International Journal of Innovative Computing, Information and Control
Volume **9**, Number **8**, August **2013**

ICIC International ©2013 ISSN 1349-4198
pp. 3319–3339

IMPROVED EFFICIENT AUTHENTICATION SCHEME WITH ANONYMITY IN GLOBAL MOBILITY NETWORKS

Chi-Tung Chen

Department of Distribution Management
National Chin-Yi University of Technology
57, Sec. 2, Zhongshan Rd., Taiping Dist., Taichung 41170, Taiwan
chi9695@ncut.edu.tw

Received June 2012; revised November 2012

Abstract. *A number of user authentication schemes have been proposed to provide roaming services in the global mobility network (GLOMONET). However, most of these schemes are based on an asymmetric cryptosystem, which has a higher computational cost. To achieve computational efficiency, Chang et al. proposed an authentication scheme using simple hash functions for mobile devices in the GLOMONET. However, this study shows that the scheme by Chang et al. does not provide user anonymity and cannot counteract insider attacks, in addition to being vulnerable to the disclosure of session keys and foreign agent spoofing. Therefore, this study proposes a more secure and efficient authentication scheme and uses the Burrows-Abadi-Needham (BAN) logic method to verify the scheme. The proposed scheme can overcome the main disadvantages of the Chang et al. scheme and satisfy the crucial design criteria for a secure remote user authentication scheme. The proposed scheme can provide a more secure functionality and has superior performance, such as a lower computational cost, less time complexity, fewer communication rounds, fewer transmitted messages, and less energy consumption. For practical purposes, this study demonstrates that the proposed scheme can be used to enhance the effectiveness and efficiency of the authentication scheme in the GLOMONET.*

Keywords: Authentication, Anonymity, Global mobility networks, Efficiency, BAN logic

1. Introduction.

With the advancement in commercial development of cellular systems and the rapid globalization of communication, offering effective global roaming services to legitimate users has become necessary. The global mobility network (GLOMONET) [7] is a network environment that provides mobile users with a global roaming service. The GLOMONET permits mobile users to access services provided by a home agent (HA) in a foreign network. A foreign network differs from the home network of a user and is managed by a foreign agent (FA). However, it can increase the possibility of illegal access from malicious intruders. Therefore, a strong authentication scheme for the GLOMONET is required to provide wireless access and roaming services in foreign networks.

Previous studies have presented a number of user authentication schemes for global roaming services [1-7]. Zhu and Ma (2004) proposed a new authentication scheme for wireless environments [4]. The scheme was based on smart cards and public key cryptosystems. Lee et al. [5] indicated that the Zhu and Ma scheme had several security weaknesses. To enhance the security, they proposed a slight modification of this scheme by using public key cryptosystems. Wu et al. [6] demonstrated that the schemes by Lee et al. and Zhu-Ma failed to provide anonymity, and subsequently exposed the identities of mobile users. Subsequently, after verifying that the Wu et al. scheme is vulnerable to certain weaknesses, He et al. [1] and Mun et al. [2] proposed a strong user authentication scheme using the elliptic curve cryptosystem (ECC) and the elliptic curve Diffie-Hellman (ECDH), respectively. However, these schemes were based on an asymmetric encryption algorithm. The asymmetric cryptosystem has a higher computational cost and energy consumption [3,9,16-19].

A number of studies [3,9,16-19] showed that a one-way hash function is efficient in computation, and its computational cost and energy consumption are less than those of asymmetric cryptosystems. To achieve computational efficiency and low energy consumption, Chang et al. [3] proposed an authentication scheme using simple hash functions for battery-powered mobile devices in the GLOMONET. However, this scheme has a number of security disadvantages. This study shows that the Chang et al. scheme does not provide user anonymity and cannot counteract insider attacks [11,12]. In addition, their scheme is vulnerable to the disclosure of session keys (*SK*s) and foreign agent spoofing (base station spoofing) [13-15]. Therefore, we propose a more secure and efficient authentication scheme with simple hash functions to overcome the main disadvantages of the Chang et al. scheme for the GLOMONET. This paper shows that the proposed scheme is superior in performance for completing the authentication process, such as demonstrating less computational cost, less time complexity, fewer communication rounds, fewer transmitted messages, and lower energy consumption. The proposed scheme is efficient and suitable for the GLOMONET and other mobile communications. We also show that the proposed scheme is capable not only of overcoming the main disadvantages of the Chang et al. scheme, but also of satisfying the six crucial design criteria for a secure remote user authentication scheme [9,22]. The six crucial design criteria include single registration, a freely chosen password, no verification table, mutual authentication, a session key agreement, and low computation and communication costs [9,22]. The proposed scheme also provides other principal secure functionalities, such as forgery attack resistance and no time-synchronization problem. Therefore, the scheme offers more secure functionality and is effective in protecting the GLOMONET. For practicality in using our results, we provide practical examples and introduce a real-case scenario to show that the proposed scheme can be used to enhance the effectiveness and efficiency of the authentication scheme in using the GLOMONET.

The remainder of this paper is organized as follows: Section 2 provides a brief review of the Chang et al. scheme; Section 3 details the weaknesses of the Chang et al. scheme; Section 4 introduces the proposed authentication scheme with anonymity, which is more secure and efficient; Section 5 presents a security analysis of the proposed scheme and the use of the Burrows-Abadi-Needham (BAN) logic [8,10] method to verify the scheme; Section 6 demonstrates the practical application of our results and provides comparisons between the performance and functionality of the proposed scheme and those of the previous related schemes; and lastly, Section 7 offers a conclusion.

2. Review of the Chang et al. Scheme.

This section presents a brief review of the scheme by Chang et al. [3]. The notations used in their scheme are shown in Table 1. The GLOMONET contains three entities: the mobile user (*MN*), the *HA*, and the *FA*. The Chang et al. scheme assumes that each *FA* and *HA* share a long-term common secret key K_{FH}. The *HA* has a secret private key, x. The Chang et al. scheme comprises three phases: registration, authentication, and session key establishment. They are described in the next two subsections.

2.1. Registration phase.

When a mobile user, *MN*, wants to perform the registration, *MN* must select the identification ID_{MN} and password PW_{MN}. Figure 1 shows the registration phase of the Chang et al. scheme. The *MN* and *HA* perform the following

Table 1. Definition of notations

Notation	Definition
MN	A mobile user
HA	The home agent of a mobile user
FA	The foreign agent of a foreign network
ID_x	The identification of an entity x
PW_{MN}	The password of MN
SID	The shadow identification of MN
$\|\|$	String concatenation operation
$\oplus$	Exclusive-OR operation
$h(\cdot)$	A secure one-way hash function
$\rightarrow$	A common channel
$\Rightarrow$	A secure channel

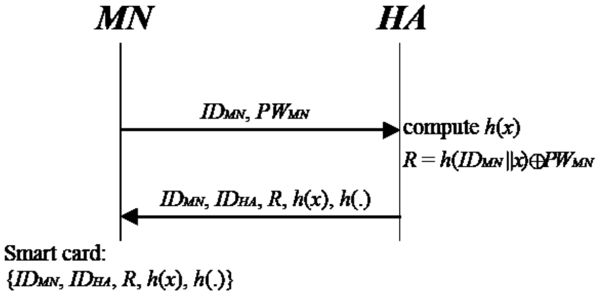

Figure 1. Registration phase of the Chang et al. scheme

steps:
Step R1. $MN \Rightarrow HA$:$\{ID_{MN}, PW_{MN}\}$. The *MN* sends ID_{MN} and PW_{MN} to the *HA* to register through a secure channel.
Step R2. The *HA* calculates the hash value, $h(x)$, and computes $R = h(ID_{MN} \parallel x) \oplus PW_{MN}$.
Step R3. $HA \Rightarrow MN$:$\{ID_{MN}, ID_{HA}, R, h(x), h(.)\}$. The *HA* issues a smart card with the secret parameters $\{ID_{MN}, ID_{HA}, R, h(x), h(.)\}$ to the *MN* through a secure channel.

2.2. **Authentication and session key establishment.** When an *MN* roams into a foreign network managed by an *FA*, the *FA* must authenticate the *MN* through the *HA* of the *MN*. The authentication and session key establishment of the Chang et al. scheme are shown in Figure 2. For authentication, the *MN* first keys in the PW_{MN}, before performing the following steps:
Step A1. The *MN* generates a nonce n_{MN} randomly and computes $C = (R \oplus PW_{MN}) \oplus n_{MN}$.
Step A2. $MN \rightarrow FA$:$\{$*login request*$, n_{MN}, ID_{HA}\}$. The *MN* sends the login request message $m_1 = \{$*login request*, n_{MN}, $ID_{HA}\}$ to the *FA*. The "*login request*" is the header of the message.

After receiving the login request message, m_1, the *FA* obtains the information of the *HA* by recognizing the ID_{HA}.
Step A3. The *FA* generates a nonce, n_{FA}.
Step A4. $FA \rightarrow HA$:$\{$*authentication request*, n_{FA}, $ID_{FA}\}$. The *FA* sends the authentication request message $m_2 = \{$*authentication request*, n_{FA}, $ID_{FA}\}$ to the *HA*. The "*authentication request* " is the header of the message.

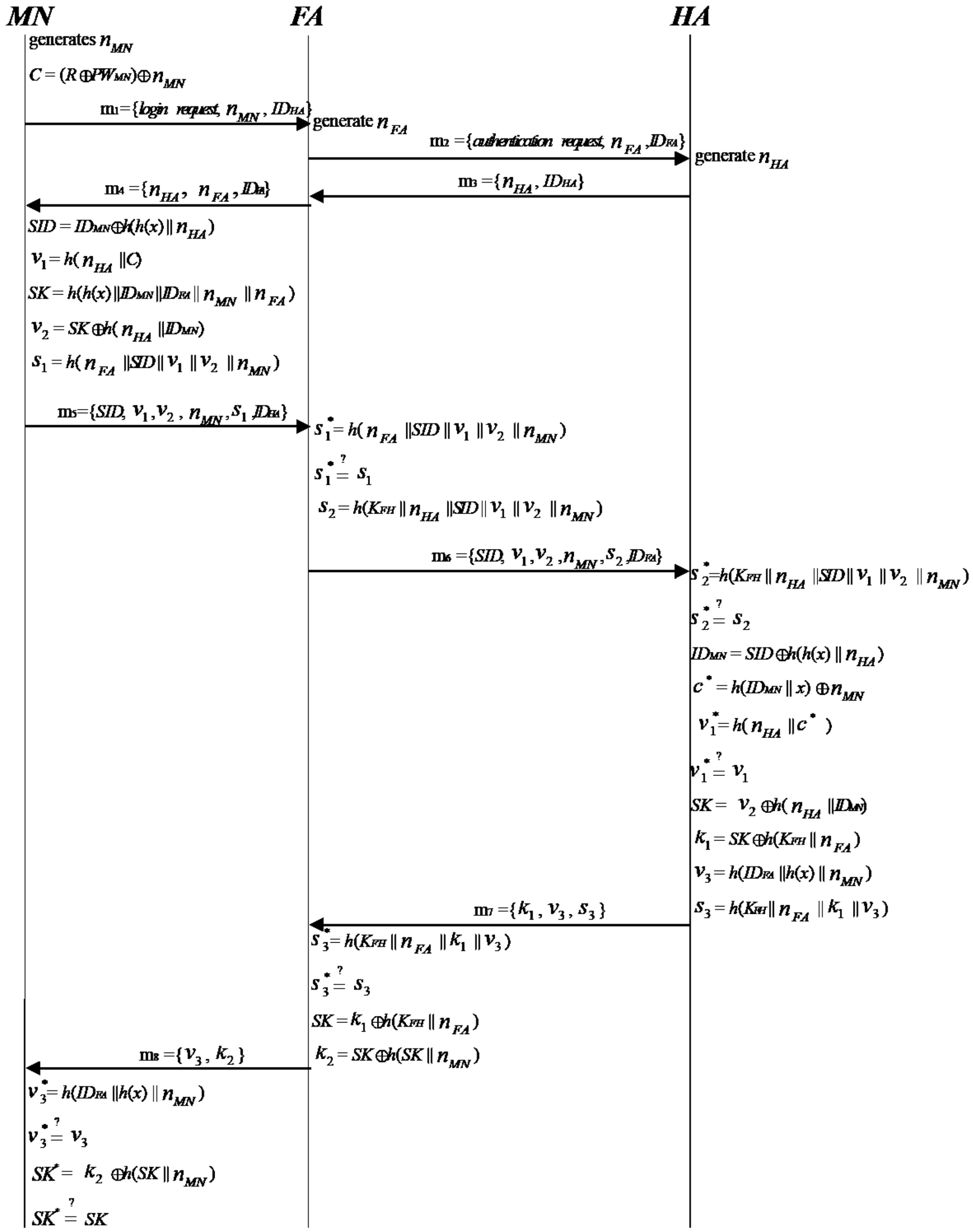
MN
FA
HA
generates n_{MN}
$C=(R\oplus PW_{MN})\oplus n_{MN}$
$m_1=\{login\ request, n_{MN}, ID_{HA}\}$
generate n_{FA}
$m_2=\{authentication\ request, n_{FA}, ID_{FA}\}$
generate n_{HA}
$m_4=\{n_{HA}, n_{FA}, ID_{FA}\}$
$m_3=\{n_{HA}, ID_{HA}\}$
$SID=ID_{MN}\oplus h(h(x)\|n_{HA})$
$v_1=h(n_{HA}\|C)$
$SK=h(h(x)\|ID_{MN}\|ID_{FA}\|n_{MN}\|n_{FA})$
$v_2=SK\oplus h(n_{HA}\|ID_{MN})$
$s_1=h(n_{FA}\|SID\|v_1\|v_2\|n_{MN})$
$m_5=\{SID, v_1, v_2, n_{MN}, s_1, ID_{FA}\}$
$s_1^*=h(n_{FA}\|SID\|v_1\|v_2\|n_{MN})$
$s_1^*\overset{?}{=}s_1$
$s_2=h(K_{FH}\|n_{HA}\|SID\|v_1\|v_2\|n_{MN})$
$m_6=\{SID, v_1, v_2, n_{MN}, s_2, ID_{FA}\}$
$s_2^*=h(K_{FH}\|n_{HA}\|SID\|v_1\|v_2\|n_{MN})$
$s_2^*\overset{?}{=}s_2$
$ID_{MN}=SID\oplus h(h(x)\|n_{HA})$
$c^*=h(ID_{MN}\|x)\oplus n_{MN}$
$v_1^*=h(n_{HA}\|c^*)$
$v_1^*\overset{?}{=}v_1$
$SK=v_2\oplus h(n_{HA}\|ID_{MN})$
$k_1=SK\oplus h(K_{FH}\|n_{FA})$
$v_3=h(ID_{FA}\|h(x)\|n_{MN})$
$s_3=h(K_{FH}\|n_{FA}\|k_1\|v_3)$
$m_7=\{k_1, v_3, s_3\}$
$s_3^*=h(K_{FH}\|n_{FA}\|k_1\|v_3)$
$s_3^*\overset{?}{=}s_3$
$SK=k_1\oplus h(K_{FH}\|n_{FA})$
$k_2=SK\oplus h(SK\|n_{MN})$
$m_8=\{v_3, k_2\}$
$v_3^*=h(ID_{FA}\|h(x)\|n_{MN})$
$v_3^*\overset{?}{=}v_3$
$SK^*=k_2\oplus h(SK\|n_{MN})$
$SK^*\overset{?}{=}SK$

FIGURE 2. Authentication and session key establishment of the Chang et al. scheme

After receiving the authentication request message, m_2, the *HA* assesses the ID_{FA} to determine whether the *FA* is a legitimate user. If the result is valid, the *HA* performs the following steps:

Step A5. The *HA* generates a nonce, n_{HA}.

Step A6. $HA \rightarrow FA$:$\{n_{HA}, ID_{HA}\}$. The *HA* sends $m_3 = \{n_{HA}, ID_{HA}\}$ to the *FA*.

Step A7. $FA \rightarrow MN$:$\{n_{HA}, n_{FA}, ID_{FA}\}$. After receiving the authentication request message, m_3, the *FA* sends $m_4 = \{n_{HA}, n_{FA}, ID_{FA}\}$ to the *MN*.

Step A8. After receiving message m_4, the *MN* records the nonce, n_{HA}, and the nonce,

n_{FA}.

Step A9. The *MN* computes the shadow identification $SID = ID_{MN} \oplus h(h(x) \parallel n_{HA})$ and the parameter $V_1 = h(n_{HA} \parallel C)$ of the *MN*.

Step A10. The *MN* generates the session key (*SK*) by computing

$$SK = h(h(x) \parallel ID_{MN} \parallel ID_{FA} \parallel n_{MN} \parallel n_{FA}).$$

Step A11. The *MN* computes the parameters $V_2 = SK \oplus h(n_{HA} \parallel ID_{MN})$ and

$$S_1 = h(n_{FA} \parallel SID \parallel V_1 \parallel V_2 \parallel n_{MN}).$$

Step A12. $MN \rightarrow FA$:$\{SID, V_1, V_2, n_{MN}, S_1, ID_{HA}\}$. The *MN* sends message $m_5 = \{SID, V_1, V_2, n_{MN}, S_1, ID_{HA}\}$ to the *FA*.

Step A13. After receiving message m_5, the *FA* computes $S_1^* = h(n_{FA} \parallel SID \parallel V_1 \parallel V_2 \parallel n_{MN})$. Thereafter, the *FA* assesses whether S_1^* and S_1 are equal.

Step A14. The *FA* computes the parameter $S_2 = h(K_{FH} \parallel n_{HA} \parallel SID \parallel V_1 \parallel V_2 \parallel n_{MN})$.

Step A15. $FA \rightarrow HA$:$\{SID, V_1, V_2, n_{MN}, S_2, ID_{FA}\}$. The *FA* sends message $m_6 = \{SID, V_1, V_2, n_{MN}, S_2, ID_{FA}\}$ to the *HA*.

After receiving message m_6, the *HA* assesses the ID_{FA} to determine whether the *FA* is an ally. If the result is valid, the *HA* performs the following steps:

Step A16. The *HA* computes $S_2^* = h(K_{FH} \parallel n_{HA} \parallel SID \parallel V_1 \parallel V_2 \parallel n_{MN})$, and then compares S_2^* with S_2. If they are equal, the *HA* authenticates the *FA*.

Step A17. The *HA* computes the user identification, $ID_{MN} = SID \oplus h(h(x) \parallel n_{HA})$, and verifies the user identification, ID_{MN}. If ID_{MN} is invalid, the *HA* terminates the connection.

Step A18. The *HA* computes $C^* = h(ID_{MN} \parallel x) \oplus n_{MN}$ and $V_1^* = h(n_{HA} \parallel C^*)$. Subsequently, the *HA* assesses whether V_1^* and V_1 are equal. After confirmation, the *HA* authenticates the *MN*. Otherwise, the *HA* sends a warning message to the *FA* and terminates the connection.

Step A19. The *HA* obtains the *SK* by computing $SK = V_2 \oplus h(n_{HA} \parallel ID_{MN})$.

Step A20. The *HA* computes $K_1 = SK \oplus h(K_{FH} \parallel n_{FA})$, $V_3 = h(ID_{FA} \parallel h(x) \parallel n_{MN})$, and $S_3 = h(K_{FH} \parallel n_{FA} \parallel K_1 \parallel V_3)$.

Step A21. $HA \rightarrow FA$:$\{K_1, V_3, S_3\}$. The *HA* sends message $m_7 = \{K_1, V_3, S_3\}$ to the *FA*.

Step A22. After receiving the authentication request message, m_7, the *FA* computes $S_3^* = h(K_{FH} \parallel n_{FA} \parallel K_1 \parallel V_3)$ and assesses whether S_3^* and S_3 are equal. If valid, the *FA* obtains the *SK* by computing $SK = K_1 \oplus h(K_{FH} \parallel n_{FA})$.

Step A23. The *FA* computes $K_2 = SK \oplus h(SK \parallel n_{MN})$.

Step A24. $FA \rightarrow MN$:$\{V_3, K_2\}$. The *FA* sends message $m_8 = \{V_3, K_2\}$ to the *MN*.

Step A25. After receiving message m_8, the *MN* computes $V_3^* = h(ID_{FA} \parallel h(x) \parallel n_{MN})$ and assesses whether V_3^* and V_3 are equal. If valid, the *FA* is a legal foreign agent, and the *MN* computes $SK^* = K_2 \oplus h(SK \parallel n_{MN})$. The *MN* assesses whether SK^* and *SK* are equal. After confirmation, the *MN* authenticates the *SK* of the *FA*. The *MN* records the authenticated *SK* for future communications with the *FA*.

3. Weaknesses of the Chang et al. Scheme.

This section shows that the Chang et al. scheme does not provide user anonymity and cannot counteract insider attacks [11,12]. In addition, their scheme is vulnerable to the disclosure of session keys and foreign agent spoofing (base station spoofing) [13-15].

3.1. Vulnerability to insider attacks and user anonymity attacks.

The *MN* in the GLOMONET uses the same password to access several *FA*s for convenience. An insider attack occurs when a user password is obtained by a privileged insider of the server in the registration phase [11,12]. In Step R1 of the Chang et al. scheme, the *MN* registers with the *HA* by presenting the PW_{MN}. Because the PW_{MN} is revealed to the *HA*, a privileged insider of the *HA* can obtain the PW_{MN} directly. Therefore, this scheme is vulnerable to insider attacks.

The anonymity property is a guarantee to mobile users that their identities are disclosed only to specified service providers, and that they cannot be obtained by others. However, the Chang et al. scheme cannot withstand user anonymity attacks.

Suppose that an adversary, *Eve*, is a legal user of the system. *Eve* may eavesdrop on the message m_4 transmitted in Step A7 and the message m_5 in Step A12 during a prior login of the *MN*; that is, $\{n_{HA}, n_{FA}, ID_{FA}\}$ and $\{SID, V_1, V_2, n_{MN}, S_1, ID_{HA}\}$. Because *Eve* is a legal user, she can obtain $\{ID_e, ID_{HAe}, R_e, h(x), h(.)\}$ from her smart card. As shown in the equation in Step A9, the shadow identification of the *MN* is $SID = ID_{MN} \oplus h(h(x) \parallel n_{HA})$, and solving for the next step yields the following:

$SID \oplus h(h(x) \parallel n_{HA}) = ID_{MN} \oplus h(h(x) \parallel n_{HA}) \oplus h(h(x) \parallel n_{HA}) = ID_{MN}$; that is,

$$ID_{MN} = SID \oplus h(h(x) \parallel n_{HA}).$$

As mentioned, *Eve* has obtained the parameter $h(x)$ from her smart card, the parameter *SID* from message m_5 of the *MN*, and the parameter n_{HA} from message m_4 of the *MN*. Therefore, an adversary can determine the identification ID_{MN} of the *MN* to identify the *MN* who is attempting to log into the system. This shows that the Chang et al. scheme cannot maintain user anonymity and is vulnerable to user anonymity attacks.

3.2. **Vulnerability to session key disclosures and foreign agent spoofing.** Reconsider the same scenario. The adversary, *Eve*, is a legal user of the system. *Eve* may eavesdrop on the message m_4 transmitted in Step A7 and the message m_5 in Step A12 during a prior login of the *MN*; that is, $\{n_{HA}, n_{FA}, ID_{FA}\}$ and $\{SID, V_1, V_2, n_{MN}, S_1, ID_{HA}\}$. Because *Eve* is a legal user, she can obtain $\{ID_e, ID_{HAe}, R_e, h(x), h(.)\}$ from her smart card. As shown in the last subsection, *Eve* can obtain the identification ID_{MN} of the *MN*. Using the equation in Step A11, the parameter $V_2 = SK \oplus h(n_{HA} \parallel ID_{MN})$, we can obtain

$V_2 \oplus h(n_{HA} \parallel ID_{MN}) = SK \oplus h(n_{HA} \parallel ID_{MN}) \oplus h(n_{HA} \parallel ID_{MN}) = SK$; that is,

$$SK = V_2 \oplus h(n_{HA} \parallel ID_{MN}).$$

Eve has obtained the parameter ID_{MN} of the *MN*, the parameter V_2 from message m_5 of the *MN*, and the parameter n_{HA} from message m_4 of the *MN*. Therefore, *Eve* can find the *SK* between the *MN* and the *FA* in the system. Although the *MN* and the *FA* have completed the mutual authentication process, thereby successfully establishing a common *SK*, the adversary can eavesdrop on the communication between the *MN* and the *FA*. This shows that the Chang et al. scheme is vulnerable to the disclosure of session keys between *MN*s and *FA*s in the system.

The Chang et al. scheme is also vulnerable to foreign agent spoofing (base station spoofing), which is a situation in which an adversary impersonates the foreign agent (base station) to obtain the private login information of the *MN* [13-15]. Suppose that an adversary, *Eve*, is a legal user of the system. In the Chang et al. scheme, *Eve* can use the following process to impersonate an *FA* in the system and convince an *MN* that she is legitimate. First, after receiving the login request message $m_1 = \{login\ request, n_{MN}, ID_{HA}\}$ from an *MN*, *Eve* can generate an *imitative* nonce n'_{FA} in Step A3. *Eve* can also create an *imitative* nonce n'_{HA} when pretending to obtain the nonce n'_{HA} from the *HA*. *Eve* can then send the imitative response message $m'_4 = \{n'_{HA}, n'_{FA}, ID'_{FA}\}$ to the *MN*. After receiving message m'_4, the *MN* computes the shadow identification $SID' = ID_{MN} \oplus h(h(x) \parallel n'_{HA})$ and the parameter $V'_1 = h(n'_{HA} \parallel C)$. The *MN* computes the session key $SK' = h(h(x) \parallel ID_{MN} \parallel ID'_{FA} \parallel n_{MN} \parallel n'_{FA})$, and then computes the parameters

$V_2' = SK' \oplus h(n'_{HA} \parallel ID_{MN})$ and $S_1' = h(n'_{FA} \parallel SID' \parallel V_1' \parallel V_2' \parallel n_{MN})$. The *MN* then sends message $m_5' = \{SID', V_1', V_2', n_{MN}, S_1', ID_{HA}\}$ to *Eve*. After receiving message m_5', *Eve* can obtain the identification ID_{MN} by computing $ID_{MN} = SID' \oplus h(h(x) \parallel n'_{HA})$ because the value $h(x)$ can be found in her smart card. Thereafter, *Eve* can obtain the $SK' = V_2' \oplus h(n'_{HA} \parallel ID_{MN})$ directly, without assistance from the *HA*. Finally, *Eve* can compute $K_2' = SK' \oplus h(SK' \parallel n_{MN})$ and $V_3' = h(ID'_{FA} \parallel h(x) \parallel n_{MN})$. Therefore, *Eve* can send the imitative response message $m_8' = \{V_3', K_2'\}$ to the *MN*. After receiving message m_8, the *MN* computes $V'^*_3 = h(ID'_{FA} \parallel h(x) \parallel n_{MN})$ and finds that V'^*_3 is equal to V_3'. Consequently, *Eve* is treated as a legal *FA*. The *MN* computes $SK'^* = K_2' \oplus h(SK' \parallel n_{MN})$ and finds that SK'^* is equal to SK'. The *MN* then authenticates the SK' provided by *Eve*. The *MN* records the authenticated SK' and then communicates with the false *FA*, who is the adversary *Eve*. Therefore, the Chang et al. scheme is vulnerable to foreign agent spoofing.

4. **Proposed Scheme.**

To overcome the weaknesses of the Chang et al. scheme, we propose a more secure and efficient authentication scheme with anonymity in the GLOMO NET. The proposed scheme uses only simple hash functions to achieve computational efficiency. The dynamic ID is used in the proposed scheme to achieve user anonymity and security [9,23]. The scheme is nonce-based; therefore, it does not have a time-synchronization problem [9]. Table 1 shows the notations used in our scheme. The GLOMONET contains three participants: the *MN*, the *HA*, and the *FA*. The *HA* selects a secret private key, Kx. Only the *HA* knows its private key. In addition, the *HA* also shares a long-term common secret key, K_{HF}, with each *FA*. The K_{HF} can be created using any key agreement protocol [3]. Each common secret key, K_{HF}, is unique and shared between each *FA* and the *HA*. The proposed scheme consists of two phases: the registration phase and verification phase, which are described in the following subsections.

4.1. **Registration phase.**

When a new *MN* registers, the *MN* must select the identification ID_{MN} and password PW_{MN}. Figure 3 shows the handshake process between the *MN* and the *HA* in the registration phase. During the process, the two entities perform the following steps:
Step R1. The *MN* freely selects a random number, r, and then computes $h(r \oplus PW_{MN})$.
Step R2. $MN \Rightarrow HA$:$\{ID_{MN}, h(r \oplus PW_{MN})\}$. The *MN* sends ID_{MN} and $h(r \oplus PW_{MN})$ to the *HA* to register through a secure channel.
Step R3. The *HA* computes $P = h(ID_{MN} \parallel h(r \oplus PW_{MN}))$, $A = h(P \parallel h(Kx \parallel ID_{HA}))$, and $S = A \oplus h(r \oplus PW_{MN})$.
Step R4. $HA \Rightarrow MN$:$\{ID_{HA}, S, h(.)\}$. The *HA* issues a smart card with the secret parameters $\{ID_{HA}, S, h(.)\}$ to the *MN* through a secure channel.
Step R5. The *MN* enters the random number r into the smart card. Thereafter, the smart card contains the secret parameters $\{r, ID_{HA}, S, h(.)\}$.

4.2. **Verification phase.**

When an *MN* roams into a foreign network managed by an *FA*, the *FA* must authenticate the *MN* through the *HA* of the *MN*. The verification phase is shown in Figure 4. For authentication, the *MN* keys his/her PW_{MN} and then performs the following steps:
Step V1. The *MN* generates a random nonce n_{MN} and computes $A = S \oplus h(r \oplus PW_{MN})$, $P = h(ID_{MN} \parallel h(r \oplus PW_{MN}))$, $T = P \oplus h(ID_{HA} \parallel ID_{FA} \parallel n_{MN})$, $U = h(r \oplus PW_{MN}) \oplus h(ID_{MN} \parallel A \parallel n_{MN})$, $SID = ID_{MN} \oplus h(A \parallel ID_{FA} \parallel n_{MN})$, and $q_1 = h(S \parallel A \parallel n_{MN})$.
Step V2. $MN \rightarrow FA$:$\{SID, U, T, q_1, ID_{HA}, n_{MN}\}$. The *MN* sends the login request message $m_1 = \{SID, U, T, q_1, ID_{HA}, n_{MN}\}$ to the *FA*.

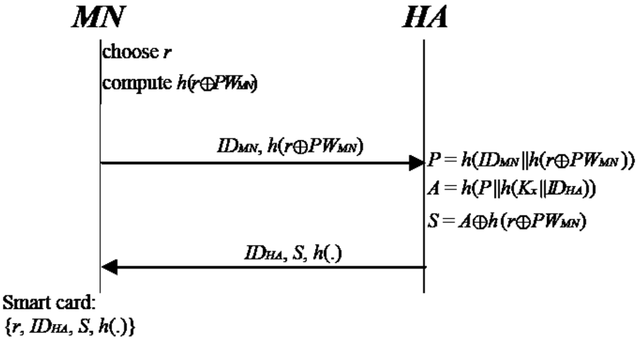
MN
HA
choose r
compute $h(r\oplus PW_{MN})$
$ID_{MN}, h(r\oplus PW_{MN})$
$P=h(ID_{MN}\|h(r\oplus PW_{MN}))$
$A=h(P\|h(K_x\|ID_{HA}))$
$S=A\oplus h(r\oplus PW_{MN})$
$ID_{HA}, S, h(.)$
Smart card:
$\{r, ID_{HA}, S, h(.)\}$

Figure 3. Registration phase of the proposed scheme

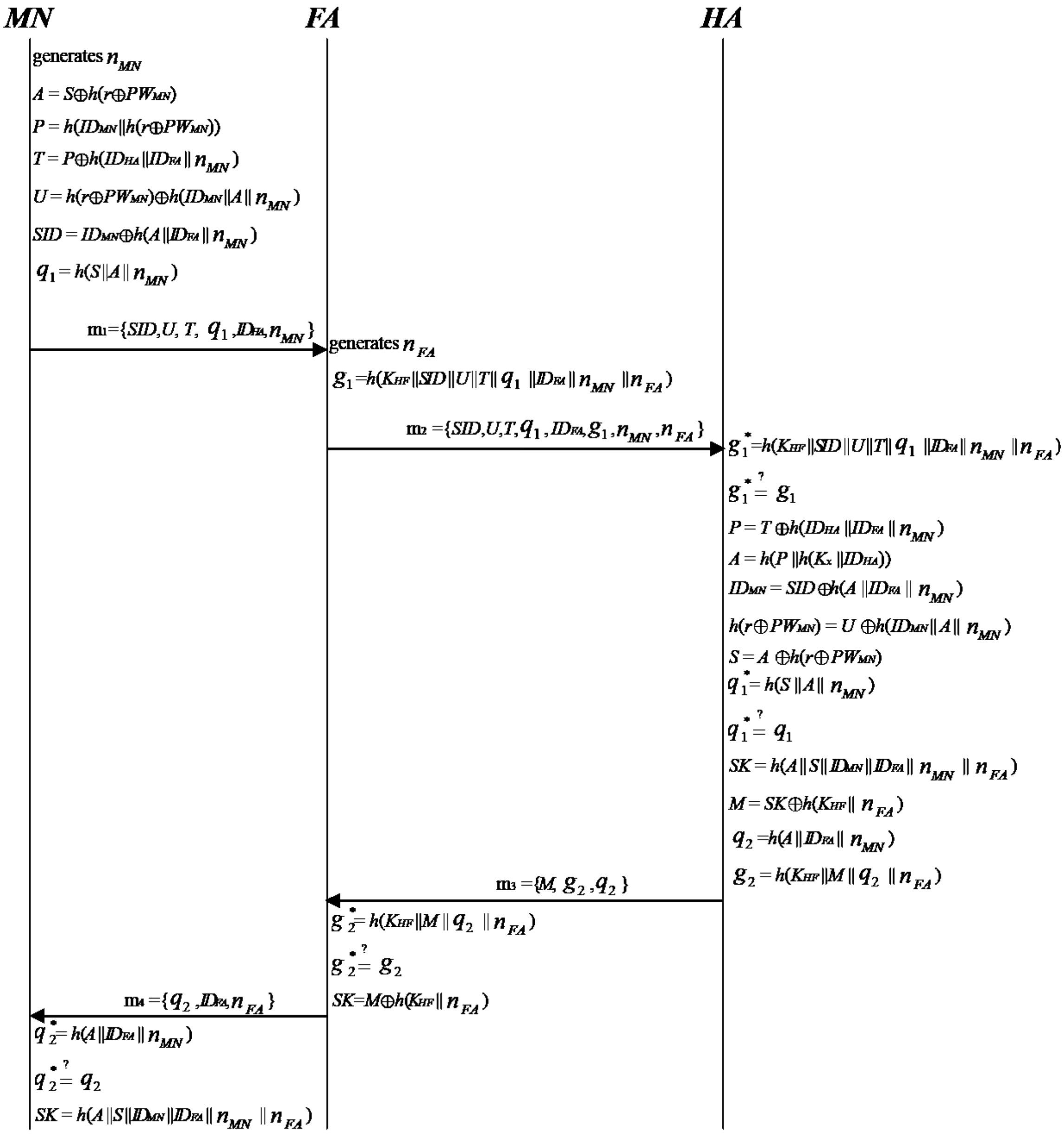
MN
FA
HA
generates n_{MN}
$A=S\oplus h(r\oplus PW_{MN})$
$P=h(ID_{MN}\|h(r\oplus PW_{MN}))$
$T=P\oplus h(ID_{HA}\|ID_{FA}\|n_{MN})$
$U=h(r\oplus PW_{MN})\oplus h(ID_{MN}\|A\|n_{MN})$
$SID=ID_{MN}\oplus h(A\|ID_{FA}\|n_{MN})$
$q_1=h(S\|A\|n_{MN})$
$m_1=\{SID,U,T,q_1,ID_{HA},n_{MN}\}$
generates n_{FA}
$g_1=h(K_{HF}\|SID\|U\|T\|q_1\|ID_{FA}\|n_{MN}\|n_{FA})$
$m_2=\{SID,U,T,q_1,ID_{FA},g_1,n_{MN},n_{FA}\}$
$g_1^*=h(K_{HF}\|SID\|U\|T\|q_1\|ID_{FA}\|n_{MN}\|n_{FA})$
$g_1^*\overset{?}{=}g_1$
$P=T\oplus h(ID_{HA}\|ID_{FA}\|n_{MN})$
$A=h(P\|h(K_x\|ID_{HA}))$
$ID_{MN}=SID\oplus h(A\|ID_{FA}\|n_{MN})$
$h(r\oplus PW_{MN})=U\oplus h(ID_{MN}\|A\|n_{MN})$
$S=A\oplus h(r\oplus PW_{MN})$
$q_1^*=h(S\|A\|n_{MN})$
$q_1^*\overset{?}{=}q_1$
$SK=h(A\|S\|ID_{MN}\|ID_{FA}\|n_{MN}\|n_{FA})$
$M=SK\oplus h(K_{HF}\|n_{FA})$
$q_2=h(A\|ID_{FA}\|n_{MN})$
$g_2=h(K_{HF}\|M\|q_2\|n_{FA})$
$m_3=\{M,g_2,q_2\}$
$g_2^*=h(K_{HF}\|M\|q_2\|n_{FA})$
$g_2^*\overset{?}{=}g_2$
$SK=M\oplus h(K_{HF}\|n_{FA})$
$m_4=\{q_2,ID_{FA},n_{FA}\}$
$q_2^*=h(A\|ID_{FA}\|n_{MN})$
$q_2^*\overset{?}{=}q_2$
$SK=h(A\|S\|ID_{MN}\|ID_{FA}\|n_{MN}\|n_{FA})$

Figure 4. The verification phase of the proposed scheme

After receiving the login request message m_1, the *FA* obtains the *HA* information by recognizing ID_{HA}. Thereafter, the *FA* performs the following steps:
Step V3. The *FA* generates a nonce n_{FA} and computes $g_1 = h(K_{HF} \parallel SID \parallel U \parallel T \parallel q_1 \parallel ID_{FA} \parallel n_{MN} \parallel n_{FA})$. The K_{HF} is a pre-shared common secret key between the *HA* and the *FA*.
Step V4. $FA \rightarrow HA$:$\{SID, U, T, q_1, ID_{FA}, g_1, n_{MN}, n_{FA}\}$. The *FA* sends message $m_2 = \{SID, U, T, q_1, ID_{FA}, g_1, n_{MN}, n_{FA}\}$ to the *HA*.

After receiving message m_2, the *HA* assesses the ID_{FA} to determine whether the *FA* is an ally. If the result is valid, the *HA* executes the following steps:
Step V5. The *HA* computes $g_1^* = h(K_{HF} \parallel SID \parallel U \parallel T \parallel q_1 \parallel ID_{FA} \parallel n_{MN} \parallel n_{FA})$, and then compares g_1^* with g_1. If they are equal, the *HA* authenticates the *FA*. The *HA* then computes $P = T \oplus h(ID_{HA} \parallel ID_{FA} \parallel n_{MN})$, $A = h(P \parallel h(Kx \parallel ID_{HA}))$, and $ID_{MN} = SID \oplus h(A \parallel ID_{FA} \parallel n_{MN})$. The *HA* also assesses whether the ID_{MN} is registered.
Step V6. The *HA* computes $h(r \oplus PW_{MN}) = U \oplus h(ID_{MN} \parallel A \parallel n_{MN})$, $S = A \oplus h(r \oplus PW_{MN})$, and $q_1^* = h(S \parallel A \parallel n_{MN})$, and then compares q_1^* with q_1. If they are equal, the *HA* authenticates the *MN* and generates the *SK* by computing $SK = h(A \parallel S \parallel ID_{MN} \parallel ID_{FA} \parallel n_{MN} \parallel n_{FA})$.
Step V7. The *HA* computes $M = SK \oplus h(K_{HF} \parallel n_{FA})$, $q_2 = h(A \parallel ID_{FA} \parallel n_{MN})$, and $g_2 = h(K_{HF} \parallel M \parallel q_2 \parallel n_{FA})$.
Step V8. $HA \rightarrow FA$:$\{M, g_2, q_2\}$. The *HA* sends message $m_3 = \{M, g_2, q_2\}$ to the *FA*.

After receiving message m_3, the *FA* performs the following steps to authenticate the *HA*:
Step V9. The *FA* computes $g_2^* = h(K_{HF} \parallel M \parallel q_2 \parallel n_{FA})$ and compares g_2^* with g_2. If they are equal, the *FA* authenticates the *HA*. Thereafter, the *FA* computes the session key $SK = M \oplus h(K_{HF} \parallel n_{FA})$.
Step V10. $FA \rightarrow MN$:$\{q_2, ID_{FA}, n_{FA}\}$. The *FA* sends message $m_4 = \{q_2, ID_{FA}, n_{FA}\}$ to the *MN*.

After receiving message m_4, the *MN* performs the following steps to authenticate the *HA*:
Step V11. The *MN* computes $q_2^* = h(A \parallel ID_{FA} \parallel n_{MN})$ and compares q_2^* with q_2. If they are equal, the *MN* authenticates the *HA*. Thereafter, the *MN* computes the $SK = h(A \parallel S \parallel ID_{MN} \parallel ID_{FA} \parallel n_{MN} \parallel n_{FA})$.

5. Security Analysis of the Proposed Scheme.

This section presents an analysis of the security of the proposed scheme. First, we verified that the proposed scheme can provide mutual authentication between the involved entities in the GLOMONET. Subsequently, we show that the proposed scheme can overcome the weaknesses of the Chang et al. scheme and prevent other possible attacks in the GLOMONET.

5.1. Mutual authentication and session key establishment.

The Burrows-Abadi-Needham (BAN) logic [8,10] method is widely used to prove the validity of authentication and key establishment protocols. In the basic notation of BAN logic, P and Q range over principals, X and Y range over statements, and K is the encryption key. Table 2 shows the constructs of the BAN logic.

The main logical postulates of the BAN logic used in the proofs are as follows [8,10]:

(1) *Message-meaning* rule for shared secrets: $\frac{P|\equiv Q \overset{y}{\rightleftharpoons} P, P \triangleleft \langle X \rangle_y}{P|\equiv Q|\sim X}$

(2) *Nonce-verification* rule: $\frac{P|\equiv \#(X), P|\equiv Q|\sim X}{P|\equiv Q|\equiv X}$

(3) *Jurisdiction* rule: $\frac{P|\equiv Q|\Rightarrow X, P|\equiv Q|\equiv X}{P|\equiv X}$

Table 2. Constructs of the BAN logic

Notation	Definition
$P\vert\equiv X$	P ***believes*** X: P would be entitled to believe X.
$P\lhd X$	P ***sees*** X: P can receive and read X.
$P\vert\sim X$	P ***said***X: P once said X.
$P\vert\Rightarrow X$	P ***controls*** X: P has jurisdiction over X.
$\#(X)$	***fresh*** (X): The formula X is fresh.
$\langle X\rangle_y$	X combined with the formula y; it is intended that y be a secret.
$P\overset{K}{\leftrightarrow}Q$	P and Q may use the shared key K to communicate.
$P\overset{y}{\rightleftharpoons}Q$	The formula y is a secret known only to P and Q.

(4) *Receiving* rule: $\frac{P\lhd(X,Y)}{P\lhd X}$ and $\frac{P\lhd\langle X\rangle_y}{P\lhd X}$

(5) *Freshness-propagation* rule: $\frac{P|\equiv\#(X)}{P|\equiv\#(X,Y)}$

(6) *Session-key* rule: $\frac{P|\equiv\#(K),P|\equiv Q|\equiv X}{P|\equiv \mathrm{P}\overset{K}{\leftrightarrow}\mathrm{Q}}$, where X is an essential variable of combination key K [10,20].

As shown in Step R3, $h(r\oplus PW_{MN}) = A\oplus S$. The proposed protocol is then summarized in the following generic form:

Message m_1. $MN \to FA$:$\{SID, U, T, q_1, ID_{HA}, n_{MN}\} = \{ID_{MN}\oplus h(A\parallel ID_{FA}\parallel n_{MN}), A\oplus S\oplus h(ID_{MN}\parallel A\parallel n_{MN}), P\oplus h(ID_{HA}\parallel ID_{FA}\parallel n_{MN}), h(S\parallel A\parallel n_{MN}), ID_{HA}, n_{MN}\}$.

Message m_2. $FA\to HA$:$\{SID, U, T, q_1, ID_{FA}, g_1, n_{MN}, n_{FA}\} = \{ID_{MN}\oplus h(A\parallel ID_{FA}\parallel n_{MN}), A\oplus S\oplus h(ID_{MN}\parallel A\parallel n_{MN}), P\oplus h(ID_{HA}\parallel ID_{FA}\parallel n_{MN}), h(S\parallel A\parallel n_{MN}), ID_{FA}, g_1, n_{MN}, n_{FA}\}$, where $g_1 = h(K_{HF}\parallel SID\parallel U\parallel T\parallel q_1\parallel ID_{FA}\parallel n_{MN}\parallel n_{FA}) = h(K_{HF}\parallel ID_{MN}\oplus h(A\parallel ID_{FA}\parallel n_{MN})\parallel A\oplus S\oplus h(ID_{MN}\parallel A\parallel n_{MN})\parallel P\oplus h(ID_{HA}\parallel ID_{FA}\parallel n_{MN})\parallel h(S\parallel A\parallel n_{MN})\parallel ID_{FA}\parallel n_{MN}\| n_{FA})$.

Message m_3. $HA\to FA$:$\{M, g_2, q_2\} = \{SK\oplus h(K_{HF}\parallel n_{FA}), h(K_{HF}\parallel SK\oplus h(K_{HF}\parallel n_{FA})\parallel h(A\parallel ID_{FA}\parallel n_{MN})\parallel n_{FA}), h(A\parallel ID_{FA}\parallel n_{MN})\}$.

Message m_4. $FA\to MN$:$\{q_2, ID_{FA}, n_{FA}\} = \{h(A\parallel ID_{FA}\parallel n_{MN}), ID_{FA}, n_{FA}\}$.

We idealized the protocol by transferring the generic form into the following idealized form [10]:

I$_1$. $MN\to FA$: $\langle n_{MN}\rangle_A$, $\langle\langle n_{MN}\rangle_A\rangle_S$, $\langle n_{MN}\rangle_P$, $\langle\langle n_{MN}\rangle_A\rangle_S$

I$_2$. $FA\to HA$: $\langle n_{MN}\rangle_A$, $\langle\langle n_{MN}\rangle_A\rangle_S$, $\langle n_{MN}\rangle_P$, $\langle\langle n_{MN}\rangle_A\rangle_S$, $\langle\langle\langle\langle n_{MN}, n_{FA}\rangle_{K_{HF}}\rangle_A\rangle_S\rangle_P$

I$_3$. $HA\to FA$: $\langle\langle n_{FA}\rangle_{K_{HF}}\rangle_{SK}$, $\langle\langle\langle n_{MN}, n_{FA}\rangle_A\rangle_{K_{HF}}\rangle_{SK}$, $\langle n_{MN}\rangle_A$

I$_4$. $FA\to MN$: $\langle n_{MN}\rangle_A$

The following assumptions were used to analyze the proposed protocol:

A$_1$. $MN|\equiv MN\overset{A}{\rightleftharpoons}HA$ A$_2$. $HA|\equiv MN\overset{A}{\rightleftharpoons}HA$

A$_3$. $FA|\equiv FA\overset{k_{HF}}{\rightleftharpoons}HA$ A$_4$. $HA|\equiv FA\overset{k_{HF}}{\rightleftharpoons}HA$

A$_5$. $HA|\equiv\#(n_{MN})$ A$_6$. $MN|\equiv\#(n_{MN})$

A$_7$. $HA|\equiv\#(n_{FA})$ A$_8$. $FA|\equiv\#(n_{FA})$

A$_9$. $HA|\equiv MN|\Rightarrow n_{MN}$ A$_{10}$. $MN|\equiv HA|\Rightarrow n_{MN}$

A$_{11}$. $HA|\equiv FA|\Rightarrow n_{FA}$ A$_{12}$. $FA|\equiv HA|\Rightarrow n_{FA}$

Lemma 5.1. *The HA can authenticate the MN and the FA in the proposed protocol.*

Proof: In the proposed protocol, the *MN* and the *FA* generate a nonce n_{MN} and a nonce n_{FA}, respectively. The following beliefs must be verified to show that the *HA* can authenticate the *MN* and the *FA*:

B$_1$. $HA|\equiv n_{MN}$

B$_2$. $HA| \equiv n_{FA}$

For B$_1$, the main steps of the proof are as follows:

S$_1$. *HA* ***sees*** $\langle n_{MN} \rangle_A$. (Using I$_2$ and the *Receiving* rule)

S$_2$. *HA* ***believes*** *MN* ***said*** n_{MN}. (Using A$_2$, S$_1$, and the *Message-meaning* rule)

S$_3$. *HA* ***believes*** *MN* ***believes*** n_{MN}. (Using A$_5$, S$_2$, and the *Nonce-verification* rule)

S$_4$. *HA* ***believes*** n_{MN}; *that is*, $HA| \equiv n_{MN}$. (Using A$_9$, S$_3$, and the *Jurisdiction* rule)

Therefore, the *HA* can authenticate the *MN*. Similarly, for B$_2$, the main steps of the proof are as follows:

S$_5$. *HA* ***sees*** $\langle n_{FA} \rangle_{K_{HF}}$. (Using I$_2$ and the *Receiving* rule)

S$_6$. *HA* ***believes*** *FA* ***said*** n_{FA}. (Using A$_4$, S$_5$, and the *Message-meaning* rule)

S$_7$. *HA* ***believes*** *FA* ***believes*** n_{FA}. (Using A$_7$, S$_6$, and the *Nonce-verification* rule)

S$_8$. *HA* ***believes*** n_{FA}; *that is*, $HA| \equiv n_{FA}$. (Using A$_{11}$, S$_7$, and the *Jurisdiction* rule)

Lemma 5.2. *The MN and the FA in the proposed protocol can authenticate the HA.*

Proof: In the proposed protocol, after receiving n_{MN} and n_{FA}, the *HA* returns them to the *FA* and *MN*, respectively. The following beliefs must be verified to show that the *FA* and the *MN* can authenticate the *HA*:

B$_3$. $FA| \equiv n_{FA}$

B$_4$. $MN| \equiv n_{MN}$

For B$_3$, the main steps of the proof are as follows:

S$_9$. *FA* ***sees*** $\langle n_{FA} \rangle_{K_{HF}}$. (Using I$_3$ and *Receiving* rule)

S$_{10}$. *FA* ***believes*** *HA* ***said*** n_{FA}. (Using A$_3$, S$_9$, and the *Message-meaning* rule)

S$_{11}$. *FA* ***believes*** *HA* ***believes*** n_{FA}. (Using A$_8$, S$_{10}$, and the *Nonce-verification* rule)

S$_{12}$. *FA* ***believes*** n_{FA}; *that is*, $FA| \equiv n_{FA}$. (Using A$_{12}$, S$_{11}$, and the *Jurisdiction* rule)

Therefore, the *FA* can authenticate the *HA*. For B$_4$, the main steps of the proof are similar, as follows:

S$_{13}$. *MN* ***sees*** $\langle n_{MN} \rangle_A$. (Using I$_4$ and *Receiving* rule)

S$_{14}$. *MN* ***believes*** *HA* ***said*** n_{MN}. (Using A$_1$, S$_{13}$, and the *Message-meaning* rule)

S$_{15}$. *MN* ***believes*** *HA* ***believes*** n_{MN}. (Using A$_6$, S$_{14}$, and the *Nonce-verification* rule)

S$_{16}$. *MN* ***believes*** n_{MN}; *that is*, $MN| \equiv n_{MN}$. (Using A$_{10}$, S$_{15}$, and the *Jurisdiction* rule)

Lemma 5.3. *The MN and the FA in the proposed protocol can share a session key SK.*

Proof: In the proposed protocol, the following beliefs must be verified to show that the *MN* and the *FA* can share an $SK = h(A \parallel S \parallel ID_{MN} \parallel ID_{FA} \parallel n_{MN} \parallel n_{FA})$:

B$_5$. $FA| \equiv MN \overset{sk}{\leftrightarrow} FA$

B$_6$. $MN| \equiv MN \overset{sk}{\leftrightarrow} FA$

For B$_5$, the main steps of the proof are as follows:

S$_{17}$. *FA* ***believes*** *HA* ***believes*** n_{FA}. (Using S$_{11}$)

S$_{18}$. *HA* ***believes*** *MN* ***believes*** n_{MN}. (Using S$_3$)

S$_{19}$. *FA* ***believes*** *MN* ***believes*** n_{MN}. (Using S$_{17}$, S$_{18}$, Lemma 5.1, and Lemma 5.2)

S$_{20}$. *FA* ***believes*** ***fresh*** (*SK*). (Using A$_8$ and the *Freshness-propagation* rule)

S$_{21}$. *FA* ***believes*** $MN \overset{sk}{\leftrightarrow} FA$; *that is*, $FA| \equiv MN \overset{sk}{\leftrightarrow} FA$. (Using S$_{19}$, S$_{20}$, and the *Session-key* rule)

S$_{21}$ shows that the *FA* believes to have the *SK* that is shared with the *MN*.

For B$_6$, the main steps of the proof are similar, as follows:

S$_{22}$. *MN* ***believes*** *HA* ***believes*** n_{MN}. (Using S$_{15}$)

S$_{23}$. *HA* ***believes*** *FA* ***believes*** n_{FA}. (Using S$_7$)

S$_{24}$. *MN* ***believes*** *FA* ***believes*** n_{FA}. (Using S$_{22}$, S$_{23}$, Lemma 5.1, and Lemma 5.2)

S$_{25}$. *MN* ***believes fresh*** (*SK*). (Using A$_6$ and the *Freshness-propagation* rule)

S$_{26}$. *MN* ***believes*** $MN \overset{sk}{\leftrightarrow} FA$; that is, $MN| \equiv MN \overset{sk}{\leftrightarrow} FA$. (Using S$_{24}$, S$_{25}$, and the *Session-key* rule)

S$_{26}$ shows that *MN* believes to have an *SK* that is shared with the *FA*.

Proposition 5.1. *The MN and the FA in the proposed protocol can mutually authenticate each other and share an established session key SK.*

Proof: Lemma 5.1 shows that the *HA* can authenticate the validity of the *MN* and the *FA*. Moreover, Lemma 5.2 shows that the *MN* and the *FA* can authenticate the *HA*. Therefore, the *MN* and the *FA* can mutually authenticate each other with the assistance of the *HA*. Mutual authentication is achieved in the proposed scheme. Finally, Lemma 5.3 verified that the *MN* and the *FA* can coordinate a common $SK = h(A \parallel S \parallel ID_{MN} \parallel ID_{FA} \parallel n_{MN} \parallel n_{FA})$ after completing the mutual authentication process. The *MN* and the *FA* share and verify the established *SK*. In other words, the proposed scheme can provide mutual authentication and session key establishment.

Generally, when an *MN* roams into a foreign network managed by an *FA*, the *MN* and the *FA* must mutually authenticate each other through the *HA* of the *MN*. In the verification phase of the proposed scheme, after receiving the message $m_2 = \{SID, U, T, q_1, ID_{FA}, g_1, n_{MN}, n_{FA}\}$ from the *FA*, the *HA* computes $h(r \oplus PW_{MN}) = U \oplus h(ID_{MN} \parallel A \parallel n_{MN})$, $S = A \oplus h(r \oplus PW_{MN})$, and $q_1^* = h(S \parallel A \parallel n_{MN})$. The *HA* then compares q_1^* with q_1 in Step V6. If they are equal, the *HA* authenticates the *MN*. In Step V9, after receiving message $m_3 = \{M, g_2, q_2\}$, the *FA* computes $g_2^* = h(K_{HF} \parallel M \parallel q_2 \parallel n_{FA})$ and compares g_2^* with g_2. If they are equal, the *FA* authenticates the *HA*. Because the *HA* has authenticated the *MN*, the *FA* can further authenticate the *MN*. In Step V5, after receiving the message $m_2 = \{SID, U, T, q_1, ID_{FA}, g_1, n_{MN}, n_{FA}\}$ from the *FA*, the *HA* computes $g_1^* = h(K_{HF} \parallel SID \parallel U \parallel T \parallel q_1 \parallel ID_{FA} \parallel n_{MN} \parallel n_{FA})$ and compares g_1^* with g_1. If they are equal, the *HA* authenticates the *FA*. Moreover, in Step V11, after receiving the message $m_4 = \{q_2, ID_{FA}, n_{FA}\}$, the *MN* computes $q_2^* = h(A \parallel ID_{FA} \parallel n_{MN})$ and compares q_2^* with q_2. If they are equal, the *MN* authenticates the *HA*. Because the *HA* has authenticated the *FA*, the *MN* can provide further authentication of the *FA*. This further demonstrates that the proposed scheme can provide mutual authentication between the *MN* and the *FA*.

5.2. **Forgery attacks and relay attacks.** A forgery attack occurs when an adversary impersonates an *MN* to deceive an *FA* (or *HA*) and gains access to their services [3].

Proposition 5.2. *The proposed scheme is secure against forgery attacks and relay attacks.*

Proof: To impersonate an *MN*, the adversary, *Eve*, may first intercept the login request message m_1 transmitted in Step V2 during a prior login of the *MN*; that is, $\{SID, U, T, q_1, ID_{HA}, n_{MN}\}$. We may even suppose that *Eve* is a legal user of the system. Because of her legal status, she has $\{ID_e, PW_e\}$ and can obtain $\{r_e, ID_{HAe}, S_e, h(.)\}$ from her smart card. To impersonate the *MN*, *Eve* must generate a new nonce n'_{MN} and send an *imitative* login request message $\{SID', U', T', q'_1, ID_{HA}, n'_{MN}\}$ to the *FA*, where $SID' = ID_{MN} \oplus h(A \parallel ID_{FA} \parallel n'_{MN})$, $U' = h(r \oplus PW_{MN}) \oplus h(ID_{MN} \parallel A \parallel n'_{MN})$, $T' = P \oplus h(ID_{HA} \parallel ID_{FA} \parallel n'_{MN})$, and $q'_1 = h(S \parallel A \parallel n'_{MN})$. To obtain the parameters SID', U', T', and q'_1, *Eve* must first acquire A, P, and $h(r \oplus PW_{MN})$ by using the following equations:

$A = h(P \parallel h(Kx \parallel ID_{HA}))$, $A = S \oplus h(r \oplus PW_{MN})$, $P = h(ID_{MN} \parallel h(r \oplus PW_{MN}))$, $P = T \oplus h(ID_{HA} \parallel ID_{FA} \parallel n_{MN})$, and $h(r \oplus PW_{MN}) = U \oplus h(ID_{MN} \parallel A \parallel n_{MN})$.

However, *Eve* cannot obtain A because she does not know Kx and $h(r \oplus PW_{MN})$. In the proposed scheme, only the *HA* knows its secret private key, Kx. Therefore, the parameters $\{SID', U', T', q_1'\}$ in the *imitative* login request message cannot be obtained, preventing *Eve* from impersonating the *MN* to access the system. This shows that the proposed scheme can withstand forgery attacks.

In a relay attack, *Eve* may replay the intercepted login request message $\{SID, U, T, q_1, ID_{HA}, n_{MN}\}$ to the *FA*. However, after receiving message m_4, *Eve* cannot compute the $SK = h(A \parallel S \parallel ID_{MN} \parallel ID_{FA} \parallel n_{MN} \parallel n_{FA})$ because she does not know A and S in the *SK*. Therefore, resistance to replay attacks is also guaranteed.

5.3. **Two-factor security.** The two-factor security property guarantees the security of the scheme when the smart card or the password of a user is stolen, although if they are both stolen, it does not guarantee security [9].

Proposition 5.3. *The proposed scheme is able to provide two-factor security.*

Proof: Suppose that an adversary has only the smart card of an *MN*, and does not possess the identification and password parameters; that is, $\{ID_{MN}, PW_{MN}\}$. Because the adversary has the smart card, he/she can extract the stored values $\{r, ID_{HA}, S, h(.)\}$ in the card by analyzing the leaked information or by monitoring the power consumption [24,25]. In addition, suppose that the adversary has also intercepted the login request message m_1 transmitted in Step V2 during a prior login of the *MN*; that is, $\{SID, U, T, q_1, ID_{HA}, n_{MN}\}$. To impersonate the *MN*, the adversary must generate a new nonce n'_{MN} and send an *imitative* login request message $\{SID', U', T', q_1', ID_{HA}, n'_{MN}\}$ to the *FA*, where $SID' = ID_{MN} \oplus h(A \parallel ID_{FA} \parallel n'_{MN})$, $U' = h(r \oplus PW_{MN}) \oplus h(ID_{MN} \parallel A \parallel n'_{MN})$, $T' = P \oplus h(ID_{HA} \parallel ID_{FA} \parallel n'_{MN})$, and $q_1' = h(S \parallel A \parallel n'_{MN})$. However, the adversary cannot obtain A because he/she does not know Kx and $h(r \oplus PW_{MN})$. The parameters $\{SID', U', T', q_1'\}$ in the *imitative* login request message cannot be obtained. Therefore, the adversary cannot impersonate a legal user to log into the system if the adversary has only the smart card of the user and does not possess the identification and password information. Conversely, if the adversary has the identification and password parameters of an *MN*, but not the smart card, the adversary cannot obtain A to compute the *imitative* parameters $\{SID', U', T', q_1'\}$ because he/she does not know Kx and the stored values $\{r, S\}$ in the smart card. In a word, the adversary cannot impersonate a legal user to log into the system after he/she extracts secret information from the smart card or knows the $\{ID_{MN}, PW_{MN}\}$ information. Therefore, the proposed scheme provides two-factor security.

5.4. **User anonymity.** User anonymity is a required security service to ensure that the actions of *MN*s are untraceable.

Proposition 5.4. *The proposed scheme can maintain user anonymity.*

Proof: In an anonymity attack, the adversary may first intercept and analyze the login request message $\{SID, U, T, q_1, ID_{HA}, n_{MN}\}$ of an *MN*, where $SID = ID_{MN} \oplus h(A \parallel ID_{FA} \parallel n_{MN})$, $U = h(r \oplus PW_{MN}) \oplus h(ID_{MN} \parallel A \parallel n_{MN})$, $T = P \oplus h(ID_{HA} \parallel ID_{FA} \parallel n_{MN})$, and $q_1 = h(S \parallel A \parallel n_{MN})$. However, deriving the identification ID_{MN} of the *MN* from the parameters *SID* and U is impossible because the adversary cannot obtain A; A cannot be retrieved because Kx and $h(r \oplus PW_{MN})$ are unknown to the adversary. Moreover, the nonce n_{MN} is a random number generated by the *MN*, and it varies dynamically in each login request. The values of *SID*, U, T, and q_1 are associated with the nonce n_{MN}; therefore, they are also different in each login request. Therefore, an adversary cannot identify the *MN* attempting to login to the system, thereby showing that the proposed scheme can maintain user anonymity.

5.5. **Session key disclosure and known-key security.** Known-key security ensures that compromised session keys cannot be used by an adversary to derive other session keys.

Proposition 5.5. *The proposed scheme can prevent session key disclosure and provide known-key security.*

Proof: Suppose that an adversary, *Eve*, is a legal user of the system. *Eve* may intercept the login request message $m_1 = \{SID, U, T, q_1, ID_{HA}, n_{MN}\}$ and the response message $m_4 = \{q_2, ID_{FA}, n_{FA}\}$. To find the session key, *SK*, *Eve* must first compute the *SK* from one of the following equations: $SK = h(A \parallel S \parallel ID_{MN} \parallel ID_{FA} \parallel n_{MN} \parallel n_{FA})$ or $SK = M \oplus h(K_{HF} \parallel n_{FA})$. However, the Kx and $h(r \oplus PW_{MN})$ are unknown; therefore, *Eve* cannot obtain A. *Eve* also does not know the K_{HF}. Therefore, deriving the session key *SK* from the equation $SK = h(A \parallel S \parallel ID_{MN} \parallel ID_{FA} \parallel n_{MN} \parallel n_{FA})$ or the equation $SK = M \oplus h(K_{HF} \parallel n_{FA})$ is impossible, demonstrating that the proposed scheme can prevent the session keys from being revealed. In the proposed scheme, the session key $SK = h(A \parallel S \parallel ID_{MN} \parallel ID_{FA} \parallel n_{MN} \parallel n_{FA})$ is established by the *MN* and the *HA* in each session. Nonce n_{MN} and nonce n_{FA}, which are used in the session key computation, are random and independent in each session [3]; thus, the session keys are also independent in each session. The knowledge of previous session keys cannot help an adversary derive other session keys. Therefore, the proposed scheme provides known-key security.

5.6. **Foreign agent spoofing.** To obtain the private login information of an *MN*, an adversary may impersonate the *FA*.

Proposition 5.6. *The proposed scheme can resist foreign agent spoofing attacks.*

Proof: To impersonate the *FA*, the adversary, *Eve*, must intercept the login request message $m_1 = \{SID, U, T, q_1, ID_{HA}, n_{MN}\}$ and respond with an imitative message $m'_4 = \{q'_2, ID'_{FA}, n'_{FA}\}$ to the *MN*. In addition, suppose that *Eve* is a legal user of the system. As demonstrated, *Eve* cannot obtain A because she does not know the Kx and $h(r \oplus PW_{MN})$. Therefore, *Eve* cannot obtain q'_2 from $q'_2 = h(A \parallel ID'_{FA} \parallel n_{MN})$. Finally, *Eve* cannot send the imitative message $m'_4 = \{q'_2, ID'_{FA}, n'_{FA}\}$ to respond to the *MN*, nor can she convince the *MN* that she is a legitimate *FA* in the system. Therefore, the proposed scheme can resist foreign agent spoofing attacks.

5.7. **Insider attacks, stolen verifier attacks, and verification tables.** In the proposed scheme, the *FA* and the *HA* do not maintain a verification table. A stolen verifier attack occurs when an adversary steals the password verifier of an *MN* to impersonate him or her.

Proposition 5.7. *The proposed scheme can prevent insider attacks and stolen verifier attacks.*

Proof: In the proposed scheme, the *MN* registers with the *HA* by presenting $h(r \oplus PW_{MN})$ instead of the PW_{MN}. The PW_{MN} and r are not disclosed to the *HA*. An insider of the *HA* cannot obtain the PW_{MN} directly. Moreover, an insider of the *HA* cannot obtain the PW_{MN} by performing an offline password-guessing attack on $h(r \oplus PW_{MN})$. In addition, an insider cannot disclose the secret private key Kx from $A = h(P \parallel h(Kx \parallel ID_{HA}))$ because it is protected by a hash function. Therefore, the proposed scheme can resist insider attacks [9]. Because the *FA* and the *HA* do not maintain a verification table, verifiable information from the *FA* or the *HA*, which can be used to threaten a system that was implemented using the proposed scheme, is unobtainable. Therefore, the scheme can resist stolen verifier attacks [9].

5.8. **Freely chosen password and single registration.** In the proposed scheme, when a new *MN* registers, he or she is free to choose a password PW_{MN} without the help of the *HA* in the registration process. Moreover, when an *MN* roams into a foreign network managed by a registered *FA*, the *FA* can authenticate the *MN* through the *HA* of the *MN*. Consequently, the *MN* is required to register only once with the *HA* to access the registered *FAs* in the GLOMONET. Therefore, the proposed scheme is a single registration scheme.

6. **Performance and Functionality Evaluation.**

This section presents the performance evaluation of the proposed scheme. We compared its performance and functionality with those of previous related schemes. To demonstrate the practical application of our results, we provide practical examples and apply a real-case scenario to discussing the efficiency and effectiveness of our scheme.

6.1. **Performance comparison and efficiency.** Table 3 shows a comparison of the performance of the proposed scheme and that of previous related schemes. The performance comparison can generally be divided into computational cost and communication cost [3,5]. The proposed scheme has two phases: a registration phase and verification phase (including authentication and session key establishment). For the performance comparison, we focused on the verification phase because it is the main part of an authentication scheme [3,25]. Table 3 lists the computational cost and communication cost of the verification phase in each protocol run, without considering redundant computations resulting from packet loss, interference, and so on [10]. For Table 3, we defined the notation *XOR* as the operation of the exclusive-OR, *Hash* as the operation of the one-way hash function, *Sym* as the operation of symmetric encryption/decryption, and *Asym* as the encryption/decryption operation or the signature operation using the asymmetric cryptosystem [3]. The scheme by Lee et al. [5] uses a hybrid cryptosystem for authentication. In the Lee et al. scheme, the computational costs of the *MN*, the *FA*, and the *HA* are $4Hash+3XOR+2Sym$, $4Hash+1XOR+2Sym+2Asym$, and $5Hash+3XOR+1Sym+2Asym$, respectively. In the Chang et al. scheme, the computational costs of the *MN*, the *FA*, and the *HA* are $7Hash+5XOR$, $3Hash+2XOR$, and $8Hash+3XOR$, respectively. In the proposed scheme, the computational costs of the *MN*, the *FA*, and the *HA* are $7Hash+5XOR$, $3Hash+1XOR$, and $10Hash+5XOR$, respectively. Therefore, the total

Table 3. Performance comparison of the proposed scheme and related schemes in the verification phase (including authentication and session key establishment)

Scheme	Ours	Chang et al. [3]	Lee et al. [5]
Computational cost:			
MN	$7Hash + 5XOR$	$7Hash + 5XOR$	$4Hash + 3XOR + 2Sym$
FA	$3Hash + 1XOR$	$3Hash + 2XOR$	$4Hash + 1XOR + 2Sym + 2Asym$
HA	$10Hash + 5XOR$	$8Hash + 3XOR$	$5Hash + 3XOR + 1Sym + 2Asym$
Total	$20Hash + 11XOR$	$18Hash + 10XOR$	$13Hash + 7XOR + 5Sym + 4Asym$
Time complexity	$O(1)$	$O(1)$	$O(n^3)$
Communication cost:			
Communication rounds	2	4	2
Transmitted messages	4	8	4

computational costs of the Lee et al. scheme [5], the Chang et al. scheme, and the proposed scheme are $13Hash+7XOR+5Sym+4Asym$, $18Hash+10XOR$, and $20Hash+11XOR$, respectively. The exclusive-OR operation requires few computations; its computational cost is low and is usually ignored [9,25]. The computation speed of one symmetric encryption/decryption operation is at least 100 times faster than an asymmetric encryption/decryption operation in software consideration [27-29]. Therefore, in each protocol run, the Lee et al. scheme must perform approximately $13Hash+405Sym$, the Chang et al. scheme requires approximately $18Hash$, and the proposed scheme necessitates approximately $20Hash$. According to the experimental results of the related research [9,16-19], a one-way hash function is efficient in computation, and its time complexity is less than that of symmetric or asymmetric cryptosystems. A practical example is as follows: It takes 0.0005 s to complete a one-way hash operation and 0.0087 s to finish symmetric en/decryption [26,27]. For each protocol run, the Lee et al. scheme requires 3.53 s, the Chang et al. scheme necessitates 0.009 s, and the proposed scheme can execute the run in 0.01 s. Therefore, the overall computational load of our scheme is reduced to 0.283% compared with the Lee et al. scheme, which has both symmetric and asymmetric cryptosystems. Compared with the Chang et al. scheme, the total computational cost of the proposed scheme only requires two extra hash operations (0.001 s computational time) in the computational process of the *HA*.

In Table 3, the RSA can represent the asymmetric cryptosystem. The security of the RSA is based on large integer factorization, and its operations are modular exponentiations. Assume that the key length and the data size are both n bits, and the time complexity of the encryption/decryption operation using an asymmetric cryptosystem is approximately $O(n^3)$ [3]. The overall time complexity of the Lee et al. scheme is dominated by the asymmetric cryptosystem; therefore, the total time complexity of their scheme is $O(n^3)$. However, the proposed scheme and the Chang et al. scheme mainly use hash functions to perform mutual authentication. The SHA can represent the one-way hash function. Because the process of the SHA consists of exclusive-OR operations and rotation operations, the computation of a hash value using an SHA can be bounded by constant time; that is, the time complexity of a hash function is $O(1)$ [3]. Therefore, the time complexity of our scheme and that of Chang et al. is only $O(1)$.

Regarding the communication cost, to complete the authentication process, the Chang et al. scheme requires two rounds of message exchange between the *MN* and the *FA*, and two rounds of message exchange between the *FA* and the *HA*. Therefore, the total number of communication rounds of the Chang et al. scheme is 4. Because each round requires two transmitted messages, the total number of transmitted messages of the Chang et al. scheme is 8. However, the proposed scheme needs only one round of message exchange between the *MN* and the *FA*, and only one round of message exchange between the *FA* and the *HA*. The total number of communication rounds of the proposed scheme is 2, and the total number of transmitted messages of the proposed scheme is 4. Therefore, the total number of communication rounds in our scheme is reduced to 50% compared with the Chang et al. scheme. The fewer numbers in communication rounds in the authentication process reduce the time required for the verification phase (authentication and session key establishment) and accelerates the whole authentication process. Moreover, the total number of transmitted messages in our scheme is also reduced to 50% compared with the Chang et al scheme. The fewer numbers of transmitted messages result in consuming less transmission power and message overhead. Therefore, in the authentication process, transmission power consumption and message overhead of our scheme can be reduced to approximately 50% compared with the Chang et al. scheme.

Table 4. Functionality comparison of the proposed scheme and related schemes

	Ours	Chang et al. [3]	Lee et al. [5]
Energy consumption	Low	Low	High
User anonymity	Yes	No	No
No verification/password table	Yes	Yes	Yes
Mutual authentication	Yes	Yes	Yes
Session key establishment	Yes	Yes	Yes
Session key disclosure resistance	Yes	No	Yes
Forgery attack resistance	Yes	Yes	No
No synchronized time mechanism	Yes	Yes	No
Freely chosen password	Yes	Yes	No
Insider attack resistance	Yes	No	No
Foreign agent spoofing resistance	Yes	No	Yes

For the comparison on energy consumption, the energy consumption for computing the exclusive-OR operation can be ignored because of its low consumption [3]. As shown in Table 3, in each protocol run, the Lee et al. scheme must compute the $13\mathit{Hash}+5\mathit{Sym}+4\mathit{Asym}$ operation, the Chang et al. scheme must compute the $18\mathit{Hash}$ operation, and the proposed scheme must compute the $20\mathit{Hash}$ operation. Therefore, in mutual authentication, the energy consumption of the Lee et al. scheme is mainly from hash functions, symmetric cryptosystem, and asymmetric cryptosystem. The energy consumption of the proposed scheme and the Chang et al. scheme is mainly from hash functions. The energy consumption from computing the hash function is substantially lower than that of an symmetric cryptosystem or asymmetric cryptosystem [3,21]. A practical example is provided as follows: Using SHA-1 to calculate the hash value, 1 byte of data consumes approximately 0.76 μJ of energy [3,21]. However, to encrypt 1 byte of data, symmetric cryptosystems AES require 9.08 μJ of energy, and asymmetric cryptosystems RSA require 816.63 mJ of energy [3,21]. Therefore, the total energy consumption of the Lee et al. scheme, the Chang et al. scheme, and the proposed scheme is approximately 3266575.28 μJ, 13.68 μJ, and 15.2 μJ, respectively. Therefore, in each protocol run, the total energy consumption of our scheme is reduced to 0.000465% compared with the Lee et al. scheme. Compared with the Chang et al. scheme, the total energy consumption of our scheme only requires extra energy (1.52 μJ) in the computational process of the HA. The energy consumption of the proposed scheme is substantially lower than that of the Lee et al. scheme (Table 4). Low energy consumption extends the battery life of the mobile device [3].

This discussion shows that the proposed scheme is applicable and has superior performance because of the following properties: lower computational cost (0.01 s), less time complexity ($O(1)$), fewer communication rounds (two rounds), fewer transmitted messages (four messages), and less energy consumption (15.2 μJ). Therefore, for practical use, the proposed scheme is an efficient scheme and can enhance the efficiency of the authentication scheme in the GLOMONET or other mobile communication networks.

6.2. **Functionality comparison and effectiveness.** Table 4 shows a comparison of the functionality of the proposed scheme and that of previous related schemes. In the table, *Yes* is used to show when a scheme satisfies a property, whereas *No* is used to indicate the opposite; and *High* is used to show that the scheme requires higher energy consumption, whereas *Low* is used to indicate the opposite. Chang et al. [3] showed that the Lee et al. scheme [5] failed to provide anonymity and is vulnerable to forgery attacks. The Lee et al. scheme suffers from a time-synchronization problem and a freely chosen password problem [3]. Section 3 showed that the Chang et al. scheme does not provide user anonymity and cannot withstand insider attacks [11,12]. Their scheme is vulnerable to the disclosure of session keys and foreign agent spoofing [13-15].

Based on the assumption of the secure one-way hash function [10], we introduce a practical scenario to demonstrate the effectiveness of the proposed scheme, showing that it can provide more functionality and is more secure. Assume that an adversary, *Eve*, is able to intercept any message that is publicly exchanged between two entities and that she can also obtain the smart card of a user. With these capabilities, *Eve* attempts to break the proposed protocol by conducting one of the following attacks: user anonymity attack, insider attack, session key disclosure, foreign agent spoofing, stolen verifier attacks, forgery attack, relay attack, known-key attack, stealing the smart card of a user, or stealing a user password. However, *Eve* as an adversary cannot identify the *MN* who is attempting to login to the system because the login request message $\{SID, U, T, q_1, ID_{HA}, n_{MN}\}$ of an *MN* changes dynamically with every login request (Proposition 5.4). Therefore, the proposed scheme can maintain user anonymity. *Eve* as an insider of the *HA* cannot obtain the PW_{MN} and the private key Kx because the *MN* registers with the *HA* by presenting $h(r \oplus PW_{MN})$ and because the Kx is protected inside the hash function $h(P \parallel h(Kx \parallel ID_{HA}))$ (Proposition 5.7). Therefore, the proposed scheme can resist her insider attacks [9]. *Eve* as an adversary cannot derive the session key *SK* from $SK = h(A \parallel S \parallel ID_{MN} \parallel ID_{FA} \parallel n_{MN} \parallel n_{FA})$ or $SK = M \oplus h(K_{HF} \parallel n_{FA})$ because she cannot obtain A and does not know K_{HF} (Proposition 5.5). Therefore, the proposed scheme can prevent the session key disclosure. In a foreign agent spoofing attack, *Eve* as an adversary cannot send the imitative message $m'_4 = \{q'_2, ID'_{FA}, n'_{FA}\}$ to respond to the *MN* because she cannot obtain A and $q'_2 = h(A \parallel ID'_{FA} \parallel n_{MN})$ (Proposition 5.6); therefore, the proposed scheme can resist her foreign agent spoofing attacks.

Thus far, this scenario has demonstrated that the proposed scheme can overcome the main disadvantages of the Chang et al. scheme (Table 4). In addition, *Eve* as an adversary cannot obtain any verifiable information from the *FA* or the *HA* to threaten the proposed scheme because the *FA* and the *HA* do not maintain a verification table (Proposition 5.7). Therefore, the scheme can resist her stolen verifier attacks [9]. During a forgery attack, *Eve* as an adversary cannot obtain the *imitative* parameters $\{SID', U', T', q'_1\}$ and send an *imitative* login request message $\{SID', U', T', q'_1, ID_{HA}, n'_{MN}\}$ to the *FA* because she cannot obtain A (Proposition 5.2). Therefore, *Eve* cannot impersonate a legal user to access the system, demonstrating that the proposed scheme can resist her forgery attack. In a relay attack, *Eve* as an adversary may replay an intercepted login request message $\{SID, U, T, q_1, ID_{HA}, n_{MN}\}$ to the *FA*. However, after receiving message m_4, *Eve* cannot compute the session key $SK = h(A \parallel S \parallel ID_{MN} \parallel ID_{FA} \parallel n_{MN} \parallel n_{FA})$ because she does not know the A and S in the *SK* (Proposition 5.2); therefore, the proposed scheme can withstand her replay attacks. In a known-key attack, the session keys are independent in each session because nonce n_{MN} and nonce n_{FA} in the session key $SK = h(A \parallel S \parallel ID_{MN} \parallel ID_{FA} \parallel n_{MN} \parallel n_{FA})$ are random and independent in each session [3]. Knowledge of previous session keys cannot be used for *Eve* to derive other session keys (Proposition 5.5). Therefore, the proposed scheme can resist her known-key attack. *Eve* as an adversary may steal the smart card of an *MN* and impersonate the *MN* to log into the system. However, *Eve* cannot obtain the *imitative* parameters $\{SID', U', T', q'_1\}$ and cannot send an *imitative* login request message $\{SID', U', T', q'_1, ID_{HA}, n'_{MN}\}$ to the *FA* because A is unknown (Proposition 5.3). However, even if *Eve* somehow steals only the identification and password of an *MN*, she still cannot compute the *imitative* parameters $\{SID', U', T', q'_1\}$ because A is unknown (Proposition 5.3). *Eve* also cannot impersonate a legal user (MN) to log into the system. Therefore, this scenario shows that the proposed scheme can withstand all malicious attacks from an adversary *Eve*.

Our scheme also provides other principal functions. In the proposed scheme, the *MN* can freely choose a password PW_{MN} without the assistance of the *HA* in the registration phase. When an *MN* roams into a foreign network managed by a registered *FA*, the *FA* can authenticate the *MN* through the *HA* of the *MN*. The *MN* is required to register only once with the *HA* to gain access to registered *FAs* in the GLOMONET. Proposition 5.1 shows that the proposed scheme can provide mutual authentication and negotiate a common session key for secure communication. Therefore, the proposed scheme can satisfy the six crucial design criteria for a secure remote user authentication scheme [22], which are as follows: freely chosen password, single registration, mutual authentication, session key agreement, low computation and communication costs, and no verification table. In addition, the proposed scheme does not have a time-synchronization problem [9] because our scheme is nonce-based and does not use a timestamp for verification. In our system, each FA shares a unique secure key with the HA. It can prevent the system from collapsing in the event that a single private datum is disclosed or a single *FA* is compromised [10]. Therefore, for practical use, the proposed authentication scheme provides more functionality and can enhance effectiveness in protecting the GLOMONET. Even if an adversary in the GLOMONET extracts information transmitted through an insecure channel or stored in a smart card, the proposed scheme remains secure.

We have demonstrated and showed that the proposed authentication scheme is effective and efficient in the GLOMONET. The proposed scheme has more security functionalities and a superior performance compared with the schemes by Chang et al. and Lee et al. A higher security functionality and superior performance are achieved at the cost of only two more hash operations (0.001 s computational time) than the Chang et al. scheme, which are required for the *HA* computational process.

7. Conclusion.

This paper proposes a more secure and effective authentication scheme with anonymity in the GLOMONET. We used the Burrows-Abadi-Needham (BAN) logic method to verify our scheme. We then compared the performance and functionality of the proposed scheme with those of previous related schemes, and demonstrated the efficiency and effectiveness of the proposed scheme by providing realistic examples of potential attacks. The proposed scheme was shown to have superior performance because of its lower computational cost, less time complexity, fewer communication rounds, fewer transmitted messages, and less energy consumption. Cryptanalysis shows that the proposed scheme can overcome the main disadvantages of the Chang et al. scheme, and it satisfies the six crucial design criteria for a secure remote user authentication scheme. The proposed scheme can withstand other possible attacks and provide greater security in functionality. More robust security and superior performance were achieved at the cost of only two more hash operations than the Chang et al. scheme, which are required for the *HA* computational process. The proposed scheme is applicable and suitable for the GLOMONET. In practical use, the proposed scheme can be employed to enhance the effectiveness and efficiency of the authentication scheme in the GLOMONET.

Acknowledgment. The author gratefully acknowledges the helpful comments and suggestions of the reviewers, which have improved the presentation.

REFERENCES

[1] 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, pp.367-374, 2011.

[2] 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, pp.214-222, 2012.

[3] 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, pp.611-618, 2009.

[4] 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.

[5] 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.

[6] 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.

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

[8] M. Burrows, M. Abadi and R. Needham, A logic of authentication, *ACM Transactions on Computer Systems*, vol.8, no.1, pp.18-36, 1990.

[9] Y. P. Liao and S. S. Wang, A secure dynamic ID based remote user authentication scheme for multi-server environment, *Computer Standard & Interfaces*, vol.31, no.1, pp.24-29, 2009.

[10] C.-C. Chang and T.-F. Cheng, A robust and efficient smart card based remote login mechanism for multi-server architecture, *International Journal of Innovative Computing, Information and Control*, vol.7, no.8, pp.4589-4602, 2011.

[11] W. C. Ku and S. M. Chen, Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards, *IEEE Transactions on Consumer Electronics*, vol.50, no.1, pp.204-207, 2004.

[12] W. S. Juang, S. T. Chen and H. T. Liaw, Robust and efficient password-authenticated key agreement using smart cards, *IEEE Transactions on Industrial Electronics*, vol.55, no.6, pp.2551-2556, 2008.

[13] M. Hossain, M. Z. Parvez and M. H. Islam, Mutual authentication between base and subscriber station can improve the security of IEEE 802.16 WiMAX network, *International Journal of Engineering*, vol.5, no.4, pp.292-301, 2011.

[14] D. He and S. Chan, A secure and lightweight user authentication scheme with anonymity for the global mobility network, *The 13th International Conference Network-Based Information Systems*, 2010.

[15] P. Trimintzios and G. Georgiou, WiFi and WiMAX secure deployments, *Journal of Computer Systems, Networks, and Communications*, vol.2010, 2010.

[16] C. C. Lee, T. H. Lin and R. X. Chang, A secure dynamic ID based remote user authentication scheme for multi-server environment using smart cards, *Expert Systems with Applications*, vol.38, no.11, pp.13863-13870, 2011.

[17] P. G. Argyroudis, R. Verma, H. Tewari and D. O'Mahony, Performance analysis of cryptographic protocols on handheld devices, *Proc. of the 3rd IEEE International Symposium on Network Computing and Applications*, Cambridge, USA, pp.169-174, 2004.

[18] M. Passing and F. Dressler, Experimental performance evaluation of cryptographic algorithms, *Proc. of the 3rd IEEE International Conference on Mobile Adhoc and Sensor Systems*, Vancouver, Canada, pp.882-887, 2006.

[19] D. S. Wong, H. H. Fuentes and A. H. Chan, The performance measurement of cryptographic primitives on palm devices, *Proc. of the 17th Annual Computer Security Applications Conference*, New Orleans, USA, pp.92-101, 2001.

[20] S. P. Yang and X. Li, Defect in protocol analysis with BAN logic on man-in-the-middle attacks, *Application Research of Computers*, vol.24, no.3, pp.149-151, 2007.

[21] N. R. Potlapally, S. Ravi, A. Raghunathan and N. K. Jha, A study of the energy consumption characteristics of cryptographic algorithms and security protocols, *IEEE Transactions on Mobile Computing*, vol.5, no.2, pp.128-143, 2006.

[22] W. S. Juang, Efficient multi-server password authenticated key agreement using smart cards, *IEEE Transactions on Consumer Electronics*, vol.50, no.1, pp.251-255, 2004.

[23] M. L. Das, A. Saxena and V. P. Gulati, A dynamic ID-based remote user authentication scheme, *IEEE Transactions on Consumer Electronics*, vol.50, no.2, pp.629-631, 2004.

[24] T. S. Messergers, E. A. Dabbish and R. H. Sloan, Examining smart card security under the threat of power analysis attacks, *IEEE Transactions on Computers*, vol.51, no.5, pp.541-552, 2002.

[25] H. C. Hsiang and W. K. Shih, Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment, *Computer Standard & Interfaces*, vol.31, no.6, pp.1118-1123, 2009.

[26] J. S. Lee and C. C. Chang, Secure communications for cluster-based ad hoc networks using node identities, *Journal of Network and Computer Applications*, vol.30, no.4, pp.1377-1396, 2007.

[27] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd Edition, John Wiley & Sons, New York, USA, 1996.

[28] Y. F. Chang, C. C. Chang and Y. L. Liu, Password authentication without the server public key, *IEICE Transactions on Communications*, vol.E87-B, no.10, pp.3088-3091, 2004.

[29] R.-C. Wang, W.-S. Juang and C.-L. Lei, A robust authentication scheme with user anonymity for wireless environments, *International Journal of Innovative Computing, Information and Control*, vol.5, no.4, pp.1069-1080, 2009.