Review

Revisiting three anonymous two-factor authentication schemes for roaming service in global mobility networks

Shuming Qiu¹, Ding Wang²,³

¹School of Mathematics and Statistics, Jiangxi Normal University, Nanchang 330022, China.
²College of Cyber Science, Nankai University, Tianjin 300350, China.
³Tianjin Key Laboratory of Network and Data Security Technology, Nankai University, Tianjin 300350, China.

Correspondence to: Prof. Ding Wang, College of Cyber Science, Nankai University, Tianjin 300350, China; and Tianjin Key Laboratory of Network and Data Security Technology, Nankai University, Tianjin 300350, China.
E-mail: wangding@nankai.edu.cn; wangding@pku.edu.cn.

How to cite this article: Qiu SM, Wang D. Revisiting three anonymous two-factor authentication schemes for roaming service in global mobility networks. J Surveill Secur Saf 2021;2:66-82. http://dx.doi.org/10.20517/jsss.2020.28.

Abstract

Designing a secure and efficient anonymous authentication protocol for roaming services in global mobile networks is a hot topic in the field of information security protocols. Based on the widely accepted attacker model, this paper analyzes the security of three representative anonymous authentication protocols in global mobile networks. It is pointed out that: (1) Xu et al.’s protocol cannot resist the claimed offline password guessing attack and mobile user impersonation attack, and do not achieve mobile user untraceability and forward security; (2) Gupta et al.’s protocol cannot resist offline password guessing attacks, and temporary information disclosure attacks; (3) Madhusudhan et al.’s protocol cannot resist mobile user impersonation attack, foreign agent impersonation attack, replay attack, offline password guessing attack and session key disclosure attack, and cannot realize the anonymity and untraceability and forward security of users. It is emphasized that the fundamental reason for the failure of these protocols lies in the violation of the four basic principles of protocol design: Public key principle, Forward security principle, User anonymity principle and Anti offline guessing attack principle. The specific mistakes of these schemes are clarified, and the corresponding correction methods are proposed.

Keywords: Global mobility networks, authentication and key agreement, perfect forward secrecy, anonymity and untraceability, offline password guessing attack

© The Author(s) 2020. Open Access This article is licensed under a Creative Commons Attribution 4.0 International License (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, sharing, adaptation, distribution and reproduction in any medium or format, for any purpose, even commercially, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.
1 INTRODUCTION

With the rapid growth of Internet application demand, the Global Mobility Network (GLOMONET) gradually shows a wide range of application prospects in various fields closely related to people's lives. This kind of network makes it easy for people to enjoy the convenience of mobile network. In the GLOMONET, when a travel mobile user with wireless device wants to get network service, she can pass the authentication of global mobile network with the help of home agent (HA) and be allowed to use the roaming service of foreign agent (FA) anywhere. Due to the openness and mobility of mobile networks and the limited resources of mobile devices, communication is vulnerable to various attacks, such as offline guessing attacks and failure to provide forward security. According to O'Dea\cite{1}, the forecast number of mobile users worldwide in 2024 will be 7.41 billion, 6.6% more than the 6.95 billion users in 2020. In other words, everyone in the world has at least one mobile device on average. The huge personal data of users is in urgent need of privacy protection. In the Internet of things, access control and authentication technology has been effectively studied\cite{2–7}. Nevertheless, how to ensure the authenticity of communication entities, prevent the abuse of services and illegal access to resources, without reducing system availability, remains a serious challenge to the GLOMONET.

1.1 Related work

In 1997, Suzuki and Nakada\cite{8} proposed an authentication technique for GLOMONET. The proposed authentication technique which only consists of two phases: registration phase and authentication phase, is suitable for the distributed security management of GLOMONET. Since then, a large number of authentication and key agreement protocols have been proposed for GLOMONET. In 2005, Lee et al.\cite{9} proposed an authentication scheme without password. In the proposed scheme, the home network cannot obtain the authentication key between the roaming user and the visited network. In 2006, Lee et al.\cite{10} proposed an enhanced scheme for eliminating the security weaknesses of Zhu and Ma's scheme\cite{11}. However, in 2009, Chang et al.\cite{12} pointed out Lee et al.'s scheme suffers from the impersonation attack. Afterwards, Chang et al.\cite{12} proposed an authentication scheme for roaming service that only used one-way hash functions and exclusive-OR operations in order to obtain security goals.

In 2010, Wu et al.\cite{13} proposed a novel lightweight authentication scheme used one-way hash functions and symmetric cryptographic operations in GLOMONET for roaming service to provide user anonymity. In 2011, Zhou and Xu\cite{14} also proposed a provable secure two-factor authentication protocol with anonymity for roaming service based on Diffie-Hellman assumption. In 2013, to overcome two kinds of impersonation attacks, He et al.\cite{15} proposed anonymous two-factor authentication protocol for Consumer Roaming Service. However, He et al.'s scheme\cite{15} is vulnerable to time synchronization attack.

In 2013, Jiang et al. showed that He et al.'s scheme\cite{16} cannot achieve two-factor security, and it suffers from multiple known attacks. In order to improve security, Jiang et al.\cite{17} proposed a scheme which based on quadratic residue assumption for GLOMONET. But it can be observed that Jiang et al.'s scheme\cite{17} suffers denial of service attack. Moreover, Wen et al.\cite{18} showed that Jiang et al.'s scheme\cite{17} is vulnerable to replay attack and the stolen-verifier attack.

In 2017, Lee et al.\cite{19} showed that Mun et al.'s scheme\cite{20} is insecure against impersonation attack and man-in-the-middle attack, and it cannot achieve anonymity. Subsequently, Lee et al.\cite{19} only used one-way hash function and exclusive-OR operation to propose an improved scheme for GLOMONET.

In 2018, Xu et al.\cite{21} showed that Gope-Hwang's scheme\cite{22} cannot resist replay attack and synchronous attack. Afterwards, they proposed an authentication and key agreement protocol for GLOMONET used only hash functions and symmetric cryptosystem. While Gupta et al.\cite{23} showed that Wu et al.'s scheme\cite{24} cannot provide untraceability of the mobile user. What's more, it's inefficiency for the verification of the wrong password. Because there are many attacks in the existing protocols, in order to eliminate these problems,
Madhusudhan and Shashidhara\cite{25} proposed a secure authentication and key agreement scheme for mobile roaming users in 2019.

Combining with a large number of related literatures, we can observe that such authentication protocols in GLOMONET can be divided into three categories based on the different basic cryptography techniques used: (1) based on hash function and exclusive-OR operation; (2) based on hash function, exclusive-OR operation and symmetric cryptography; (3) based on public key cryptography. The authentication protocols of (1) and (2) always have some security problems, such as offline password attack and perfect forward secrecy. However, when the public key cryptography is not used properly, the authentication protocols of (3) are also vulnerable to various attacks.

1.2 Contribution
We provide a better understanding of user anonymous and untraceability, offline password guessing attack and perfect forward secrecy, etc, and we believe it would facilitate the design of secure and usability authentication and key agreement schemes for GLOMONET. Specifically, a summary of our contributions are as follows:

a) We analyze Xu et al.\cite{21}, Gupta et al.\cite{23} and Madhusudhan et al.\cite{25} protocols, and find that none of the three anonymous authentication protocols in GLOMONET environment can achieve the user anonymity and untraceability, and they are vulnerable to offline password guessing attacks, and there are forward secrecy issues and mobile user impersonation attack, etc.

b) We highlight four basic design principles of anonymous two-factor authentication protocol in GLOMONET: (1) Public key technology principle. Under the assumption of non tamper resistant smart card, using public key technology is a necessary condition to resist offline password guessing attack; (2) Perfect forward secrecy principle. Public key technology is a necessary condition for preserving perfect forward secrecy; (3) Mobile users anonymity and untraceability principle. Using public key technology is a necessary condition for realizing user anonymity and untraceability; (4) Anti offline password guessing principle. At present, using "Fuzzy-Verifiers" and "Honeywords" technology is a good choice for realizing anti offline password guessing attack\cite{26}.

1.3 Roadmap of this paper
The remainder of this paper is as follows: Section 2 describes the system model and attacker model. Section 3 reviews the efficient anonymous authentication scheme proposed by Xu et al. And the security of the scheme is analyzed in Section 4. Section 5 describes the two-factor authentication scheme based on quadratic residue hypothesis proposed by Gupta et al. And Section 6 points out the security problems of the scheme. Section 7 and Section 8 respectively review and analyze the scheme of Madhusudhan et al. Section 9 highlights four basic design principles of two-factor authentication scheme in GLOMONET. Finally, Section 10 summarizes the conclusion.

2 SYSTEM MODEL AND ATTACKER MODEL
This section introduces the system model of authentication and key agreement in GLOMONET and attacker model. The notations used in this paper are presented in Table 1.

2.1 System model
In a two-factor authentication and key exchange protocol for roaming service in GLOMONET, there exist there participants namely the mobile user (MU), the FA and the HA. First of all, MU needs to register themselves with HA before she wants to get mobile network roaming service. In the registration phase, MU sends the registration request to HA, and sends the identity or password information after privacy processing to HA on the secure channel. Then, HA stores some key parameters processed by cryptography in a new smart card and sends the smart card to the corresponding MU. Then, in order to obtain the access rights of FA, MU
needs the assistance of HA. The specific process is as follows: (1) MU sends roaming service login request to FA; (2) FA sends authentication request to HA; (3) HA sends response to FA after authenticating FA; (4) FA sends response to user after authenticating HA; (5) After MU authenticates FA, the session key is calculated. Therefore, mobile users can use the session key to enjoy roaming service safely.

### 2.2 Attacker model

Many scholars\cite{26-43} have studied the attacker model of password authentication protocol, among which the Dolev-Yao model\cite{31} is the most classic. Due to the openness of the network, side channel attacks have developed rapidly in recent years (such as timing attacks, electromagnetic attacks and energy consumption attacks). Side-channel attack means that the attacker has strong ability and can extract security parameters stored in smart devices (e.g., smart cards). When analyzing the authentication protocol in GLOMONET, this paper will adopt a new attack model which combines multiple attack models, such as those presented in reported works\cite{26,27,32-47}. Finally, the capacities of the adversary for two-factor authentication schemes in GLOMONET are summarized as follows.

1) All parameters stored in the smart card of the mobile users can be extracted using side channel attack by the adversary A.
2) A can eavesdrop, delete, intercept, replay, modify and block all message in the open channel.
3) A can offline enumerate all pairs of \((PW_{MU}, ID_{MU})\) from \((D_{PW}, D_{ID})\) within polynomial time, where \(D_{ID}\) refers to the space of identities and \(D_{PW}\) refers to the space of passwords. In fact, according to the reported work\cite{37,38} the space of identities and passwords is very limited in real life, \(|D_{ID}| \leq |D_{PW}| \leq 10^6\).
4) Any adversary A can register as a legitimate mobile user if anyone can do this.
5) A may can obtain previous session keys by improper erasure (e.g. using digital forensic techniques).
6) A can obtain the private key of the mobile user, the home agent and the foreign agent when carrying out the perfect forward secrecy attack.

### 3 Xu et al.’s Scheme

In 2018, Xu et al.\cite{21} pointed out that Gopa and Hwang’s scheme\cite{22} is vulnerable to replay attack and has the problem of computational burden. Afterwards, Xu et al.\cite{21} designed an improved authentication scheme for roaming service in GLOMONET. However, here we show that Xu et al.’s scheme\cite{21} still has several serious defects, including lack of mobile user untraceability and perfect forward secrecy, offline password guessing attack, and mobile user impersonation attack.

#### 3.1 Registration phase

S1. A new mobile user MU sends her real identity \(ID_{MU}\) to the home agent HA through the secure channel.
S2. On receiving the \(ID_{MU}\), HA generates two random numbers \(n_h\) and \(n_0\) and then calculates \(K_{uh} = h(ID_{MU}||n_h)\) and \(EID = E_k(ID_{MU}||n_0)\), where \(K_{uh}\) is a shared key between MU and HA and \(k\) is a secret key of HA. Afterwards, HA stores \(ID_{MU}, K_{uh}\) and sends the message \(\{EID, K_{uh}, h(\cdot)\}\) to MU via the secure channel.
S3. MU chooses a password \(PW_{MU}\) and calculates \(EID^* = EID@s(h(ID_{MU}||PW_{MU}))\), \(K_{uh}^* = K_{uh}@h(ID_{MU}||PW_{MU})\). Finally, MU replaces \(EID, K_{uh}\) with \(EID^*, K_{uh}^*\), respectively. And the smart card SC contains these param-
We suppose that MU generates a random number $N_m$ and inputs her identity $ID_{MU}$ and password $PW_{MU}$ into the smart card SC. Then, SC computes $K_{uh} = K_{uh}^* \oplus h(ID_{MU}||PW_{MU})$, $EID = EID^* \oplus h(ID_{MU}||PW_{MU})$, $N_x = h(ID_{MU}||K_{uh}) \oplus N_m$ and $V_1 = h(EID)||N_x||T_1||ID_{MU}||K_{uh}$. Finally, MU sends the message $M_{A1} : \{EID, N_x, ID_h, V_1, T_1\}$ to FA, where $T_1$ is a Time-stamp.

S2. After receiving $M_{A1}$, FA first checks the validity of $T_1$. If not, FA terminates this session immediately. Otherwise, FA generates a random number $N_f$ and calculates $N_f = h(K_{fh}) \oplus N_f$, $V_2 = h(EID)||N_f||T_2||K_{fh}||N_f)$. Finally, FA sends the message $M_{A2} : \{EID, N_f, ID_f, V_1, T_1, N_f, V_2\}$ to HA, where $T_2$ is a Time-stamp.

3.2 Authentication and key agreement phase

In this part, with the help of the home agent HA, the mobile user MU and the foreign agent FA will authenticate each other and establish a common session key.

S1. MU generates a random number $N_m$ and inputs her identity $ID_{MU}$ and password $PW_{MU}$ into the smart card SC. Then, SC computes $K_{uh} = K_{uh}^* \oplus h(ID_{MU}||PW_{MU})$, $EID = EID^* \oplus h(ID_{MU}||PW_{MU})$, $N_x = h(ID_{MU}||K_{uh}) \oplus N_m$ and $V_1 = h(EID)||N_x||T_1||ID_{MU}||K_{uh}$. Finally, MU sends the message $M_{A1} : \{EID, N_x, ID_h, V_1, T_1\}$ to FA, where $T_1$ is a Time-stamp.

S2. After receiving $M_{A1}$, FA first checks the validity of $T_1$. If not, FA terminates this session immediately. Otherwise, FA generates a random number $N_f$ and calculates $N_f = h(K_{fh}) \oplus N_f$, $V_2 = h(EID)||N_f||T_2||K_{fh}||N_f)$. Finally, FA sends the message $M_{A2} : \{EID, N_f, ID_f, V_1, T_1, N_f, V_2\}$ to HA, where $T_2$ is a Time-stamp.

S3. On receiving the $M_{A2}$, HA checks the validity of $T_2$ time. If not, HA end the session immediately. Otherwise, HA figures out $N_f = h(K_{fh}) \oplus N_f$, $V_2 = h(EID)||N_x||T_2||K_{fh}||N_f)$. And it further verifies whether $V_2^* = V_2$. If it is not equal, it end this session. Otherwise, then HA decrypts $EID$ through $ID_{MU}||n_0 = D_k(EID)$ and obtains MU’s real identity $ID_{MU}$ and the random number $n_0$. Afterwards, it calculates $V_2^* = h(EID)||N_x||T_2||ID_{MU}||K_{uh}$ and verifies whether $V_2^*$ is equal to $V_2$. If not, it ends this session. If so, HA generates a random number $n_1$ and computes $D = E_k(ID_{MU}||n_1)$ and the new pseudo identity $FID^* = FID \oplus h(ID_{MU}||K_{uh})$. Afterwards, HA calculates $N_m = h(ID_{MU}||K_{uh}) \oplus N_x$, $N_r = h(K_{uh}||ID_{MU}||N_m) \oplus N_f \oplus n_0$, $n_r = h(K_{fh}||ID_{f}||N_f) \oplus N_m \oplus n_0$, $V_3 = h(N_r||N_f) \oplus K_{fh}$ and $V_4 = h(N_r||FID^*||N_m) \oplus K_{uh}$. Lastly, HA sends the response $M_{A3} : \{N_r, N_r^*, V_3, V_4, FID^*\}$ to FA.

S4. Upon receiving the $M_{A3}$, FA figures out $V_2^* = h(N_r||N_f) \oplus K_{fh}$ and verifies whether it is equal to $V_2$. If so, it calculates $N_m \oplus n_0 = h(K_{fh}||ID_{f}||N_f) \oplus N_r$ and the session key $SK = N_m \oplus n_0 \oplus N_f$. Finally, FA sends the message $M_{A4} : \{N_r, N_r^*, V_3, V_4, FID^*\}$ to MU.

S5. Upon receiving the $M_{A4}$, MU computes $V_2^* = h(N_r||FID^*||N_m) \oplus K_{uh}$ and checks whether it is equal to $V_4$. If so, she computes $N_f \oplus n_0 = h(K_{uh}||ID_{MU}||N_m) \oplus N_r^*$ and the session key $SK = N_m \oplus n_0 \oplus N_f$. Afterwards, MU computes $FID = FID^* \oplus h(ID_{MU}||K_{uh})$ and replaces $EID$ with $FID$.

3.3 Password update phase

The mobile user MU can change her password by itself. In order to change the password, MU needs to use her old password $PW_M$ and enters the new password $PW_M^*$. After that, she calculates $K_{uh} = K_{uh}^* \oplus h(ID_{MU}||PW_M)$, $EID = EID^* \oplus h(ID_{MU}||PW_M)$, $K_{uh}^* = K_{uh} \oplus h(ID_{MU}||PW_M^*)$ and $EID^{**} = EID \oplus h(ID_{MU}||PW_M^*)$. Lastly, MU replaces $\{K_{uh}^*, EID^*\}$ with $\{K_{uh}^{**}, EID^{**}\}$ in the smart card, respectively.

4 CRYPTANALYSIS OF XU ET AL.’S SCHEME

4.1 Lack of mobile user untraceability

We suppose that $A$ gets the message $\{EID, N_s, ID_h, V_1, T_1\}$. Since $EID = E_k(ID_{MU}||n_0)$ is a fixed value, $A$ can track the login request behavior of legitimate mobile user $ID_{MU}$. Therefore, Xu et al.’s scheme cannot provide mobile user untraceability.

4.2 Offline password guessing attack: Case I (via special parameter in smart card)

Suppose that the adversary $A$ extracts these parameters $\{EID^*, h()\}$ and gets the message $\{EID, N_s, ID_h, V_1, T_1\}$. The adversary $A$ can guess the user password offline. The specific process is as follows:

1. $A$ first selects $PW^*$ from the password dictionary space $D_{PW}$ and selects $ID^*$ from the identity dictionary space $D_{ID}$.
2. $A$ computes $\delta = EID^* \oplus EID^* = h(ID_{MU}||PW_{MU})$.
3. $A$ computes $\delta^* = h(ID^*||PW^*)$.
4. $A$ checks whether $\delta^*$ is equal to $\delta$. 
If equal, $\mathcal{A}$ finds the correct password and identity of MU. Otherwise, $\mathcal{A}$ repeat steps 1)-4) until she finds the correct password and identity.

The time complexity of the above attack is: $O(|\mathcal{D}_{PW}| \times |\mathcal{D}_{ID}| \times T_h)$, where $|\mathcal{D}_{PW}|$ and $|\mathcal{D}_{ID}|$ denote the number of passwords in $\mathcal{D}_{PW}$ and the number of identity in $\mathcal{D}_{ID}$. $T_h$ is the running time of hash computation. Usually $|\mathcal{D}_{ID}| \leq |\mathcal{D}_{PW}| \leq 10^6$\cite{32,37}, therefore, the above attack is very efficient. In fact, why the above attack is successful is that, $\mathcal{A}$ can obtain the parameter $EID^*$ in smart card and $EID$ in public channel, and directly figures out the exact parameter $h(ID_{MU}||PW_{MU})$ directly. Finally, $\mathcal{A}$ just needs to traverse the space of passwords and identities.

4.3 Offline password guessing attack: Case II (via special parameter in smart card)

Suppose that the adversary $\mathcal{A}$ extracts these parameters $\{EID^*, K_{ah}^*, h()\}$ and gets the message $\{EID, N_s, ID_n, V_1, T_1\}$. The adversary $\mathcal{A}$ can guess the user password offline. The specific process is as follows:

1) $\mathcal{A}$ first selects $PW^*$ from the password dictionary space $\mathcal{D}_{PW}$ and selects $ID^*$ from the identity dictionary space $\mathcal{D}_{ID}$.
2) $\mathcal{A}$ computes $K_{ah} = (K_{ah}^* \oplus h(ID_{MU}||PW_{MU})) \oplus ((EID^* \oplus h(ID_{MU}||PW_{MU})) \oplus EID) = K_{ah}^* \oplus EID^* \oplus EID$.
3) $\mathcal{A}$ computes $K_{ah}' = K_{ah} \oplus h(ID^*||PW^*)$.
4) $\mathcal{A}$ checks if $K_{ah}'$ is equal to $K_{ah}$.

If equal, $\mathcal{A}$ finds the correct password and identity of MU. Otherwise, $\mathcal{A}$ can repeat steps 1)-4) until the equation holds.

The time complexity is: $O(|\mathcal{D}_{PW}| \times |\mathcal{D}_{ID}| \times T_h)$, therefore, the above attack is efficient.

4.4 Offline password guessing attack: Case III (via verification value in public channel)

Suppose that the adversary $\mathcal{A}$ extracts these parameters $\{EID^*, K_{ah}^*, h()\}$ and gets the message $\{EID, N_s, ID_n, V_1, T_1\}$. The adversary $\mathcal{A}$ can guess the user password offline. The specific process is as follows:

1) $\mathcal{A}$ first selects $PW^*$ from the password dictionary space $\mathcal{D}_{PW}$ and selects $ID^*$ from the identity dictionary space $\mathcal{D}_{ID}$.
2) $\mathcal{A}$ computes $V_1 = h(EID||N_s||T_1||ID^*||K_{ah}^*)$.
3) $\mathcal{A}$ checks if $V_1$ is equal to $V_1$.

If equal, $\mathcal{A}$ finds the correct password and identity of MU. Otherwise, $\mathcal{A}$ can repeat steps 1)-4) until the equation holds. The time complexity of the above attack is: $O(|\mathcal{D}_{PW}| \times |\mathcal{D}_{ID}| \times 2T_h)$, therefore, the above attack is also very efficient.

4.5 No perfect forward secrecy

In Xu et al.’s scheme\cite{21}, $\mathcal{A}$ can obtain the established session key between the mobile user MU and the foreign agent FA if $\mathcal{A}$ gets the private key $k$ of HA.

1) $\mathcal{A}$ eavesdrops the message $\{EID, N_s, N_s^*\}$ in public channel and extracts the parameter $\{EID^*, K_{ah}^*, h()\}$ in smart card.
2) $\mathcal{A}$ decrypts $EID$ using the long term private key $k$ of HA, that is, $D_k(EID) = ID_{MU}||n_0$.
3) $\mathcal{A}$ computes $K_{ah} = (K_{nh}^* \oplus h(ID_{MU}||PW_{MU})) \oplus ((EID^* \oplus h(ID_{MU}||PW_{MU})) \oplus EID) = K_{ah}^* \oplus EID^* \oplus EID$.
4) $\mathcal{A}$ computes $N_m = h(ID_{MU}||K_{ah}) \oplus N_s$.
5) $\mathcal{A}$ computes $N_f \oplus n_0 = h(K_{ah}||ID_{MU}||N_m) \oplus N_s^*$.
6) Finally, $\mathcal{A}$ successfully calculates the session key $SK = N_m \oplus n_0 \oplus N_f$. The adversary $\mathcal{A}$ can successfully obtain $SK$. The above attack is also very efficient.
4.6 Mobile user impersonation attack
According to Section 2), the adversary $A$ can figure out the shared key $K_{uh}$ between MU and HA. Thus, if $A$ obtains the identity $ID_{MU}$ of the mobile user MU by using of offline guessing attack, she becomes capable to impersonate MU. To do so, $A$ captures the login request message $\{EID, N_s, ID_h, T_1\}$ in public channel and extracts the parameter $\{EID^*, K_{uh}^*, h()\}$ in smart card. Afterwards, $A$ performs the following steps.

1. $A$ computes $K_{uh} = (K_{uh}^* + h(ID_{MU} || PW_{MU})) + ((EID^* \oplus h(ID_{MU} || PW_{MU})) \oplus EID) = K_{uh}^* \oplus EID^* \oplus EID$.
2. $A$ chooses a random number $N_s^*$, and then calculates $N_s^* = h(ID_{MU} || K_{uh}) \oplus N_s$.
3. $A$ computes $V_s^* = h(EID) || N_s^* || T_1^*$, where $T_1^*$ is the current Time-stamp.
4. The adversary $A$ sends the forged message $M_{A1}^* = \{EID, N_s^*, ID_h, V_s^*, T_1^*\}$ to FA.

Since FA only checks the validity of $T_1^*$, the forged message $M_{A1}^*$ is easy to pass the authentication of FA. On the other hand, since the forged message $M_{A1}^* = \{EID, N_s^*, ID_h, V_s^*, T_1^*\}$ is indistinguishable from the real $M_{A1}$, MU also can pass the authentication of HA. Therefore, Xu et al.’s scheme [21] cannot resist mobile user impersonation attack.

5 GUPTA ET AL.’S SCHEME
Gupta et al.’s scheme [22] uses public key encryption based on quadratic residue assumption. Quadratic residue assumption is described as follows: Assume $p, q$ are large primes, $n = pq$, and $x$ and $n$ is given. It’s hard to get $y$ from the equation $x = y^2 \mod n$. However, if the factors of $n$ i.e. $p$ and $q$ are known, Chinese remainder theorem can solve this problem. More detailed description can be found in Jiang et al.’s scheme [17].

Moreover, in order to solve the problems of efficient typo detection, DoS attack and password guessing attack, the proposed scheme uses the “Fuzzy-Verifier” technique [26]. And Gupta et al.’s scheme [23] has four phases. However, registration phase and mutual authentication phase are needed in this paper. The detailed descriptions of the two phases are as follows.

5.1 Registration phase
S1. A mobile user MU selects a random number $b$ and a new password $PW_{MU}$. MU computes $HPW_{MU} = h(PW_{MU} || b)$. Afterwards, MU sends $ID_{MU}$ and $HPW_{MU}$ to HA through a secure channel.
S2. Upon getting $ID_{MU}, HPW_{MU}$ from MU at the time $T_{rg}$, HA computes $B_1 = h((h(ID_{MU}) \oplus h(HPW_{MU})) \mod n_0)$, where $n_0$ is an integer and $2^4 \leq n_0 \leq 2^8$, then it checks whether $ID_{MU}$ is in User_List or not. If not, HA generates a new entry for $ID_{MU}$ as $ID_{MU}, l_i, T_{rg}, Honey_List$, where $l_i$ is a unique random number corresponding to MU, Honey_List to record the number of login failure and initialized to 0. Otherwise, HA updates $T_{rg}$ and $l_i$ in the User_List. HA computes $K_i = h(ID_{MU} || l_i || T_{rg}), C_i = K_i \oplus HPW_{MU}$. After that, HA stores $\{B_1, C_i, n_0, l_i, h(\cdot), n\}$ in the smart card.$n$ is a public key of the home server which used for the encryption by the mobile users. Then HA sends it to MU. On receiving the smart card, MU enters $b$ into the smart card.

5.2 Mutual authentication phase
In this phase, the mobile user MU can get access of the foreign server by performing authentication and key agreement. Assuming $z$ is prime, $E$ is an Elliptic curve over the field $GF(z)$ where $E$ has large embedding degree, and $P$ is a base point in Elliptic curve.
S1. MU inserts the smart card into a card reader and inputs $ID_{MU}$ and $PW_{MU}$.
S2. The smart card figures out $HPW_{MU} = h(PW_{MU} || b), B_1 = h((h(ID_{MU}) \oplus h(HPW_{MU})) \mod n_0)$ and verifies if the computed $B_1$ is equal to the stored $B_1$. If the computed $B_1 \neq$ stored $B_1$, blocks the session. Otherwise, the smart card calculates $K_i = C_i \oplus HPW_{MU}$ and $M_1 = (ID_{MU}, ID_{FA}, ID_{HA}, K_i, T_1, rP)^2 \mod n$, where $ID_{FA}, ID_{HA}$ are the identities of the foreign agent and home agent respectively, $T_1$ is the timestamp
at which the message $M_1$ is sent, $r$ is a random number generated by the mobile user. Afterwards, MU sends the $M_1$ to the foreign agent FA.

S3. On receiving $M_1$, FA chooses a random number $s$ and calculates $M_2 = (M_1||T_2||sP)$. $T_2$ is the timestamp when the message $M_2$ is generated. Subsequently, FA uses ECDSM and private key $S_K$, on the message $M_2$ to generate digital signature $\sigma_r$. Then FA publishes its public key $PK_v$ to all the servers periodically, which is corresponding to the private key $S_K$ and certified by the certificate authority CA. In the end, FA sends the home agent HA the message $M_2$ and signature $\sigma_r$.

S4. On receiving $M_2$ and $\sigma_r$, HA verifies the timestamp $T_2$. If the timestamp $T_2$ is not valid, HA ends this session. Otherwise, HA checks the signature $\sigma_r$ using the public key of FA. If the verification is not successful, HA sends the failure notice to FA. If so, HA using the private key $p, q$ decrypts $M_1$ where $n = p \times q$. Then HA obtains $ID_{MU}, ID_{FA}, ID_{HA}, K_i, T_3, rP$. Afterwards, HA verifies them. HA refuses this session if anyone is not valid. Otherwise, HA searches whether $ID_{MU}$ is in the $User\_List$ or not. If not, HA rejects the authentication request and sets $Honey\_List$ to $Honey\_List + 1$. In case the value of $Honey\_List$ crosses the preset threshold value (e.g., 10), HA suspends the card till MU does not re-register. If the $ID_{MU}$ is in the $User\_List$, HA obtains $l_i$ and $T_3$ from the $User\_List$ and compute $K_i = h(ID_{MU}||l_i||T_3)$. Subsequently, HA verifies whether the computed $K_i$ equal with the received $K_i$. If the verification is valid, MU is successfully authenticated. Otherwise, HA sends FA the authentication failure notice. When authentication is successful, HA figures out $M_3 = rP||T_3, M_4 = sP||T_3, \sigma_H = Sign(M_3, SK_H)$ and $M_5 = h(K_i||sP||T_3)$ where $\sigma_H$ is digital signature generated using ECDSM. $T_3$ is the timestamp when $M_3$ and $M_4$ are sent. Sign is ECDSM signature generation algorithm, $SK_H$ is the private key of HA for ECDSM signature generation. HA publishes the public key $PK_H$ to all the servers which is corresponding to $SK_H$ and certified by the certificate authority CA. HA sends $(M_3, M_4, M_5, \sigma_H)$ to FA.

S5. On receiving $(M_3, M_4, M_5, \sigma_H)$, FA checks first $T_3$. If $T_3$ is not valid, FA discards the message. Otherwise, FA uses the public key $PK_H$ to check the $\sigma_H$. If it is fails, FA discards the message. Otherwise, FA sets $SK = srP$ and sends $(M_4, M_5)$ to MU.

S6. On receiving $(M_4, M_5)$ from FA, MU checks the timestamp $T_3$. If $T_3$ is not valid, MU discards the message $(M_4, M_5)$. Otherwise, MU computes $K_i = C_i \oplus Hpw_{MU}$ and $M'_5 = h(K_i||sP||T_3)$. Finally, MU checks $M'_5 = M_5$. If they are equal, MU figures out the session key $SK = rsP$. Otherwise, MU terminates this session.

6 CRYPTANALYSIS OF GUPTA ET AL.’S SCHEME

Here, we show that Gupta et al.’s scheme\cite{23} still has two serious flaws, namely, offline password guessing attack and session-specific temporary information attack.

6.1 Offline password guessing attack: Case I

Suppose that the adversary $A$ extracts these parameters $\{C_i, b\}$ from the smart card, gets the message $\{M_1, M_3\}$ and the public key $n$ of HA. The adversary $A$ can guess the user password offline. The specific process is as follows:

1) $A$ first selects $PW^*$ and three identities $\{ID^*_{MU}, ID^*_{FA}, ID^*_{HA}\}$ from the password dictionary space $D_{PW}$ and three identity dictionary space $D_{ID}$, respectively. Moreover, $A$ chooses a timestamp $T_1$ from the appropriate time interval $\Delta T$.

2) $A$ calculates $HPw_{MU}^* = h(PW_{MU}^*||b)$.

3) $A$ computes $K_i^* = C_i \oplus HPw_{MU}^*$.

4) Since $M_4 = rP||T_3, A$ can compute $M'_5 = (ID^*_{MU}, ID^*_{FA}, ID^*_{HA}, K_i^*, T_3, rP)^2 \mod n$.

5) $A$ verifies whether $M'_5$ is equal to $M_1$.

If it is equal, $A$ finds out the correct password and identity of MU. Otherwise, $A$ repeats steps 1)-5) until the equation holds.
The time complexity of the above attack is: \( O(|D_{PW}| * 3|D_{ID}| * \Delta T * T_h) \), therefore, the above attack is efficient.

### 6.2 Offline password guessing attack: Case II

Suppose that the adversary \( A \) extracts these parameters \( \{C_i, b\} \), gets the message \( \{M_4, M_5\} \). The adversary \( A \) can guess the user password offline. The specific process is as follows:

1. \( A \) first selects \( PW' \) from the password dictionary space \( D_{PW} \) and selects three identities \( \{ID^*_{MU}\} \) from three identity dictionary space \( D_{ID} \).
2. \( A \) calculates \( HPW^*_{MU} = h(PW^*_{MU}||b) \).
3. \( A \) computes \( K_i^* = C_i \oplus HPW^*_{MU} \).
4. Since \( M_4 = sP||T_3 \), \( A \) can compute \( M^*_4 = h(K_i^*||sP||T_3) \).
5. \( A \) verifies whether \( M^*_4 \) is equal to \( M_5 \).

If they are equal, \( A \) gets the correct password and identity of MU. Otherwise, \( A \) can repeat steps 1)-5) until the equation holds.

The time complexity of the above attack is: \( O(|D_{PW}| * |D_{ID}| * 2T_h) \), therefore, the above attack is very efficient.

### 6.3 Session-specific temporary information attack

In Gupta et al.'s scheme\[^{[23]}\] if all temporary information \( s, r \) are compromised, then \( A \) can compute \( SK = srP \). Therefore, in the case of temporary information disclosure, Gupta et al.'s scheme\[^{[23]}\] is vulnerable to session-specific temporary information attack.

### 7 MADHUSUDHAN ET AL.'S SCHEME

In 2019, Madhusudhan et al.\[^{[25]}\] only used hash function and symmetric password to construct an authentication scheme\[^{[25]}\] in GLOMONET, and they claimed this scheme to be able to resist various attacks and provide user anonymity. But here, we show that Madhusudhan et al.'s scheme\[^{[25]}\] cannot provide user anonymity and perfect forward secrecy, and it is vulnerable to at least five types of attacks. The specific cryptanalysis process is as follows:

#### 7.1 Initialization phase

Suppose that HA computes \( n = pq \), where \( p, q \) are two prime numbers. And \( p' \) and \( q' \) are public primes, HA selects \( G \) (multiplication group) and an element \( g \in G \) with order \( q' \). Then HA choose a symmetric key \( S_{HA} = a(<q') \) and computes the public key \( P_{HA} = g^a \text{ mod } p' \). Similarly, FA chooses a private key \( S_{FA} = b(<q') \) then computes the public key \( P_{FA} = g^b \text{ mod } p' \).

#### 7.2 Registration phase

S1. A new MU randomly chooses \( ID_{MU} \), and \( PW_{MU} \) and a random number \( b \). Afterwards, MU submits \( (ID_{MU}||b) \) to HA.

S2. Upon receiving \( (ID_{MU}||b) \) from MU, HA calculates \( R_{MU} = h((ID_{MU}||b)||ID_{HA}||x) \), where \( x \) is a secret number of HA, and \( C_{MU} = (g^b \text{ mod } p) \oplus (ID_{MU}||b) \). Then, HA initiates a counter \( n_{MU} = 0 \) for MU and stores \( (ID_{MU}||b,n_{MU}) \) in its database and sends the parameters \( \{R_{MU},C_{MU},n_{MU}, h(.)\} \) to MU.

S3. On receiving the parameters, MU computes \( R_M = h(ID_{MU}||PW_{MU}||b) \). Then, MU keeps \( \{R_{MU},C_{MU},b,R_M,n_{MU}, h(.)\} \).

#### 7.3 Login and authentication phase

In this phase, MU and FA agree on a session key and perform mutual authentication through HA to access the required services. The login and authentication phases' procedures are depicted in Fig. 3.
S1. MU inputs $ID_{MU}^*$ and calculates $R_M^* = h(ID_{MU}^* || PW_{MU}^* || b)$. After, MU checks whether $R_M^* = R_M$ or not. If not, MU end the session. Otherwise, the legality of MU is ensured. Then MU generates a nonce $N_{MU}$ and computes $U = R_{MU} \oplus N_{MU}, V = (C_{MU} \oplus h(ID_{MU}^* || b) || ID_{FA}) \oplus N_{MU}, W = (U || n_{MU} || C_{MU} \oplus h(ID_{MU}^* || b))$. Finally, the mobile user MU sends FA the message $M_1 = \{U, V, W\}$.

S2. Upon receiving $M_1$, FA generates a random number $N_{FA}$. Afterwards, FA encrypts the message $M_1$ with $N_{FA}$. Subsequently, FA sends the encrypted information with FAs identity to HA.

S3. Upon receiving $M_2$, HA decrypts the received information and authenticates on it. If the authentication is successful, a session key is generated by HA for communication between FA and MU. If not, HA refutes the login request $M_2$. Otherwise, HA calculates $D_{KFH}(E_{KFH}(M_1, N_{FA})), B = h(x), g^b \mod p, N_{MU}^* = V \oplus ((g^b \mod p) || ID_{FA}), N_{MU}^* = (C_{MU} \oplus (ID_{MU}^* || b)) || ID_{FA}), N_{MU}^* = (g^b \mod p) \oplus (ID_{MU}^* || b) \oplus (ID_{MU}^* || b) || ID_{FA}) \oplus N_{MU} \oplus ((g^b \mod p) || ID_{FA}), N_{MU}^* = N_{MU}, R_{MU}^* = U \oplus N_{MU}^*$. Furthermore, HA checks whether $R_{MU}^*$ exists in HA. If it so, HA authenticates MU. Otherwise, HA ends this session. Afterwards, HA calculates $W^* = (U || n_{MU} || (g^b \mod p))$, then HA checks whether $W^*$ is equal to $W$ or not. If it is equal, HA authenticates MU. Otherwise, HA ends the session. Subsequently, HA figures out the session key $SK = h(g^b \mod p) \oplus N_{MU} \oplus N_{FA}$. Lastly, HA calculates the message $M_3 = \{E_{KFH}(SK)\}$ and sends to FA.

S4. Upon receiving $M_3$, FA figures out $D_{KFH}(E_{KFH}(SK)), V_1 = h(SK || N_{FA})$. Lastly, FA returns the message $M_4 = \{V_1, N_{FA}\}$ to MU.

S5. Upon receiving the message $M_4$, MU figures out $SK^* = C_{MU} \oplus (ID_{MU}^* || b) \oplus N_{MU} \oplus N_{FA}, V_1^* = h(SK^* || N_{FA})$. MU performs further routine verification. If both pass the verification, the authentication and key agreement process are completed successfully.

8 CRYPTOANALYSIS OF MADHUSUDHAN ET AL.’S SCHEME

8.1 No provision of mobile user anonymity and untraceability

Since the adversary $A$ can get the parameters $\{R_{MU}, C_{MU}, b, R_M, n_{MU}, h()\}$ of the smart card and the message $\{M_1 = \{U, V, W, ID_{FA}\}\}$ over public channel, she is able to compute $N_{MU} = U \oplus R_{MU}$ and $(C_{MU} \oplus ID_{MU}^* || b) || ID_{FA}) = V \oplus N_{MU}$. Afterwards, $A$ gets $C_{MU} \oplus ID_{MU}$. And then $A$ obtains $ID_{MU} = (C_{MU} \oplus ID_{MU}^* || b)) \oplus C_{MU}$ using $C_{MU}$. Therefore, Madhusudhan et al.’s scheme[25] cannot provide mobile user anonymity and untraceability.

8.2 Offline password guessing attack

Suppose that the adversary $A$ extracts these parameters $\{R_{MU}, C_{MU}, b, R_M, n_{MU}, h()\}$ from the smart card. The adversary $A$ can guess the user’s password in the offline way, and the specific process is as follows:

1) $A$ first selects $PW_{MU}^*$ and three identities $ID_{MU}^*$ from the password dictionary space $D_{PW}$ and three identity dictionary space $D_{ID}$, respectively.
2) $A$ calculates $R_M^* = h(ID_{MU}^* || PW_{MU}^* || b)$.
3) $A$ verifies whether $R_M^*$ is equal to $R_M$.

If it is equal, $A$ finds out the correct password and identity of MU. Otherwise, $A$ can repeat steps 1)-3) until the equation holds.

The time complexity of the above attack is: $O(|D_{PW}| \ast |D_{ID}| \ast T_h)$, therefore, the above attack is very efficient. On the other hand, according to Section , $A$ has been able to get $ID_{MU}$. Hence, the time complexity of the above attack can be reduce to $O(|D_{PW}| \ast T_h)$.
8.3 Replay attack
The attacker resends the $M_4$ to the mobile user, and the mobile user is unable to check the freshness of $M_4$. A method is: the user constructs the session key $SK$ and the new message $M_5$ to FA, FA checks the validity of $M_5$ and figures out $SK$ by using of its secret key.

8.4 Mobile user impersonation attack
According to Section , $\mathcal{A}$ has been able to get $ID_{MU}$ and $ID_{FA}$. $\mathcal{A}$ must forge a real login request message so as to impersonate the legitimate mobile user. In fact, $\mathcal{A}$ can take the following steps:

1) $\mathcal{A}$ chooses a random number $N_{MU}^*$ and computes $U^* = R_{MU} \oplus N_{MU}^*$.
2) $\mathcal{A}$ computes $V^* = (C_{MU} \oplus ID_{MU}||b||ID_{FA}) \oplus N_{MU}^*$.
3) $\mathcal{A}$ computes $W^* = (U^*||n_{MU}||C_{MU} \oplus h(ID_{MU}||b))$.
4) The adversary $\mathcal{A}$ sends the forged message $M_1^* = \{U^*, V^*, W^*\}$ to FA.

Obviously, the forged message $M_1^*$ is easy to pass the authentication of FA. And since the forged message $M_1^* = \{U^*, V^*, W^*\}$ is indistinguishable from the real $M_1$, MU can also pass the authentication of HA. Moreover, The time cost of this attack is only $T_h$. Therefore, Madhusudhan et al.’s scheme\cite{25} cannot resist mobile user impersonation attack.

8.5 Session key disclosure attack
Suppose that the adversary $\mathcal{A}$ can extract the parameters $\{R_{MU}, C_{MU}, b, h()\}$ of the smart card and the message $\{U, ID_{FA}, N_{FA}\}$ over public channel. Moreover, according to Section , $\mathcal{A}$ has been able to get $ID_{MU}$. Then $\mathcal{A}$ can figure out the established session key $SK$ by performing the following steps:

1) $\mathcal{A}$ computes $N_{MU} = U \oplus R_{MU}$.
2) $\mathcal{A}$ chooses a random number $SK = C_{MU} \oplus h(ID_{MU}||b) \oplus N_{MU} \oplus N_{FA}$.

Therefore, the adversary can easily get the session key without the private key $x$ of HA in Madhusudhan et al.’s scheme\cite{28}.

8.6 Foreign agent impersonation attack: Case I
Suppose that the adversary $\mathcal{A}$ can get the parameters $\{R_{MU}, C_{MU}, b, R_M, n_{MU}, h()\}$ of the smart card and the message $\{M_1 = \{U, V, W\}, ID_{FA}, M_4 = \{V_1, N_{FA}\}\}$ over public channel. According to Section , $\mathcal{A}$ has been able to get $ID_{MU}$. In order to impersonate the legitimate foreign agent FA, $\mathcal{A}$ must forge a real respond message to the mobile user. Accordingly, $\mathcal{A}$ can take the following steps:

1) $\mathcal{A}$ computes $N_{MU} = U \oplus R_{MU}$.
2) $\mathcal{A}$ chooses a random number $N_{FA}^*$.
3) $\mathcal{A}$ computes $SK^* = C_{MU} \oplus h(ID_{MU}||b) \oplus N_{MU} \oplus N_{FA}^*$.
4) $\mathcal{A}$ computes $V_1^* = h(SK^*||N_{FA}^*)$.
5) The adversary $\mathcal{A}$ sends the forged respond message $M_4^* = \{V_1^*, N_{FA}^*\}$ to FA.

Obviously, since the forged respond message $M_4^* = \{V_1^*, N_{FA}^*\}$ is indistinguishable from the real $M_4$, FA can pass the authentication of MU. Moreover, The time cost of this attack is only $2T_h$. Therefore, Madhusudhan et al.’s scheme\cite{25} is vulnerable to foreign agent impersonation attack.

8.7 Foreign agent impersonation attack: Case II
Suppose that the adversary $\mathcal{A}$ can get the parameters $\{R_{MU}, C_{MU}, b, R_M, n_{MU}, h()\}$ of the smart card and the message $U, ID_{FA}, M_4 = \{V_1, N_{FA}\}$ over public channel. In order to impersonate the legitimate foreign agent FA, $\mathcal{A}$ must forge a real respond message to the mobile user. Accordingly, $\mathcal{A}$ can take the following steps:

1) $\mathcal{A}$ computes $N_{MU} = U \oplus R_{MU}$.
2) $\mathcal{A}$ can compute $g^B \mod p||ID_{FA} = V \oplus N_{MU}$ because $N_{MU} = V \oplus (g^B \mod p||ID_{FA})$. Accordingly, $\mathcal{A}$

\[Qiu et al. J Surrveill Secur Saf 2021;2:66-82 \quad \text{http://dx.doi.org/10.20517/jsss.2020.28} \quad \text{Page 11 of 17} \]
Although a lot of work has been done to study the security flaws of existing protocols, there are relatively few studies to analyze the flaws of existing protocols from the perspective of the protocol design principles for GLOMONET, so the same common mistakes are repeated again and again. In fact, many security flaws of Xu et al.’s, Gupta et al.’s and Madhusudhan et al.’s schemes, that are pointed out in this paper, are caused by violating the basic design principles of the authentication schemes in GLOMONET (the details are summarized in Table 2). In fact, there are many security flaws in existing protocols because they violate the following four design principles proposed in this paper (see Table 3). Therefore, the four design principles proposed for authentication schemes summarized in this paper provide a reference for researchers to design secure and effective two-factor authentication protocols for GLOMONET.

### Table 2. Summary of six representative schemes violating the basic design principles of authentication schemes

| Schemes | Weaknesses | Principles not followed |
|---------|------------|-------------------------|
| Xu et al. [21] | Lack of mobile user untraceability, Offline password guessing attack, No perfect forward secrecy | Mobile user anonymity and untraceability [29], Anti offline password guessing [27], Perfect forward secrecy [27], Public key technology [27] |
| Gupta et al. [22] | Mobile user impersonation attack, Offline password guessing attack | Anti Offline password guessing [27], Mobile user anonymity and untraceability [29], Anti offline password guessing [27], Perfect forward secrecy [27], Public key technology [27] |
| Madhusudhan et al. [25] | Offline password guessing attack, Lack of mobile user untraceability | Anti offline password guessing [27], Public key technology [27] |

8.8 No perfect forward secrecy

In Madhusudhan et al.’s scheme [25], we suppose that \( \mathcal{A} \) can extract the parameters \( \{R_{MU}, C_{MU}, b, h()\} \) of the smart card and the message \( \{U, ID_{FA}, N_{FA}\} \) over public channel. Once the adversary \( \mathcal{A} \) obtains the home agent HAs private key \( x \), she can deduce the established session key by MU and FA by executing the following steps:

1) \( \mathcal{A} \) computes \( N_{MU} = U \oplus R_{MU} \).
2) \( \mathcal{A} \) can compute \( B = h(x) \), and then figures out \( g^B \mod p \).
3) \( \mathcal{A} \) chooses a random number \( SK = h(g^B \mod p) \oplus N_{MU} \oplus N_{FA} \).

Therefore, with help of the private key \( x \) of HA, the adversary can easily get the session key in Madhusudhan et al.’s scheme [25]. Accordingly, Madhusudhan et al.’s scheme [25] cannot provide perfect forward secrecy.

9 THE DESIGN PRINCIPLES OF AUTHENTICATION SCHEME IN GLOMONET

Although a lot of work has been done to study the security flaws of existing protocols, there are relatively few studies to analyze the flaws of existing protocols from the perspective of the protocol design principles for GLOMONET, so the same common mistakes are repeated again and again. In fact, many security flaws of Xu et al.’s, Gupta et al.’s and Madhusudhan et al.’s schemes, that are pointed out in this paper, are caused by violating the basic design principles of the authentication schemes in GLOMONET (the details are summarized in Table 2). In fact, there are many security flaws in existing protocols because they violate the following four design principles proposed in this paper (see Table 3). Therefore, the four design principles proposed for authentication schemes summarized in this paper provide a reference for researchers to design secure and effective two-factor authentication protocols for GLOMONET.

9.1 PKTP: Public key technology principle

Public key technology principle means that public key cryptosystem (eg., RSA, ECC and quadratic residue.) is used in the proposed authentication scheme. In order to improve the security and efficiency of authentication in global mobility networks, Lee et al. [19] propose a new authentication protocol. But the protocol only uses private key cryptography primitives (such as hash operation and XOR operation), and it is vulnerable to offline password guessing attack, and it also cannot provide perfect forward secrecy. Moreover, Ma et al. [27] also...
Table 3. A summary of the existing schemes that violate the four design principles of two-factor authentication schemes

| Design principles | The essence of the principles | Typical schemes violating the principles |
|-------------------|-------------------------------|-----------------------------------------|
| PKTP              | Under the assumption of non tamper resistant smart card, public key cryptography is a necessary condition to achieve two-factor security. | [16,18,19,22,55,59,64−67,70,71] |
| PFSP              | Public key technology is a necessary condition to achieve forward security, and the server-end has at least two public key operations. | [16,18−20,22,59,62,66,67,70,71] |
| MUAUP             | Under the assumption of non tamper resistant smart card, public key cryptography is the basic component of user anonymity and untraceability. | [19,20,24,53,56,59−66,70] |
| AOLPGP            | Public key technology and "Fuzzy verifiers" technology are the basic components to resist offline password guessing attack. | [16,18−20,22,53−55,57−59,62−71] |

proved that under the assumption of non-tamper resistant smart card, the two factor authentication protocol without public key cryptography cannot resist offline password guessing attack. Therefore, it is a necessary condition for authentication scheme to use public key technology in GLOMONET.

9.2 PFSP: Perfect forward secrecy principle

The meaning of perfect forward security is to ensure that the previously established session key is still secure when one or more long-term private keys are leaked. In 2000, Park et al. [48] researched the perfect forward secrecy principle of authentication and key agreement scheme for the first time. In 2014, Ma et al. [27] further points out that for the purpose of achieving perfect forward security, the two-factor authentication and key agreement scheme protocol must satisfy two basic conditions: (1) using public key cryptography; (2) at least two public key cryptography operations are required at the server side. This just explains the failure of forward security of Xu et al. [21]’s and Madhusudhan et al. [25]’s schemes.

In order to achieve perfect forward security, authentication protocols can take advantage of the difficulty of factorization of large integers, computational Diffie-Hellman problems on elliptic curves and chaotic maps, and lattice cryptography for compatibility with quantum resistance. Based on the balance between security and practicability, the designer can make a reasonable choice of public key cryptography technology according to the actual application requirements in GLOMONET.

9.3 MUAUP: Mobile users anonymity and untraceability principle

In GLOMONET, mobile users anonymity and untraceability is one of the most basic security properties. In actual mobile application scenarios, such as mobile electronic payment and mental health online consultation, mobile users may not want strangers to know their user names and communication traces.

In 2014, Wang et al. [49] proposed the anonymity public key principle for the two-factor protocol for wireless sensor network environment. Based on the work of Halevi et al. [50] and Impagliazzo et al. [51], Wang et al. strictly proved that it is infeasible to use symmetric key technology to realize user anonymity. Moreover, Wang et al. [49] also pointed out that the anonymity principle is universal and can be applied to other mobile application scenarios. Therefore, Xu et al. [21]’s and Madhusudhan et al. [25]’s protocols only use symmetric cryptography primitives such as hash function and XOR operation, which cannot realize user anonymity and untraceability. Specifically, in Xu et al.’s scheme [21], a fixed parameter $EID$ is transmitted by the mobile user on the common channel, which causes the adversary to track the mobile user's communication behavior. In Madhusudhan et al.'s scheme [25], the adversary can directly figure out the identity of mobile user. In the final analysis, the reason why provides anonymity and untraceability failure is that these parameters are not well protected by public key cryptography.

9.4 AOLPGP: Anti offline password guessing principle

Any authentication protocol in GLOMONET should be able to guarantee the security of password. If the password of mobile user can be guessed offline in polynomial time, it indicates that the protocol is vulnerable to
offline password guessing attacks. Moreover, in this case, the security of the authentication protocol is completely collapsed. In Xu et al.’s scheme [21], the adversary can guess the mobile user’s password and identity in three ways. Gupta et al.’s scheme [22] suffers from offline password guessing attack of two ways. Madhusudhan et al.’s scheme [25] is also vulnerable to offline password guessing attack. In order to achieve “local password security update”, Xu et al.’s scheme and Madhusudhan et al.’s scheme store password verification parameters in smart cards, which makes them convenient for offline password guessing, that is, there is a “security vs. usability” balance problem proposed by Huang et al. [52]. Fortunately, combining “Fuzzy-Verifiers” technology [33] with “Honeywords” technology in the field of system security, Wang et al. [26] successfully solves the problems left over in [52], achieves a better balance of “security vs. usability”, and achieves security beyond the traditional upper limit.

We can observe that Gupta et al.’s scheme uses “Fuzzy-Verifiers” technology [33] and “Honeywords” technology to provide local password verification, however, these parameters $M_3$, $M_5$ are constructed improperly in public channel, so that the adversary can use them to perform offline guessing attacks. In addition to offline guessing attacks, there are online guessing attacks. However, online guessing attack is easy to be detected, and can also be dealt with by setting the number of online wrong logins.

10 CONCLUSION

This paper analyzes the security of three representative anonymous authentication protocols in GLOMONET environment, highlights some serious security threats against these protocols, and gives the specific attack methods that attackers may take, which will provide better reference for the analysis and design of such protocols in GLOMONET. Specifically, this paper first points out that Xu et al.’s scheme [21] is vulnerable to three kinds of offline password guessing attacks and suffers from mobile user impersonation attack. Moreover, Xu et al.’s scheme [21] cannot also achieve perfect forward secrecy and user anonymity and untraceability. Next, it shows that Gupta et al.’s scheme [22] cannot resist two kinds of offline password guessing attacks and session-specific temporary information attack. Then, it is pointed out that Madhusudhan et al.’s scheme [25] is vulnerable to offline password guessing attacks, replay attack, mobile user impersonation attack, session key disclosure attack and two kinds of foreign agent impersonation attack, and cannot achieve mobile user anonymity and perfect forward secrecy.

It is pointed out that the above protocols [21,22,25] fail to resist offline password guessing attack and achieve anonymity and forward secrecy because it violates four basic principles of two-factor authentication protocol design: public key cryptography technology principle, perfect forward security principle, user anonymity & untraceability principle and anti offline password guessing principle. According to the basic design principles of authentication schemes, designing efficient and usability secure anonymous two-factor authentication protocols for roaming service in GLOMONET is worth studying in the next step.

DECLARATIONS

Acknowledgments
The authors thank the anonymous reviewers for their invaluable comments.

Authors’ contributions
Made substantial contributions to conception and design of the study and performed data analysis and interpretation: Qiu SM, Wang D
Availability of data and materials
Not applicable.

Financial support and sponsorship
This work was supported by the Science and technology research project of Education Department of Jiangxi Province (No.GJJ191680), and Doctoral Foundation of Jiangxi Normal University.

Conflicts of interest
Both authors declared that there are no conflicts of interest.

Ethical approval and consent to participate
Not applicable.

Consent for publication
Not applicable.

Copyright
© The Author(s) 2020.

REFERENCES
1. Forecast number of mobile users worldwide from 2020 to 2024. S. O’Dea 2020. Available from: https://www.statista.com/statistics/218984/number-of-global-mobile-users-since-2010. [Last accessed on 27 Jan 2021]
2. Jiang Q, Huang XH, Zhang N, Zhang K, Ma XD, Ma JF. Shake to communicate: secure handshake acceleration-based pairing mechanism for wrist worn devices. IEEE Internet Things 2019;6:5618-30.
3. Guo Y, Zhang Z, Guo Y. Fog-Centric authenticated key agreement scheme without trusted parties. IEEE Syst J 2020;99:1-10.
4. Jiang Q, Zhang N, Ni J, Ma J, Choo KKR. Unified biometric privacy preserving three-factor authentication and key agreement for cloud-assisted autonomous vehicles. IEEE Trans Veh Technol 2020;69:9390-401.
5. Aghili SF, Mala H, Shojafar M, Peris-Lopez P. Laco: lightweight three-factor authentication, access control and ownership transfer scheme for e-health systems in IOT. Future Gener Comp Sy 2019;96:410-24.
6. Aghili SF, Mala H, Shojafar M, ContiM. PAKIT: Proactive authentication and key agreement protocol for internet of things,IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS),2019 Apr 29-May 2, Paris, France: IEEE; 2019. pp. 348-53.
7. Qiu SM, Wang D, Xu GA, Kumari S. Practical and provably secure three-factor authentication protocol based on extended chaotic-maps for mobile lightweight devices. IEEE T Depend Secure 2020.
8. Suzuki S, Nakada K. An authentication technique based on distributed security management for the global mobility network. IEEE J Sel Areas Commun 1997;15:1608-17.
9. Lee T, Chang C, Hwang T. Private authentication techniques for the global mobility network. Wirel Pers Commun 2005;35:329-36.
10. Lee C, Hwang M, Liao I. Security enhancement on a new authentication scheme with anonymity for wireless environments. IEEE Trans Ind Electron 2006;53:1683-7.
11. Zhu J, Ma J. A new authentication scheme with anonymity for wireless environments. IEEE Trans Consum Electron 2004;50:231-5.
12. Chang C, Lee C, Chiu Y. Enhanced authentication scheme with anonymity for roaming service in global mobility networks. Comput Commun 2009;32:611-8.
13. Wu S, Zhu Y, Pu Q. A novel lightweight authentication scheme with anonymity for roaming service in global mobility networks. Int J Netw Manag 2011;21:384-401.
14. Zhou T, Xu J. Provable secure authentication protocol with anonymity for roaming service in global mobility networks. Comput Netw 2011;55:205-13.
15. He DB, Kumar N, Khan MK, Lee J. Anonymous two-factor authentication for consumer roaming service in global mobility networks. IEEE Trans Consumer Electron 2013;59:811-7.
16. He DB, Chan S, Chen C, Bu J, Fan R. Design and validation of an efficient authentication protocol for roaming service in global mobility networks. Wirel Pers Commun 2011;61:465-76.
17. Jiang Q, Ma J, Li G, Yang L. An enhanced authentication scheme with privacy preservation for roaming service in global mobility networks. Wirel Pers Commun 2013:68:1477-91.
18. Wen F, Susilo W, Yang G. A secure and effective anonymous user authentication scheme for roaming service in global mobility networks. Wirel Pers Commun 2013;73:993-1004.
19. Lee C, Lai Y, Chen C, Chen S. Advanced secure anonymous authentication scheme for roaming service in global mobility Networks. Wirel
20. Mun H, Han K, Lee YS, Yeun CY, Choi HH. Enhanced secure anonymous authentication scheme for roaming service in global mobility networks. *Math Comput Model* 2012;55:214-22.

21. Xu G, Liu J, Lu Y, Zeng X, Zhang Y, Li X. A novel efficient MAKA protocol with desynchronization for anonymous roaming service in Global Mobility Networks. *J Netw Comput Appl* 2018;107:83-92.

22. Gothe P, Hwang T. Lightweight and energy-efficient mutual authentication and key agreement scheme with user anonymity for secure communication in global mobility networks. *IEEE Syst J* 2016;10:1370-9.

23. Gupta M, Chaudhari NS. Anonymous two factor authentication protocol for roaming service in global mobility network with security beyond traditional limit. *Ad Hoc Netw* 2019;84:56-67.

24. Wu F, Xu LL, Kumari S, et al. An enhanced mutual authentication and key agreement scheme for mobile user roaming service in global mobility networks. *Annales des Télécommunications* 2017;72:131-44.

25. Madhusudhan R, Shashidhara R. Mobile user authentication protocol with privacy preserving for roaming service in GLOMONET. *Peer Peer Netw Appl* 2020;13:82-103.

26. Wang D, Wang P. Two birds with one stone: two-factor authentication with security beyond conventional bound. *IEEE Trans Dependable Secur Comput* 2018;15:708-22.

27. Ma CG, Wang D, Zhao S. Security flaws in two improved remote user authentication schemes using smart cards. *Int J Commun Syst* 2014;27:2215-27.

28. Wang D, Cheng H, He DB, Wang P. On the challenges in designing identity-based privacy-preserving authentication schemes for mobile devices, *IEEE Syst J* 2018;12:916-25.

29. Wang D, Wang P. On the anonymity of two-factor authentication schemes for wireless sensor networks: Attacks, principle and solutions. *Comput Netw* 2014;73:41-57.

30. Wang D, Wang N, Wang P, Qing S. Preserving privacy for free: Efficient and provably secure two-factor authentication scheme with user anonymity. *Inf Sci* 2015;321:162-178.

31. Dolev D, Yao A. On the security of public key protocols. *IEEE Trans Inf Theory* 1983;29:198-208.

32. Wang D, Wang P. On the Implications of Zipf's Law in Passwords, in: *Computer Security - ESORICS 2016 - 21st European Symposium on Research in Computer Security*, 2016 Sep 26-30, Heraklion, Greece. Springer; 2016. Part I, vol. 9878 of Lecture Notes in Computer Science, pp. 111-31.

33. Wang D, He DB, Wang P, Chu C. Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment. *IEEE Trans Dependable Secur Comput* 2015;12:428-42.

34. Eisenbarth TR, Kasper T, Moradi A, et al. On the power of power analysis in the real world: a complete break of the keeLoq code hopping scheme. 28th Annual International Cryptology Conference, 2008 Aug 17-21, Santa Barbara, CA, USA. Springer; 2008.

35. Kocher PC, Jaffe J, Jun B. Differential Power Analysis. Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology, 1999 Aug 15-16; Santa Barbara, California, USA. Springer; 1999. pp. 388-97.

36. Messerges TS, Dabbish EA, Sloan RH. Examining smart-card security under the threat of power analysis attacks. *IEEE Trans Computers* 2002;51:541-52.

37. Wang D, Zhang Z, Wang P, Yan J, Huang X. Targeted online password guessing: an underestimated threat. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016 Oct 24-28, Vienna, Austria. ACM; 2016. pp. 1242-54.

38. Wang D, Cheng H, Wang P, Xu H, Jian G. Zipf's Law in Passwords. *IEEE Syst J* 2019;13:238-47.

39. He DB, Wang D. Robust biometrics-based authentication scheme for multi-server Environment. *IEEE Syst J* 2015;9:816-23.

40. Wang CY, Ding K, Li WT, et al. An enhanced user authentication protocol based on elliptic curve cryptosystem in cloud computing environment. *Wirel Commun Mob Comput* 2018;18(9):1-13.

41. Wang CY, Xu GA, Li WT. A secure and anonymous two-factor authentication protocol in multiuser environment. *Secur Commun Netw* 2018;2018:9062675:1-15.

42. Wang CY, Xu GA. Cryptanalysis of three password-based remote user authentication schemes with non-tamper-resistant smart card. *Secur Commun Netw* 2017;1619741:1-14.

43. Krawczyk H. HMQV: A high-performance secure diffie-hellman protocol. Advances in Cryptology - CRYPTO 2005: 25th Annual International Cryptology Conference, 2005 Aug 14-18, Santa Barbara, California, USA. Springer; 2005. pp. 546-66.

44. Wang D, Li WT, Wang P. Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks. *IEEE Trans Ind Inform* 2018;14:4081-92.

45. Juels A, Rivest RL. Honeywords: making password-cracking detectable. 2013 ACM SIGSAC Conference on Computer and Communications Security, 2013 Nov 4-8, Berlin, Germany. ACM; 2013. pp. 145-60.
51. Impagliazzo R, Rudich S. Limits on the provable consequences of one-way permutations. Proceedings of the 21st Annual ACM Symposium on Theory of Computing, 1989 May 14-17, 1989, Seattle, Washington, USA. ACM; 1989. pp. 44-61.
52. Huang X, Chen X, Li J, Xiang Y, Xu L. Further observations on smart-card-based password-authenticated key agreement in distributed systems. *IEEE Trans Parallel Distributed Syst* 2014;25:1767-75.
53. Lu Y, Xu G, Li L, Yang Y. Robust privacy-preserving mutual authenticated key agreement scheme in roaming service for global mobility Networks. *IEEE Syst J* 2019;13:1454-65.
54. Odelu V, Banerjee S, Das AK, et al. A secure anonymity preserving authentication scheme for roaming service in global mobility networks. *Wirel Pers Commun* 2017;96:2351-87.
55. Madhusudhan R, Shashidhara. An efficient and secure authentication scheme with user anonymity for roaming service in global mobile networks. Proceedings of the 6th International Conference on Communication and Network Security, 2016 Nov 26-29, New York, NY, USA. ACM; 2016. pp. 119-26.
56. Kuo W, Wei H, Cheng J. An efficient and secure anonymous mobility network authentication scheme. *J Inf Secur Appl* 2014;19:18-24.
57. Srinivas J, Mishra D, Mukhopadhyay S, Kumari S, Guleria V. An authentication framework for roaming service in global mobility networks. *Inf Technol Control* 2019;48:129-45.
58. Li X, Niu J, Kumari S, Wu F, Choo, KKR. A robust biometrics based three-factor authentication scheme for Global Mobility Networks in smart city. *Future Gener Comput Syst* 2018;83:607-18.
59. Gope P. Enhanced secure mutual authentication and key agreement scheme with user anonymity in ubiquitous global mobility networks. *J Inf Secur Appl* 2017;35:160-7.
60. He DB, Ma M, Zhang Y, Chen C, Bu J. A strong user authentication scheme with smart cards for wireless communications. *Comput Commun* 2011;34:367-74.
61. Yoon E, Yoo K, Ha K. A user friendly authentication scheme with anonymity for wireless communications. *Comput Electr Eng* 2011;37:356-64.
62. Kang M, Rhee HS, Choi J. Improved user authentication scheme with user anonymity for wireless communications. *IEICE Trans Fundam Electron Commun Comput Sci* 2011;94-A:860-64.
63. Li H, Yang Y, Pang L. An efficient authentication protocol with user anonymity for mobile networks. 2013 IEEE Wireless Communications and Networking Conference (WCN), 2013 Apr 7-10, Shanghai, China. IEEE; 2013. pp. 1842-47.
64. Lee H, Lee D, Moon J, et al. An improved anonymous authentication scheme for roaming in ubiquitous networks. *PLOS ONE* 2018;13:1-33.
65. CChaudhry SA, Albeshri A, Xiong N, Lee C, Shon T. A privacy preserving authentication scheme for roaming in ubiquitous networks. *Clust Comput* 2017;20:1223-36.
66. Farash MS, Chaudhry SA, Heydari M, et al. A lightweight anonymous authentication scheme for consumer roaming in ubiquitous networks with provable security. *Int J Commun Syst* 2017;30:e3019.1-20.
67. Gope P, Hwang T. Enhanced secure mutual authentication and key agreement scheme preserving user anonymity in global mobile networks. *Wirel Pers Commun* 2015;82:2231-45.
68. Ghahramani M, Javidan R, Shojafer M. A secure biometric-based authentication protocol for global mobility networks in smart cities. *J Supercomput* 2020;76:8729-55.
69. Wu F, Li X, Xu L, Kumari S, Sangaiah AK. A novel mutual authentication scheme with formal proof for smart healthcare systems under global mobility networks notion. *Comput Electr Eng* 2018;68:107-18.
70. Park K, Park Y, Park Y, Alavalapati GR, Das AK. Provably secure and efficient authentication protocol for roaming service in global mobility networks. *IEEE Access* 2017;5:25110-25.
71. Shashidhara R, Bojjagani S, Maurya AK, Kumari S, Xiong H. A robust user authentication protocol with privacy-preserving for roaming service in mobility environments. *Peer Peer Netw Appl* 2020;13:1943-66.