity in global mobile networks," *Wireless Pers. Commun.*, to be published. [Online]. Available: http://link.springer.com/article/10.1007%2Fs11277-015-2344-z

Prosanta Gope received the M.Tech degree in computer science and engineering from the National Institute of Technology, Durgapur, India, in 2009. He is currently working toward the Ph.D. degree in computer science and information engineering with the National Cheng Kung University, Tainan, Taiwan.

His research interests include authentication, authenticated encryption, access control systems, security in mobile communication, and cloud computing.

Tzonelih Hwang received the M.S. and Ph.D. degrees in computer science from the University of Southwestern Louisiana, Lafayette, LA, USA, in 1988.

He is currently a Distinguished Professor with the Department of Computer Science and Information Engineering, National Cheng Kung University, Tainan, Taiwan. He has published more than 250 technical papers and holds five patents. His research interests include network and information security, access control systems, error control codes, security in mobile communication, and quantum cryptography.

Dr. Hwang has actively participated in several research activities, including as a research scientist at the Center for Advanced Computer Studies, University of Southwestern Louisiana. He is also associated as a vigorous member of the editorial board of some reputable international journals.