Wireless Networks (2022) 28:745–763
https://doi.org/10.1007/s11276-021-02820-x

ORIGINAL PAPER

An improved anonymous DoS-resistant authentication protocol in smart city

Rui Chen[1] · **Yongcong Mou**[2] · **Min Zhang**[3]

Accepted: 8 October 2021 / Published online: 27 January 2022

Abstract

With the development and practical application of 5G technology, the construction of smart cities has progressed into an entirely new level. Mobile wireless networks in smart cities provide people with ubiquitous network services, thereby making the entire city organic. However, the open character of such wireless networks results in network security issues. As a result, people suffer from potential network threats while enjoying the convenience of wireless networks. To solve this problem, various roaming authentication protocols for mobile network are proposed. We find that a contradiction exists between user anonymity and resistance to denial of service (DoS) attacks. Most current protocols attach importance to user privacy protection. Hence, they are vulnerable to DoS attacks, which cause network paralysis. We put forward an anonymous authentication protocol with DoS resistance for smart cities by overcoming the defects of the protocol of Xie et al. Then, two formal validation tools, namely, ProVerif and BAN logic, are introduced to verify the security of our scheme. Security analyses indicate that our protocol not only meets many known security properties but also shows higher efficiency compared with related works. In addition, the proposed protocol achieves a good balance between user anonymity and DoS attack resistance, while many other schemes failed to do so because they ignore this type of attack. Thus, it is more suitable for smart cities.

Keywords Smart city · GLOMONET · Anonymity · Authentication · Denial of Service

1 Introduction

With the continuous improvement of the mobile telecommunications industry, the study of wireless mobile network application has been a trending research topic. Mobile wireless networks have also been increasingly applied in human communications. The application of such networks overthrows traditional business models and motivates the exploration of new business opportunities. Meanwhile, people's consumption habits and way of life are changing slowly. Smart cities have been constructed following the trend of mobile internet development. As a result, such cities have high intelligence, high resource utilization, affordable cost of living, and improved quality of life by utilizing information and communication technologies.

From the perspective of technology development, the construction of smart cities requires the realization of comprehensive perception, ubiquitous interconnection, pervasive computing, and integration application of Internet of Things(IoT) and cloud computing. Global Mobility Network (GLOMONET) based on 5G [1–3] mobile communication technology are the network infrastructure of smart cities. Such networks provide wireless connection maintenance anytime and anywhere and relay services to mobile users (*MU*s). A typical GLOMONET scenario has three participants, namely, the *MU*, the home agent (*HA*), and the foreign agent (*FA*). The authentication model of GLOMONET is called three-party authentication [4], which involves the three participants. In other words, the mutual authenticate of *MU* and *FA* require the help of *HA*.

✉ Rui Chen
crs1934@hotmail.com

[1] College of Computer Science, Sichuan Normal University, Chengdu 610066, China

[2] Sichuan Water Conservancy Vocational College, Chengdu 611231, China

A *MU* who registered in *HA* don’t usually stay in one place all the time, he/she can travel to anywhere within the scope of global mobile communication network and obtain the registered network service through the visited foreign agent. AS the *MU* enters the wireless network coverage of the *FA*, the *FA* can authenticate the *MU* through *HA*. On the other hand, *MU* can also verify the authenticity of *FA* and avoid connecting to Pseudo Base Stations (PBS). Mutual authentication is a very important security measure. It requires *MU*, *FA* and *HA* to authenticate each other before providing any network services, so as to avoid the risk of information leakage.

The GLOMONET suffers from various malicious attacks due to the opening and sharing characters of the wireless channel. Such attacks result in sensitive information leakage and communication failure. Currently, user authentication and privacy preserving are considered as both contact and contradiction issue when referring to GLOMONET. Therefore, designing a secure and robust protocol for roaming services in smart cities is a challenging task. Figure 1 indications some typical security scenarios that require identity authentication in smart cities, such as vehicle network, mobility network and telemedicine network.

Smart cities also have a few disadvantages. As the cities become smarter, they need more and more devices, such as street lights, public displays and so on, to integrate sensors, screens, batteries and processors. Once these devices run out of power or malfunctions, they will likely be thrown away and become e-waste. The components in electronic products contain a variety of toxic substances, which bring serious hazards to the environment and human health.

1.1 Related works

Numerous researchers have analyzed and designed security protocols and proposed various authentication protocols for GLOMONET. However, cryptanalysis shows that most protocols are insecure and cannot resist possible attacks, especially the denial of service (DoS) attacks.

Since Zhu et al. [5] presented a first authentication protocol for wireless network environment, many similar schemes have been put forward in decades. In these protocols, two-factor schemes based on passwords and smart cards have gained considerable attention because of their higher security compared with password-based schemes.

In 2011, He et al. [6] proposed an authentication scheme for GLOMONET environment, but Jiang et al. [7] indicated that this scheme have two security flaws and unable to achieve two-factor security. Subsequently they proposed an improved scheme based on quadratic residue. However, Wen et al. [8] found that the scheme in [7] cannot withstand spoofing, stolen verifier, and replay attacks. Then they designed a new authentication scheme for roaming environment. Farash et al. [9] and Gope et al. [10] exposed that the scheme in [8] is suffering from offline password guessing and forge attacks, and unfair key agreement. Then, they independently improved the scheme to fix these security flaws. However, Youngseok et al. [11] and Karuppiah et al. [12] individually

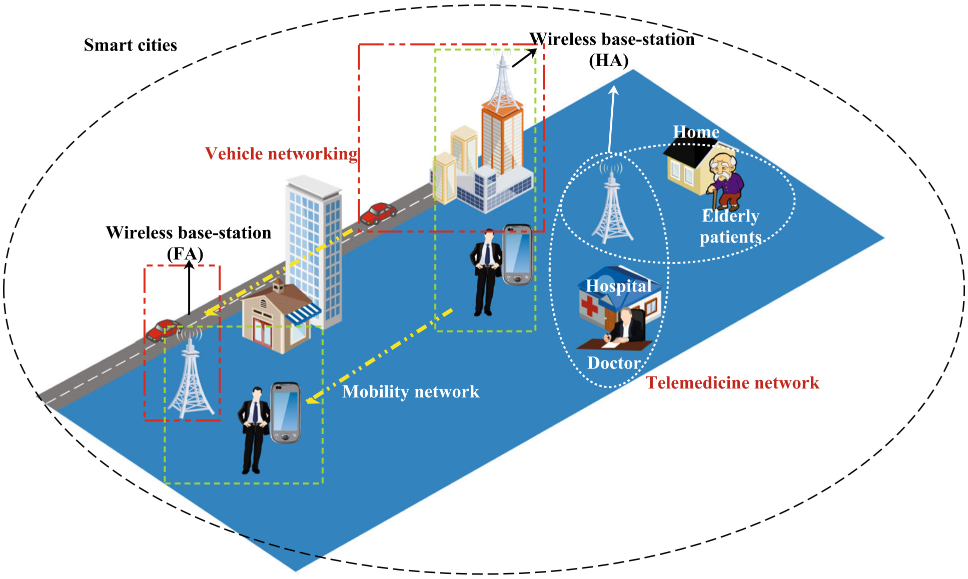


Fig. 1 Typical security scenarios of smart cities

proved that the scheme in [9] also has some weaknesses and cannot protect user privacy.

Authors of [13] analyzed the drawbacks in Mun et al.'s scheme [14]. They also pointed out that this scheme can neither prevent forgery and insider attacks nor provide mutual authentication. Then, they presented an improvement scheme without timestamp. Later, Wen et al. [15] found that the scheme in [16] is insecure against offline password guessing and impersonation attacks. After analyzing the security flaws of Miyoung et al.'s protocol [17], Karuppiah et al. [18, 19] put forward two enhanced authentication schemes for GLOMONET.

In 2016, Gope et al. [20] indicated that the scheme in [21] suffers from forgery and insider attacks. Then, on the basis of this scheme, a new lightweight authentication scheme is presented by Gope et al. Later, they proposed a new two-factor authentication scheme [22] to fix the security flaws in He et al.'s scheme [23]. However, Wu et al. [24] and Xu et al. [25] showed that Gope et al.'s scheme remains insecure because it is vulnerable to desynchronization and replay attacks.

Subsequently, Chaudhry et al. [26] designed a novel scheme to make up for the flaws of Farash et al.'s scheme [9]. However, Lee et al. [27] revealed that Chaudhry et al.'s scheme cannot withstand impersonation and stolen-mobile-device attacks. Later on, Fraz et al. [28] indicated that the protocol in [29] cannot provide user-anonymous and mutual authentication and resist replay and DoS attack. Then, Fraz et al. [28] presented a similar lightweight authentication scheme to fix the security weaknesses. In the same year, Chen et al. [30] discovered that a recent scheme [31] have several security flaws and unable to achieve mutual authentication. Hence, Chen improved the scheme for wireless communications networks.

In 2018, Madhusudhan et al. [32] discussed the security issues in Shin et al.'s scheme [18] and indicated that this scheme is inefficient and unsafe to stolen verifier, impersonation, DoS, insider, and synchronization attacks. Then, Madhusudhan enhanced the scheme to remedy these security drawbacks existing in [18]. Later on, a provable security scheme that utilizes random numbers to resist the desynchronization attack was proposed by Wu et al. [33].

Since 2020, a lot of authentication protocols for various IoT scenarios are proposed, such as IoT-based telemedicine network and intelligent transportation system. Li et al. [34] presented an identity based signature scheme for the IoT networks and claimed that their scheme can satisfy user anonymity and strong unforgeability. With regard to the limited resources of sensing nodes in IoT environment, Aydin et al. [35] proposed a lightweight group authentication schemes for wireless communication environments, which can be applied to different group authentication scenarios.

That same year, Kumar et al. [36] designed an authentication protocol based on Electrocardiogram (ECG) or Electroencephalogram (EEG) signals for Body Sensor Network (BSN). Everyone has different ECG and EEG signal which can be used for creating secure connection between patients and telemedicine system. Deebak et al. [37] found that the scheme in [38] cannot provide patient anonymity and suffers from health-report revelation and health-report forgery attacks. Then they put forward an improved service authentication framework for the Telecare Medical Information System (TMIS) and evaluated the algorithm efficiency by using Field Programmable Gate Array (FPGA) platform. Jangirala et al. [39] proposed a three-factor authentication scheme for IoT-based Intelligent Transportation System (ITS) which provides data transmission service and authentication service between vehicles to semi-trusted Cloud-Gateway (CG) node.

Recently, Physical Unclonable Functions (PUF) has been interested to many researchers by its unique physical characteristics. Several mutual authentication schemes [40–43] based on PUF have been proposed in the last year. Bansal et al. [40] presented a lightweight and privacy-preserving authentication scheme for Vehicle-to-Grid ecosystem (V2G) systems. Their scheme uses PUFs to verify the identity of an electric vehicles and the power grid. Shortly afterward, Alladi et al. [41, 42] put forward two lightweight mutual authentication schemes for Unmanned Aerial Vehicles (UAV) communication network. Focus of their studies are the research on security wireless data transmission between UAVs and its ground station. A more recent study [44] presented an anonymous ligthweight authentication scheme for group data sharing in opportunistic mobile social networks(OMSN), which provide privacy preservation of group users while sharing data in OMSN scenarios.

1.2 Our contributions

Main contributions of this study include:

- Through a comprehensive analysis of relevant literature, we summarize and analyze the exclusive relationship between user anonymity and DoS attack resistance. The achievement of user untraceability must lead to DoS attack, and the achievement of DoS attack resistance is at the cost of sacrificing user anonymity.
- Some security flaws in Xie et al.'s scheme [47], such as lack of local verification in the login phase and missing session key update phase, are highlighted. In addition, their scheme cannot work when numerous *MU*s from a same *HA* flood into an *FA* simultaneously.

- An enhanced authentication protocol has been presented to balance the anonymous and security demand.
- The proposed protocol is secured on the basis of the analysis of automated tools, namely, ProVerif and BAN logic. Moreover, the performance analysis shows that the new protocol has better efficiency compared with some current authentication protocols.

1.3 Organization of the paper

The remainder of this article is arranged as follows. Section 2 shows the mutually exclusive relationships of anonymous and DoS attack resistance. Section 3 discusses the scheme in [47] and analyzes its security flaws. A detailed description of the proposed scheme and its security analysis and formal security proof are provided in Sects. 4 and 5. Section 6 gives the functional and performance comparisons and some conclusions are drawn in the last section.

2 Anonymous and DoS attack

As in the description in [45], the definition of user anonymity is primarily directed against the client instead of the server. In addition, the notion of user anonymity in an authentication scheme has different scopes and meanings in different application scenarios. In general, user anonymity can be divided into two kinds, namely, weak and strong anonymity. The former refers to user identity protection, which ensures that no one is able to get the real identity of the *MU* except the respective *HA*. Meanwhile, the latter refers to user untraceability. User untraceability contains the user identity protection and unlinkable message. On this basis, the adversary neither obtains the real identities of users nor their current location and moving history through the user activities in roaming. Therefore, most researchers have designed anonymous authentication protocols with user untraceability because such protocols provide high-level user privacy protection. To achieve this goal and realize privacy protection, the *MU* must take some measures, such as dynamic identity and random number techniques, which can provide effective protection against eavesdropping and intercept attacks.

Through the above two techniques, the login request messages sent by the *MU* are different from each other. Thus, the message receiver, except for the *HA*, cannot identify the message senders. Even though numerous login request messages from the same *MU* are received, the *FA* also cannot identify the *MU* because each message is unique. Hence, the adversary can launch DoS attacks and send large amounts of randomly generated invalid login data intentionally to overwhelm the *FA* and *HA* because the *FA* believes that these messages belong to different *MU*s and forwards these messages to the *HA* following the rules of authentication protocol. This actions quickly exhaust network bandwidth and resources, possibly frustrating legal users to use the resources they needed. In accordance with references and research, user untraceability and DoS attack resistance is hardly achieved simultaneously because the two requirements are mutually exclusive. However, majority of current studies [6–10, 15–18, 18–22, 24, 29, 32, 33, 46–51] focuses on strong user anonymity. Hence, these studies fail to consider DoS attack prevention. As user anonymity is achieved, it becomes vulnerable to DoS attacks because the authentication protocols in GLOMONET require an *FA* to forward the login request messages of the *MU* to the *HA* unconditionally [4, 52]. Therefore, DoS attacks can be easily launched by an adversary to an *HA* through an *FA*.

An effective method to prevent DoS attacks is to use message-specific puzzles (i.e., client puzzles [53]). This method requires the *FA* to identify the message sender and send puzzle problems to the *MU* if the number of request messages exceeds a previously set threshold value. Evidently, the client puzzle techniques cannot provide user anonymity.

In this article, we discuss this topic and find measures to solve the problem, thus balancing the requirement of user untraceability and DoS attack resistance.

3 Brief review and security analysis of Xie et al.'s scheme

3.1 Brief review of Xie et al.'s Scheme

The scheme of Xie et al. [47] has three main phases, namely, registration, login, and authentication. Table 1 shows the notations of this paper.

Table 1 Notations

Notations	Description
MU, FA, HA	Mobile user, Home agent and Foreign agent
$ID_{MU}, ID_{FA}, ID_{HA}$	Identity of *MU*, *FA* and *HA*
PW_{MU}	Password of *MU*
K_{FH}	The shared key between *HA* and *FA*
x	Private key of *HA*
$f()$	A number generating function
T_{seed}	A timestamp for function $f()$
T_{AUTH}	The average time of authentication phase

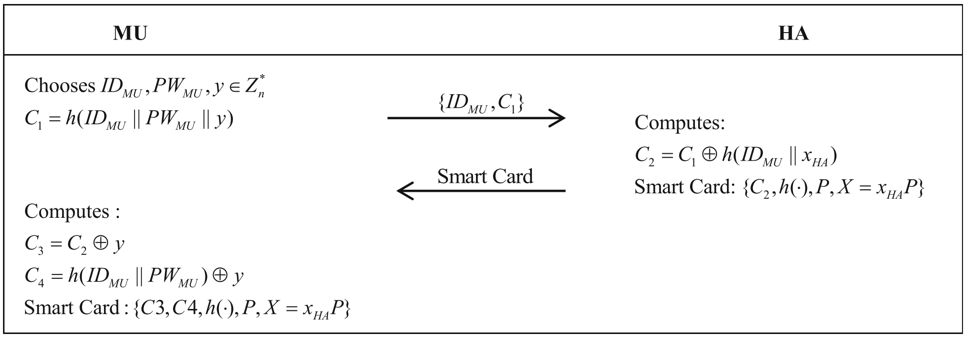


Fig. 2 Registration process of Xie et al's scheme

3.1.1 Registration

The *MU* should register with the *HA* to access the network services or obtain roaming services when visiting an *FA*. The registration process is depicted in Fig. 2.

3.1.2 Login and authentication

When an *MU* enters the coverage of an *FA* and wants to obtain the registered services from the *FA*, then the *MU* and the *FA* need to authenticate each other through the *HA* and establish the shared session key for securing communication. The detailed steps of this process are depicted in Fig. 3.

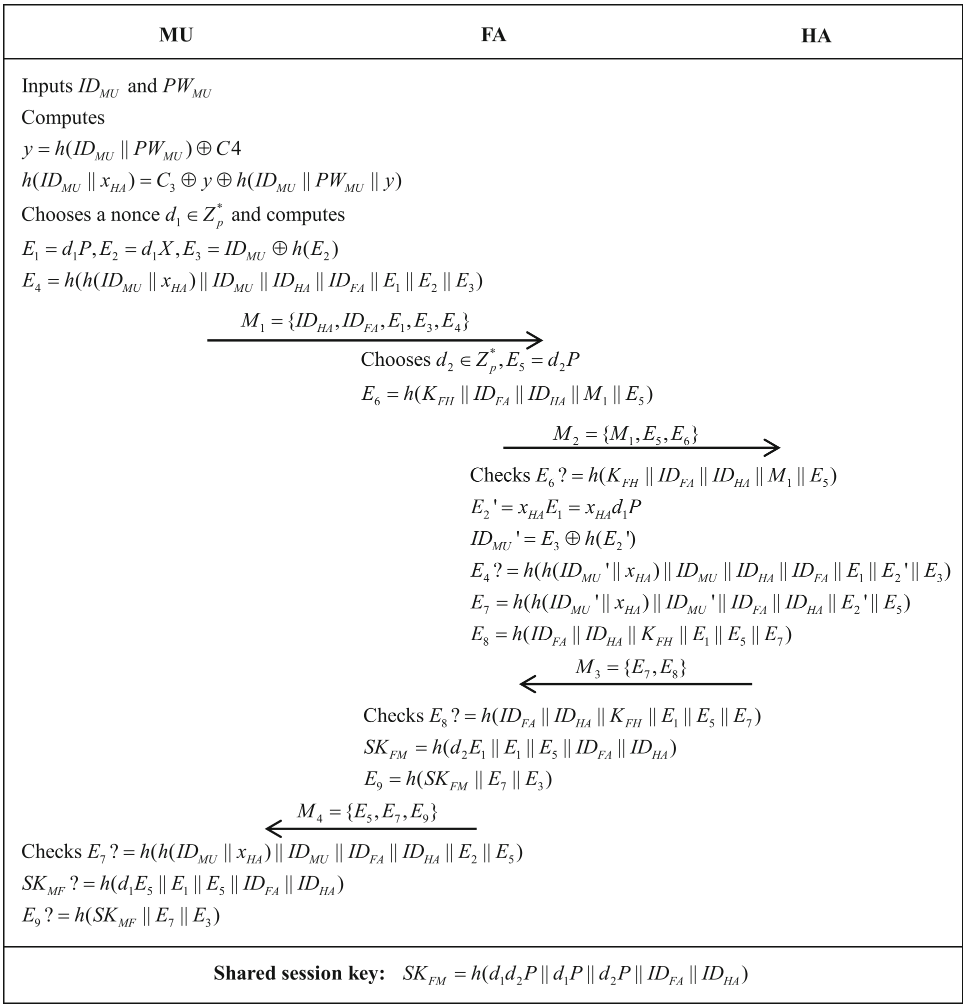


Fig. 3 Login and authentication phases of Xie et al's scheme

3.2 Security analysis of Xie et al.'s Scheme

3.2.1 Lack of input validation during the login process

To obtain the registered network services from the visited *FA*, the *MU* should first enter the user information (i.e. ID_{MU} and PW_{MU}), then generates the login message and send it to the *FA*. However, the user information is never inspected by the smart card in Xie et al.'s scheme. Therefore, even if user enters problematic data, accidentally or purposely, the login and the authentication are still performed until the *HA* discovers that the login message is illegal. These additional authentication steps reduce the efficiency of the authentication system and result in extra communication and computational overhead. We can avoid unnecessary operations by verifying the input information locally during login.

3.2.2 Lack of identification when numerous *MU*s visit an *FA* simultaneously

For instance, in a short period, numerous *MU*s from the same *HA* simultaneously roam into the coverage of the *FA*. These *MU*s send login requests to the *FA*, and the *FA* forwards these messages to the *HA*. After the successful authentication of login data, the *HA* replies $\{E_7, E_8\}$ for every login message to the *FA* in a short period. However, the *FA* cannot identify every *MU* through the reply message $\{E_7, E_8\}$ because the two hash values do not match the *MU* individually. Hence, Xie et al.'s scheme cannot complete the authentication under the circumstances.

3.2.3 Vulnerability to DoS attack

To achieve strong user anonymity, the scheme in [47] adopts the random number technique. Hence, every login request message based on a randomly selected number is different from each other. This weak point can result in adversary or malicious *MU*s to launch a DoS attack easily by generating substantial illegal login requests to the *FA*, and the *FA* directly forwards any unauthenticated login message to the *HA*. Lastly, the available service resources of the *HA* and the *FA* are exhausted quickly. As a result, these resources can no longer provide normal services to legitimate *MU*s.

3.2.4 Lack of session key update phase

If an *MU* stays in the coverage of an *FA* for a long period and keeps in touch with the *FA*, the *MU* and the *FA* must regularly update the session key for security reasons. However, the scheme in [47] disregards the issue on update session key and provides the specific update method.

4 Outline of our scheme

A new improved authentication scheme for smart city environment is put forward in this section.

4.1 Initialization

HA first selects the public parameters $\{F_p, n, E, P, G, h(.), f()\}$, then generates a random number $x \in Z_n^*$ as secret key. Next, *HA* establish the shared key K_{FH} with *FA* through a secure key agreement protocol. Finally, *HA* publishes the public parameters and keeps x secret.

4.2 Registration

When an *MU* joins the authentication system, the following steps should be performed to register on their *HA*. The details of the registration phases are shown in Fig. 4.

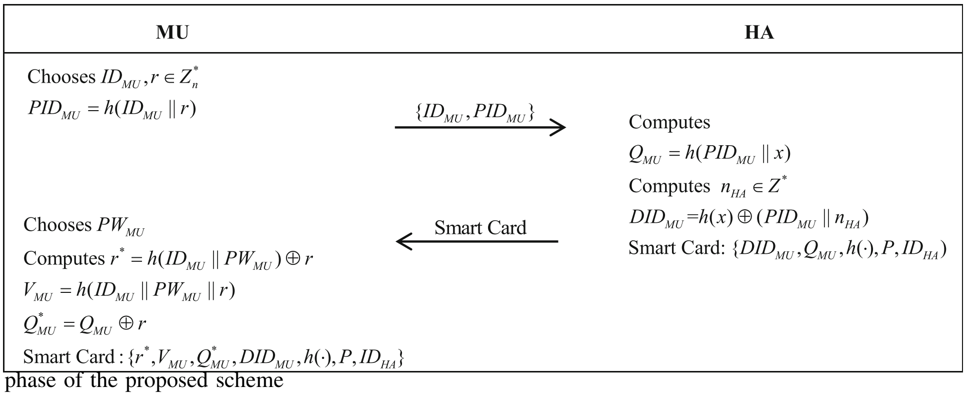


Fig. 4 Registration phase of the proposed scheme

Step 1. The MU first selects ID_{MU} and generates a random number $r \in Z_n^*$. Next, the MU calculates $PID_{MU} = h(ID_{MU} \parallel r)$ and sends $\{ID_{MU}, PID_{MU}\}$ as a registration message to the HA.

Step 2. Once the registration message is received, the HA computes $Q_{MU} = h(PID_{MU} \parallel x)$, then generates a random nonce $n_{HA} \in Z^*$ and calculates $DID_{MU} = h(x) \oplus (PID_{MU} \parallel n_{HA})$. Then, the HA stores $\{DID_{MU}, Q_{MU}, h(.), P, ID_{HA}\}$ into a smart card (SC) and submits it to the MU.

Step 3. The MU selects a password PW_{MU} and computes $r^* = h(ID_{MU} \parallel PW_{MU}) \oplus r, V_{MU} = h(ID_{MU} \parallel PW_{MU} \parallel r), Q^*_{MU} = Q_{MU} \oplus r$ and finally stores $\{r^*, V_{MU}, Q^*_{MU}, DID_{MU}, h(.), P, ID_{HA}\}$ into the SC.

4.3 Login and authentication

If an MU visits an FA and tries to obtain the registered services. At this time, the MU and the FA should complete mutual authentication through the HA. The details of this process is demonstrated in Fig. 5.

Step 1. The MU enters ID_{MU} and PW_{MU} into the device terminal. Then, the SC in the terminal computes $r = h(ID_{MU} \parallel PW_{MU}) \oplus r^*$ and checks $V_{MU}? = h(ID_{MU} \parallel PW_{MU} \parallel r)$. If the two values

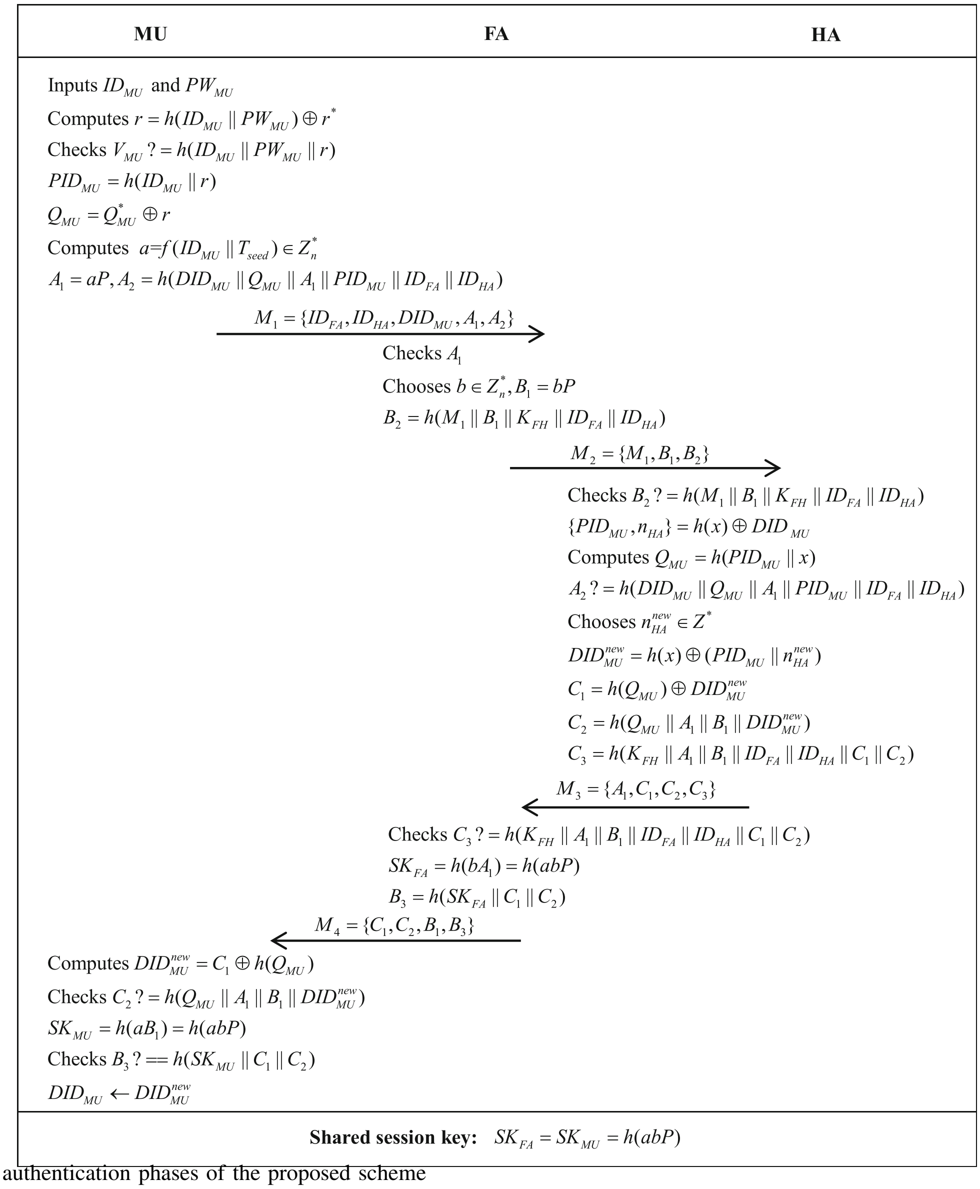


Fig. 5 Login and authentication phases of the proposed scheme

are unequal and the amount of password retries reached the predefined threshold(e.g. 3), then the login action is canceled; otherwise, the MU calculates $PID_{MU} = h(ID_{MU} \| r)$ and $Q_{MU} = Q^*_{MU} \oplus r$. Then, the MU takes the current timestamp T_{seed} as seed to generate a random number $a = f(ID_{MU} \| T_{seed})$, where $f()$ is a number-generating function. The timestamp T_{seed} is stored for a certain period to resist the DoS attack (we use T_{AUTH} to represent the average time of authentication process, then the time interval can be set to T_{AUTH}). Later, the MU computes $A_1 = aP, A_2 = h(DID_{MU} \| Q_{MU} \| A_1 \| PID_{MU} \| ID_{FA} \| ID_{HA})$ and sends $M_1 = \{ID_{FA}, ID_{HA}, DID_{MU}, A_1, A_2\}$ to FA.

Step 2. Upon getting M_1, FA first verifies the message to resist a potential DoS attack. The values A_1 do not change during a given period (T_{AUTH}); thus, the FA has enough time to identify the MUs by comparing A_1 in received messages. If the number of incoming messages from the same MU is greater than a previously set threshold value, then the FA can determine whether he/she is under DoS attack, terminate the session, and inform the HA. Otherwise, the FA generates a nonce $b \in Z^*_n$ and further computes $B_1 = bP, B_2 = h(M_1 \| B_1 \| K_{FH} \| ID_{FA} \| ID_{HA})$. Then, the FA forwards $M_2 = \{M_1, B_1, B_2\}$ to the HA.

Step 3. Upon receiving M_2 from the FA, the HA initially checks whether B_2 is equal to $h(M_1 \| B_1 \| K_{FH} \| ID_{FA} \| ID_{HA})$. The session is terminated if the two values are unequal; otherwise, the HA computes $\{PID_{MU}, n_{HA}\} = h(x) \oplus DID_{MU}, Q_{MU} = h(PID_{MU} \| x)$ and checks $A_2? = h(DID_{MU} \| Q_{MU} \| A_1 \| PID_{MU} \| ID_{FA} \| ID_{HA})$. If the result is equal, then the HA generates a random number $n^{new}_{HA} \in Z^*$ and calculates $DID^{new}_{MU} = h(x) \oplus (PID_{MU} \| n^{new}_{HA})$. Then, the HA computes $C_1 = h(Q_{MU}) \oplus DID^{new}_{MU}, C_2 = h(Q_{MU} \| A_1 \| B_1 \| DID^{new}_{MU}), C_3 = h(K_{FH} \| A_1 \| B_1 \| ID_{FA} \| ID_{HA} \| C_1 \| C_2)$. Lastly, the HA sends the message $M_3 = \{A_1, C_1, C_2, C_3\}$ to the FA.

Step 4. After obtaining the reply message, the FA initially checks the validation of C_3 by comparing it with $h(K_{FH} \| A_1 \| B_1 \| ID_{FA} \| ID_{HA} \| C_1 \| C_2)$. After successful verification, the FA generates the secret session key $SK_{FA} = h(bA_1) = h(abP)$ and $B_3 = h(SK_{FA} \| C_1 \| C_2)$ and sends $M_4 = \{C_1 \| C_2 \| B_1 \| B_3\}$ to the MU.

Step 5. After M_4 is received, the MU computes $DID^{new}_{MU} = C_1 \oplus h(Q_{MU})$ and verifies $C_2? = h(Q_{MU} \| A_1 \| B_1 \| DID^{new}_{MU})$. If they are the same, then the MU computes the session key $SK_{MU} = h(aB_1) = h(abP)$ and checks $B_3? = h(SK_{MU} \| C_1 \| C_2$ to authenticate FA. Lastly, the MU replaces DID_{MU} with DID^{new}_{MU}. The mutual authentication procedure is then completed, and the shared session key SK_{FA}/SK_{MU} is established.

4.4 Password update

MU can update the password at any time through these steps.

Step 1. MU first puts SC into the terminal device and enters ID_{MU}, PW_{MU}.

Step 2. SC computes $r = h(ID_{MU} \| PW_{MU}) \oplus r^*$ and compares V_{MU} with $h(ID_{MU} \| PW_{MU} \| r)$. If they are unequal, the phase is cancelled.

Step 3. SC asks MU for new password PW^{new}_{MU}.

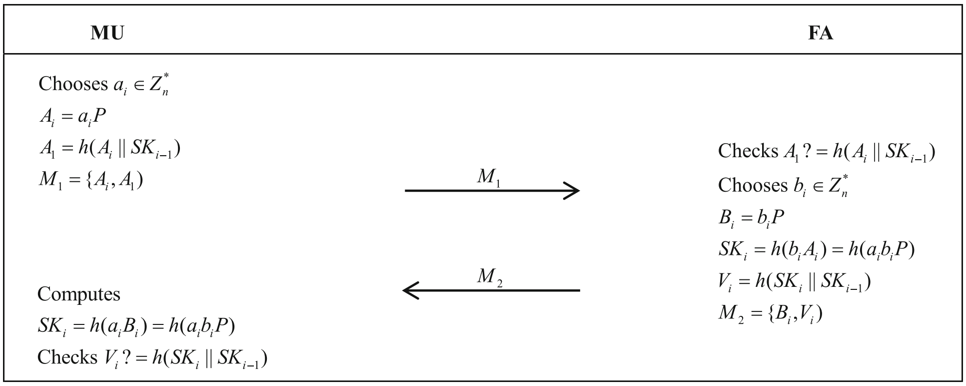


Fig. 6 Session key update phase of the proposed scheme

Step 4. Upon receiving PW_{MU}^{new}, SC calculates $r^{new*} = h(ID_{MU} \parallel PW_{MU}^{new}) \oplus r$, $V_{MU}^{new} = h(ID_{MU} \parallel PW_{MU}^{new} \parallel r)$, and replaces $\{r^*, V_{MU}\}$ with $\{r^{new*}, V_{MU}^{new}\}$.

4.5 Session key update

The shared session key should be updated regularly if MU stays in FA for a long period. Their ith session key $SK_i(i = 2;\ldots;n)$ can be generated as follows. Figure 6 gives a detailed description about this phase.

Step 1. MU first generates a number $a_i \in Z_n^*$ randomly and calculates $A_i = a_iP, A_1 = h(A_i \parallel SK_{i-1})$ where SK_{i-1} is the $(i-1)$th session key, then MU sends $M_1 = \{A_i, A_1\}$ to FA.

Step 2. FA compares A_1 with $h(A_i \parallel SK_{i-1})$. If they are unequal, the phase is cancelled. Otherwise, FA generates a random number $b_i \in Z_n^*$ and computes $B_i = b_iP, SK_i = h(b_iA_i) = h(a_ib_iP), V_i = h(SK_i \parallel SK_{i-1})$, then FA sends $M_2 = \{B_i, V_i\}$ back to MU.

Step 3. When getting M_2, MU calculates $SK_i = h(a_iB_i) = h(a_ib_iP)$ and checks $V_i ?= h(SK_i \parallel SK_{i-1})$. If the two values are equal, the MU replaces SK_{i-1} with SK_i.

5 Security analysis of our proposed scheme

This section first gives a formal proof using the BAN logic [54] and Proverif tool [55], and then provides an informal security analysis of the proposed scheme.

The significance of formal proof is to prove the security of the scheme logically, while the significance of informal security analysis is that some flaws cannot be discovered by formal security. Hence, the informal(traditional) analysis can be regarded as beneficial supplement to formal proof in terms of the aspect of security analysis.

5.1 Formal security analysis

We will provide a formal security proof with the BAN logic [54], which can prove whether a protocol can reach the target and help with the further improvement of the protocol.

To implement the BAN logic usually need to complete four steps: idealize the proposed scheme, make assumption, setting goal and analysis of the protocol. Table 2 lists the notations used in BAN logic.

(1) The idealized form of the messages:

$M_1.MU \rightarrow FA : \langle PID_{MU}, n_{HA}\rangle_{h(x)}, (ID_{FA}, ID_{HA}, A_1)_{Q_{MU}}$

$M_2.FA \rightarrow HA : \langle PID_{MU}, n_{HA}\rangle_{h(x)}, (ID_{FA}, ID_{HA}, A_1)_{Q_{MU}}, \{\langle PID_{MU}, n_{HA}\rangle_{h(x)}, (ID_{FA}, ID_{HA}, A_1)_{Q_{MU}}, B_1\}_{K_{FH}}$

$M_3.HA \rightarrow FA : (A_1, B_1, ID_{FA}, ID_{HA}, \langle DID_{MU}^{new}\rangle_{Q_{MU}}, (A_1, B_1, DID_{MU}^{new})_{Q_{MU}}, MU \overset{A_1}{\longleftrightarrow} FA)_{K_{FH}}, \langle DID_{MU}^{new}\rangle_{h(Q_{MU})}, (A_1, B_1, DID_{MU}^{new})_{Q_{MU}}$

$M_4.FA \rightarrow MU :$
$\langle DID_{MU}^{new}\rangle_{Q_{MU}}, (A_1, B_1, DID_{MU}^{new}, MU \overset{B_1}{\longleftrightarrow} FA)_{Q_{MU}}, (\langle DID_{MU}^{new}\rangle_{Q_{MU}}, (A_1, B_1, DID_{MU}^{new})_{Q_{MU}}, MU \overset{SK}{\longleftrightarrow} FA)_{SK}$

(2) Initiative premises:

$A_1 : MU \mid\equiv \#(a)$. $A_2 : FA \mid\equiv \#(b)$.

$A_3 : FA \mid\equiv FA \overset{K_{FH}}{\longleftrightarrow} HA$. $A_4 : MU \mid\equiv MU \overset{Q_{MU}}{\longleftrightarrow} HA$.

$A_5 : FA \mid\equiv HA \Rightarrow MU \overset{A_1}{\longleftrightarrow} FA$.

$A_6 : MU \mid\equiv HA \Rightarrow MU \overset{B_1}{\longleftrightarrow} FA$.

$A_7 : FA \mid\equiv MU \Rightarrow a$.

(3) Establishment of security goals:

$G_1 : MU \mid\equiv MU \overset{SK}{\longleftrightarrow} FA$

$G_2 : FA \mid\equiv MU \overset{SK}{\longleftrightarrow} FA$

$G_3 : MU \mid\equiv FA \mid\equiv MU \overset{SK}{\longleftrightarrow} FA$

$G_4 : FA \mid\equiv MU \mid\equiv MU \overset{SK}{\longleftrightarrow} FA$

(4) Scheme analysis:

From M_3, we have

$S_1 : FA \triangleleft (A_1, B_1, ID_{FA}, ID_{HA}, \langle DID_{MU}^{new}\rangle_{Q_{MU}}, (A_1, B_1, DID_{MU}^{new})_{Q_{MU}}, MU \overset{A_1}{\longleftrightarrow} FA)_{K_{FH}}$

From S_1 and A_3 and message-meaning rule, we have:

$S_2 : FA \mid\equiv HA \mid\sim (A_1, B_1, ID_{FA}, ID_{HA}, \langle DID_{MU}^{new}\rangle_{Q_{MU}}, (A_1, B_1, DID_{MU}^{new})_{Q_{MU}}, MU \overset{A_1}{\longleftrightarrow} FA)_{K_{FH}}$

From S_2 and A_2 and the freshness conjuncatenation rule, we have

$S_3 : FA \mid\equiv HA \mid\equiv (A_1, B_1, ID_{FA}, ID_{HA}, \langle DID_{MU}^{new}\rangle_{Q_{MU}}, (A_1, B_1, DID_{MU}^{new})_{Q_{MU}}, MU \overset{A_1}{\longleftrightarrow} FA)_{K_{FH}}$

Table 2 Notations of BAN logic

Notations	Description
$P \mid\equiv X$	The principal P believes the statement X
$\#(X)$	The message X is fresh
$P \Rightarrow X$	P has jurisdiction over the statement X
$P \overset{K}{\longleftrightarrow} Q$	K is a shared key between P and Q
$P \triangleleft X$	P sees the statement X
$P \mid\sim X$	P once said the statement X
$\{X\}_K$	The formula X encrypted under K
$(X)_K$	The formula X hashed under the key K
$\langle X\rangle_Y$	The formula X combined with the key Y

Fig. 7 Definitions

```
(*———channels————-*)
free ch1:   channel.
free ch2:   channel.
free sch:   channel [private].
(*——-shared keys———*)
free SKMU:   bitstring [private].
free SKFA:   bitstring [private].
(*—–constants—–*)
free x: bitstring [private].
free IDMU: bitstring [private].
free PWMU: bitstring [private].
free KFH: bitstring [private].
free IDFA: bitstring.
free IDHA: bitstring.
const P: bitstring.
(*—functions,reductions and equations—-*)
fun h(bitstring): bitstring.
fun mul(bitstring,bitstring): bitstring.
fun add(bitstring,bitstring):   bitstring.
fun xor(bitstring,bitstring): bitstring.
fun con(bitstring): bitstring.
fun senc(bitstring,bitstring): bitstring.
fun f(bitstring): bitstring.
reduc forall m: bitstring, n: bitstring; sdec(senc(m,n),n)=m.
equation forall m: bitstring,n: bitstring; xor(xor(m,n),n)=m.
equation forall m: bitstring,n: bitstring; mul(m,mul(n,P)) = mul(n,mul(m,P)).
(*————events————-*)
event MUStart(bitstring).
event MUAuth(bitstring).
event FAStart(bitstring).
event FAAuth(bitstring).
(*————-queries————*)
query attacker(SKMU).
query attacker(SKFA).
query attacker(IDMU).
query attacker(PWMU).
query id: bitstring; inj-event(MUAuth(id)) ==> inj-event(MUStart(id)).
query id: bitstring; inj-event(FAAuth(id)) ==> inj-event(FAStart(id)).
```

From S_3 and the belief rule, we have

$S_4 : FA \mid\equiv HA \mid\equiv MU \overset{A_1}{\longleftrightarrow} FA$

From S_4 and A_5 and the jurisdiction rule, we have

$S_5 : FA \mid\equiv MU \overset{A_1}{\longleftrightarrow} FA$

According to S_5 and $SK = h(bA_1) = h(aB_1) = h(abP)$, we have

$S_6 : FA \mid\equiv MU \overset{SK}{\longleftrightarrow} FA \qquad (G_2)$

From M_4, we have

$S_7 : MU \triangleleft (A_1, B_1, DID_{MU}^{new}, MU \overset{B_1}{\longleftrightarrow} FA)_{Q_{MU}}$

From S_1 and A_4 and message-meaning rule, we have:

$S_8 : MU \mid\equiv HA \mid\sim (A_1, B_1, DID_{MU}^{new}, MU \overset{B_1}{\longleftrightarrow} FA)_{Q_{MU}}$

From S_8 and A_1 and the freshness conjuncatenation rule, we have

$S_9 : MU \mid\equiv HA \mid\equiv (A_1, B_1, DID_{MU}^{new}, MU \overset{B_1}{\longleftrightarrow} FA)_{Q_{MU}}$

From S_9 and the belief rule, we have

$S_{10} : MU \mid\equiv HA \mid\equiv MU \overset{B_1}{\longleftrightarrow} FA$

From S_{10} and A_6 and the jurisdiction rule, we have

$S_{11} : MU \mid\equiv MU \overset{B_1}{\longleftrightarrow} FA$

According to S_{11} and $SK = h(aB_1) = h(bA_1) = h(abP)$, we have

$S_{12} : MU \mid\equiv MU \overset{SK}{\longleftrightarrow} FA \qquad (G_1)$

From M_4, we have

$S_{13} : MU \triangleleft (\langle DID_{MU}^{new} \rangle_{Q_{MU}}, (A_1, B_1, DID_{MU}^{new})_{Q_{MU}}, MU \overset{SK}{\longleftrightarrow} FA)_{SK}$

From S_{11} and S_{13} and the message-meaning rule, we have

$S_{14} : MU \mid\equiv FA \mid\sim (\langle DID_{MU}^{new} \rangle_{Q_{MU}}, (A_1, B_1, DID_{MU}^{new})_{Q_{MU}}, MU \overset{SK}{\longleftrightarrow} FA)_{SK}$

From S_{14} and A_1 and the freshness conjuncatenation rule, we have

$S_{15} : MU \mid\equiv FA \mid\equiv (\langle DID_{MU}^{new} \rangle_{Q_{MU}}, (A_1, B_1, DID_{MU}^{new})_{Q_{MU}}, MU \overset{SK}{\longleftrightarrow} FA)_{SK}$

From S_{15} and the belief rule, we have

$S_{16} : MU \mid\equiv FA \mid\equiv MU \overset{SK}{\longleftrightarrow} FA \qquad (G_3)$

According S_9 and A_6 and belief rule, we have

$S_{17} : FA \mid\equiv MU \mid\equiv B_1$

From A_7 and $SK = h(aB_1) = h(abP)$, we have

$S_{18} : FA \mid\equiv MU \mid\equiv SK$

From S_6 and S_{18}, we have

$S_{19} : FA \mid\equiv MU \mid\equiv MU \overset{SK}{\longleftrightarrow} FA \qquad (G_4)$

5.2 Security analysis with ProVerif

ProVerif is a popular and powerful formal protocol analysis tool that can automatically analyze protocols based on imported PV files. If the protocol has vulnerabilities, then the ProVerif tool obtains test result and a corresponding attack sequence. We will formally verify our protocol using the latest version of ProVerif tool (Ver2.00). A brief description of the code is provided as follows:

First, the used components, such as communication channels, shared keys, constants, function and equations, events, and queries, are defined in Fig. 7. Our verification code has four events and six queries. The four events are used to verify the authentication property of the *MU* and the *FA*. The first two queries are used to verify the secrecy of the session key. The middle two queries are used to test the security of the identity and password of the *MU*. The last two queries are used to test whether the events occur correctly. The processes of the *MU*, *FA*, and *HA* are illustrated in Figs. 8, 9 and 10, respectively. We execute all the codes using the instruction "*process* !*MU*| !*HA*| !*FA*". The execution results of the ProVerif tool only have two states: true and false. Any proposition must be either true or false. A true result indicates that the protocol has required an authentication property, whereas a false result means the protocol has vulnerabilities. Figure 11 shows the verification results of queries and events. As shown in the picture, all output results of the six queries are true. Therefore, the session key and privacy information of the *MU* are safe against a network attack. The first two results demonstrate that the adversary cannot obtain the shared session key. The third and fourth results demonstrate that the identity and password of the *MU* is secure. The last two results demonstrate that the events about the *MU* and the *FA* are started and terminated in the right order. Figure 12 shows the whole workflow of the ProVerif algorithms and the four dotted lines at the top indicates the flow of data. The authentication data set out from *MU* and return to *MU*.

5.3 Informal security analysis

We will show that the proposed scheme can overcome the defect of the original scheme and satisfy all the secure requirements.

5.3.1 User anonymity and untraceability

The real identity of the *MU* is included in DID_{MU} and A_2. The acquisition of hash value A_2 is an one-way process from which we cannot get the original string back. In addition, the adversary cannot obtain ID_{MU} by computing DID_{MU} without the secret key x and random number n_{HA} of *HA*. Our scheme also supports user untraceability because every login request message and response message contain a randomly selected number. As such, the communication messages $\{M_1, M_2, M_3, M_4\}$ are different every time and unlinkable. This unlinkability is the property that makes the attacker unable to trace user's moving history. Hence,

Fig. 8 Process of *MU*

```
let MU =
    new r: bitstring;
    let HPWMU = h(con((PWMU, r))) in
    out(sch, (IDMU, HPWMU));
    in(sch, (xDIDMU:bitstring, xQMU:bitstring));
    let rm = xor(h(con((IDMU, PWMU))), r) in
    let VMU = h(con((IDMU, PWMU, r))) in
    let mQMU = xor(xQMU, rm) in
    !(
        event MUStart(IDMU);
        new Tseed: bitstring;
        let r' = xor(h(con((IDMU, PWMU))), rm) in
        let PIDMU = h(con((IDMU, h(con((PWMU, r')))))) in
        let QMU = xor(mQMU, r') in
        let a = f(Tseed) in
        let A1 = mul(a, P) in
        let A2 = h(con((xDIDMU, QMU, A1, PIDMU, IDFA, IDHA))) in
        let M1 = con((IDFA, IDHA, xDIDMU, A1, A2)) in
        out(ch1, M1);
        in(ch1, mM4:bitstring);
        let (mC1:bitstring, mC2:bitstring, mB1:bitstring, mB3:bitstring) = mM4 in
        let mDIDMUnew = xor(mC1, h(QMU)) in
        if mC2 = h(con((QMU, A1, mB1, mDIDMUnew))) then
            let SKMU = h(mul(a, mB1)) in
                if mB3 = h(con((SKMU, mC1, mC2))) then
                let xDIDMU = mDIDMUnew in
                0
    ).
```

user anonymity and untraceability can be achieved in our scheme.

5.3.2 Local password verification

In the proposed protocol, the *SC* verifies the correctness of the entered user information of the *MU* through V_{MU} before sending a login request message to the *FA*. Without correct user information, the adversary cannot generate the correct r from r^* and pass the verification, thereby resulting in the immediate termination of the login phase. Hence, the proposed scheme supports local password verification and avoids unnecessary system overhead in communication and performance.

5.3.3 Resistance to DoS attacks

As stated in Section 1.2, user anonymity and resistance to DoS attacks are mutually contradictory. Thus, we take a middle-of-the-road approach to solve this difficult problem. In the login phase, the random number a is generated by $f(ID_{MU} \| T_{seed})$, where T_{seed} is kept in a preset time threshold (e.g., T_{AUTH}). Hence, the login request message $M_1 = ID_{FA}, ID_{HA}, DID_{MU}, A_1, A_2$ does not change within this period. The *FA* can quickly find out the DoS attack through verifying the login messages sent from the *MU*s. A legal *MU* does not send numerous login request messages to the *FA*. Hence, our method does not decrease user anonymity. Above all, the proposed protocol can effectively prevent a DoS attack while protecting the *MU*'s privacy.

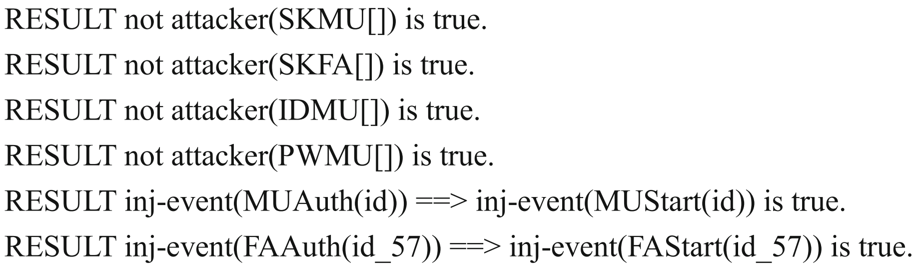
Fig. 9 Process of *FA*

```
let FA =
    in(ch1, fM1: bitstring);
    event FAStart(IDFA);
    new b: bitstring;
    let B1 = mul(b, P) in
    let B2 = h(con((fM1, B1, KFH, IDFA, IDHA))) in
    let M2 = con((fM1, B1, B2)) in
    out(ch2, M2);
    in(ch2, fM3:bitstring);
    let (fIDHA:bitstring, fIDFA:bitstring, fDIDMU:bitstring, fA1:bitstring, fA2:bitstring) = fM1 in
    let (fhA1:bitstring, fC1:bitstring, fC2:bitstring, fC3:bitstring) = fM3 in
    if fhA1 = fA1 then
        if fC3 = h(con((KFH, fA1, B1, IDFA, fIDHA, fC1, fC2))) then
            let SKFA = h(mul(b, fA1))    in
            let B3 = h(con((SKFA, fC1, fC2))) in
            let M4 = con((fC1, fC2, B1, B3)) in
            out(ch1, M4).
```

Fig. 10 Process of *HA*

```
let HAReg =
    in(sch, (hIDMU: bitstring, hHPWMU: bitstring));
    new nHA: bitstring;
    let PIDMU = h(con((hIDMU, hHPWMU))) in
    let QMU = h(con((PIDMU, x))) in
    let DIDMU = xor(h(x), con((PIDMU, nHA))) in
    out(sch, (DIDMU, QMU)).

let HAAuth =
    in(ch2, (hM2: bitstring));
    let (hM1:bitstring, hB1:bitstring, hB2:bitstring) = hM2 in
    let (hIDFA:bitstring, hIDHA:bitstring, hDIDMU:bitstring, hA1:bitstring, hA2:bitstring) = hM1 in
    if hB2 = h(con((hM1, hB1, KFH, hIDFA, IDHA))) then
        let (PIDMU': bitstring, nHA': bitstring) = xor(h(x), hDIDMU) in
        let QMU' = h(con((PIDMU', x))) in
        if hA2 = h(con((hDIDMU, QMU', hA1, PIDMU', hIDFA, IDHA))) then
            event MUAuth(PIDMU');
            event FAAuth(hIDFA);
            new nHAnew: bitstring;
            let hDIDMUnew = xor(h(x), con((PIDMU', nHAnew))) in
            let C1 = xor(h(QMU'), hDIDMUnew) in
            let C2 = h(con((QMU', hA1, hB1, hDIDMUnew))) in
            let C3 = h(con((KFH, hA1, hB1, hIDFA, IDHA, C1, C2))) in
            let M3 = con((hA1, C1, C2, C3)) in
            out(ch2, M3).
let HA = HAReg | HAAuth.
process !MU | !HA | !FA
```



```
RESULT not attacker(SKMU[]) is true.
RESULT not attacker(SKFA[]) is true.
RESULT not attacker(IDMU[]) is true.
RESULT not attacker(PWMU[]) is true.
RESULT inj-event(MUAuth(id)) ==> inj-event(MUStart(id)) is true.
RESULT inj-event(FAAuth(id_57)) ==> inj-event(FAStart(id_57)) is true.
```

Fig. 11 Results of the queries

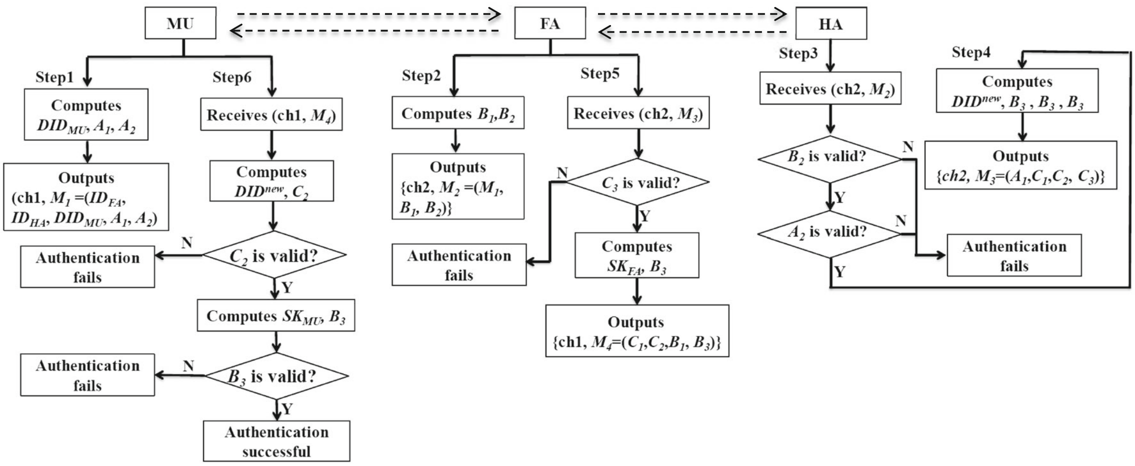


Fig. 12 The flowchart of the ProVerif algorithms

5.3.4 Resistance to impersonation attack

If an adversary wants to impersonate the *MU*, then the adversary must forge $Q_{MU} = Q^*_{MU} \oplus r$. However, the value Q_{MU} cannot be forged because it is generated by the *HA* with the secret key x and PID_{MU}. Therefore, our scheme can resist impersonation attacks. Without the secret keys K_{FH} and x, the adversary cannot forge a legal message B_2, C_1, C_2, and C_3. Therefore, impersonation attacks can be prevented in our protocol.

5.3.5 Mutual authentication

All the three entities can achieve mutual authentication through the transmitted messages. The *HA* can authenticate the *FA* by checking B_2 and the *MU* through PID_{MU}, Q_{MU}, and A_2. Similarly, the *FA* can also authenticate the *HA* directly and the *MU* indirectly by checking the hash value C_3. Lastly, the *MU* can authenticate the *HA* and the *FA* by examining C_2 and B_3, respectively.

5.3.6 Resistance to offline password guessing attacks with smart card security breach

We suppose the attacker gets $\{r^*, V_{MU}, Q^*_{MU}, DID_{MU}\}$ from the *MU*'s smart card and the transmitted messages $\{M_1, M_2, M_3, M_4\}$. The password of the *MU* is contained in $r^* = h(ID_{MU} \parallel PW_{MU}) \oplus r, V_{MU} = h(ID_{MU} \parallel PW_{MU} \parallel r)$, $Q^*_{MU} = Q_{MU} \oplus r = h(PID_{MU} \parallel x) \oplus r, DID_{MU} = h(x) \oplus (PID_{MU} \parallel n_{HA}) = h(x) \oplus (h(ID_{MU} \parallel r) \parallel n_{HA})$ and A_2. As shown in these data, the adversary cannot retrieve the PW_{MU} unless he/she has ID_{MU} and r or obtains the secret key x, which is held by the *HA*. Hence, our scheme can prevent this type of guessing attack.

5.3.7 Resistance to replay attack

The numbers a and b in our scheme are individually chosen by the *MU* and the *FA* for each login and authentication. Thus, the transmitted messages constantly change in different sessions. If the adversary replays the eavesdropped messages, such as M_1, M_2, M_3, and M_4, then the *MU*, the

Table 3 Functionality comparison

	Arshad [50]	Fraz [28]	Wu [24]	Karuppiah [19]	Wu [33]	Karuppiah [18]	Li [46]	Xie [47]	Our scheme
P1	YES	NO	YES	YES	YES	YES	YES	YES	YES
P2	NO	YES	NO	YES	NO	YES	YES	NO	YES
P3	NO	YES	NO	NO	NO	NO	NO	NO	YES
P4	YES	YES	YES	YES	YES	YES	NO	YES	YES
P5	YES	YES	YES	YES	YES	YES	NO	YES	YES
P6	YES	NO	YES	YES	YES	YES	YES	YES	YES
P7	YES	NO	YES	YES	YES	YES	YES	YES	YES
P8	YES	YES	YES	YES	YES	YES	YES	YES	YES
P9	YES	YES	YES	YES	YES	NO	YES	YES	YES
P10	YES	YES	YES	YES	YES	YES	YES	YES	YES
P11	NO	NO	NO	NO	NO	NO	NO	NO	YES
P12	NO	NO	NO	NO	NO	NO	YES	NO	YES
P13	YES	YES	YES	YES	YES	YES	YES	YES	YES

P1: User anonymity and un-traceability
P2: Local password verfication
P3: Resistant to the DoS attack
P4: Resistant to the impersonation attack
P5: Mutual authentication
P6: Resistance to off-line password guessing attack with smart card security breach
P7: Resistant to the replay attack
P8: Resist insider attack
P9: Strong forward secrecy
P10: Fair key agreement
P11: Support the concurrent visit by many *MU*s
P12: Session key update
P13: Password update freely

FA, and the *HA* can easily detect this type of attack by comparing the received messages with the old messages.

5.3.8 Resistance to insider attack

In the registration phase, *MU* computes $PID_{MU} = h(ID_{MU} \| r)$ and submits $\{ID_{MU}, PID_{MU}\}$ to the *HA*. The password PW_{MU} of the *MU* is never sent to the *HA*. Evidently, a malicious insider user won't get PW_{MU} and the proposed scheme is secure against this kind of attack.

5.3.9 Strong forward secrecy

Assume that an adversary obtains the previous session keys and retrieves the data in the smart card and long-term secret information of the *MU* and the *HA*, such as *x*. The adversary still cannot generate the current session key $SK_{MU}(SK_{FA})$ because it contains one-time random nonce *a* and *b*. The current session key cannot be linked with previous session keys or any other secret data. Thus, the improved protocol achieves strong forward secrecy.

Table 4 Time cost of related operations (ms)

Operations	Time
T_H	0.0023
T_{SE}	0.0046
T_M	2.226
T_{EXP}	3.85

5.3.10 Fair key agreement

The shared session key in our scheme is $SK_{MU} = SK_{FA} = h(abP)$, which is composed of two numbers and a public parameter *P*. The two numbers are generated by the *MU* and the *FA* independently. Hence, our scheme achieves fair key agreement.

Table 5 The comparisons of computation cost (ms)

Scheme	Login and authentication phase	Total
Arshad [50]	$18T_H + 5T_{SE} + 4T_M$	8.91044
Fraz [28]	$12T_H$	0.00276
Wu [24]	$34T_H + 2T_{SE} + 4T_M$	8.91274
Karuppiah [19]	$21T_H + 6T_{SE} + 3T_{EXP}$	11.55759
Wu [33]	$30T_H + 4T_M$	8.9109
Karuppiah [18]	$24T_H + 2T_{SE} + 3T_{EXP}$	11.55644
Li [46]	$17T_H + 6T_M$	13.35991
Xie [47]	$17T_H + 6T_M$	13.35991
Our scheme	$20T_H + 4T_M$	8.9086

5.3.11 Support the concurrent visit through many *MU*s

When numerous *MU*s from the same *HA* visits an *FA* in a short period, the visited *FA* receives numerous reply messages sent by the *HA*. Hence, we must take effective measures to help the *FA* match the reply messages with the *MU*s; otherwise, login and authentication end during the *FA* verification. In our improved scheme, each reply message from the *HA* to the *FA* contains value A_1, which is generated by the *MU*. Hence, the *FA* can easily map every received message to every visited *MU*. Therefore, our scheme can cope with this issue.

5.3.12 Session key update regularly

If an *MU* stays in the network coverage of an *FA* for a long period, then the *MU* and the *FA* should update the shared session key periodically in case of potential network attacks and sensitive information leaks. The proposed scheme provides an efficient method to update the shared session key between the *MU* and the *FA* by taking advantage of previous session key and randomly chosen numbers.

5.3.13 Password update freely

Given people's limited memory, the password chosen by the *MU* is usually short and easily remembered. Such password is vulnerable to brute force password attacks. In the proposed scheme, the password of the *MU* can be changed freely, thereby providing users with safe network services.

6 Functional and performance comparison

In this section, we analyze the functionality and give the performance comparison of the proposed scheme with recently works.

6.1 Functional analysis

The results of functionality comparisons are listed in the Table 3. As shown in the table, the new protocol satisfies all functionality requirements and more secure than other schemes.

6.2 Performance analysis

We provide a simple performance comparison of the new protocol with those of other studies.

Some notations used to evaluate the performance are listed as follows:

- T_H: The time for a one-way hash operation.
- T_{SE}: The time for a symmetric encryption/decryption.
- T_M: The time for a multiplication operation in ECC.
- T_{EXP}: The time for a modular exponent.

Table 4 shows the execution time of the related operations following [56], which provides the computation cost of common operation and algorithm, such as hash, encryption/decryption, elliptic curve cryptography (ECC), and modular exponent. These results are to be achieved by using Pairing-Based Cryptography (PBC) library, as well as RSA and AES algorithm etc. The computer (Intel CPU E2200 2.20 GHz, 2 GB of RAM) used in [56] is not up-to-date, but all the results are obtained under the same test condition. Thus, these data are sufficient for comparison between different schemes.

Table 5 presents the performance comparison result between our scheme and those of other relevant studies. The table indicates that the new scheme has a lower computation cost compared with all other schemes, except for the scheme in [28]. However, the scheme in [28] has many security weaknesses, such as no resistance to replay attack and poor user anonymity.

7 Conclusion

In this study, we initially present a brief introduction of authentication protocols in smart cities based on GLOMONETs. Then, we summarize and analyze the contradictory relationships between user anonymity and DoS attack resistance. We find that many recent studies can achieve user anonymity, but they are vulnerable to DoS attacks. We analyze the security weaknesses of a recent authentication scheme and propose an improved one that balances DoS attack resistance and user anonymity to some extent. Results of security analyses and performance comparison illustrate that the improved scheme is secure and also meets all known security requirements. Furthermore, the proposed scheme has higher execution efficiency compared other schemes. It also has remarkable application potential to smart cities.

Acknowledgements This work was supported in part by the General Project of Education Department in Sichuan under Grants 18ZB0485.

References

1. Farooq, M. U., Waseem, M., Qadri, M. T., & Waqar, M. (2016). Understanding 5g wireless cellular network: Challenges, emerging research directions and enabling technologies. *Wireless Personal Communications, 95*(2), 261–285.
2. Akpakwu, G., Silva, B., Hancke, G. P., & Abu-Mahfouz, A. M. (2017). A survey on 5g networks for the internet of things: Communication technologies and challenges. *IEEE Access, 5*(12), 3619–3647.
3. Lynggaard, P., & Skouby, K. E. (2015). Deploying 5g-technologies in smart city and smart home wireless sensor networks with interferences. *Wireless Personal Communications, 81*(4), 1399–1413.
4. He, D., Chen, C., Bu, J., Chan, S., & Yan, Z. (2013). Security and efficiency in roaming services for wireless networks: Challenges, approaches, and prospects. *Communications Magazine IEEE, 51*(2), 142–150.
5. Zhu, J., & Ma, J. (2004). A new authentication scheme with anonymity for wireless environments. *IEEE Transactions on Consumer Electronics, 51*(21), 231–235.
6. He, D., Chan, S., Chen, C., Bu, J., & Fan, R. (2011). Design and validation of an efficient authentication scheme with anonymity for roaming service in global mobility networks. *Wireless Personal Communications, 61*(2), 465–476.
7. Jiang, Q., Ma, J., Li, G., & Yang, L. (2013). An enhanced authentication scheme with privacy preservation for roaming service in global mobility networks. *Wireless Personal Communications, 68*(4), 1477–1491.
8. Wen, F., Susilo, W., & Yang, G. (2014). A secure and effective anonymous user authentication scheme for roaming service in global mobility networks. *Wireless Personal Communications, 78*(1), 247–269.
9. Farash, M. S., Chaudhry, S. A., Heydari, M., Sadough, S. M. S., Kumari, S., & Khan, M. K. (2015). A lightweight anonymous authentication scheme for consumer roaming in ubiquitous networks with provable security. *International Journal of Communication Systems, 30*(4), e3019.
10. Gope, P., & Hwang, T. (2015). Enhanced secure mutual authentication and key agreement scheme preserving user anonymity in global mobile networks. *Wireless Personal Communications, 82*(4), 2231–2245.
11. Chung, Y., Choi, S., Lee, Y., Park, N., & Won, D. (2016). An enhanced lightweight anonymous authentication scheme for a scalable localization roaming service in wireless sensor networks. *Sensors, 16*(10), 1653.
12. Karuppiah, M., Kumari, S., Das, A. K., Li, X., Wu, F., & Basu, S. (2016). A secure lightweight authentication scheme with user anonymity for roaming service in ubiquitous networks. *Security & Communication Networks, 9*(17), 4192–4209.
13. Zhao, D., Peng, H., Li, L., & Yang, Y. (2014). A secure and effective anonymous authentication scheme for roaming service in global mobility networks. *Wireless Personal Communications, 78*(1), 247–269.
14. Mun, H., Han, K., Lee, Y. S., Yeun, C. Y., & Choi, H. H. (2012). Enhanced secure anonymous authentication scheme for roaming service in global mobility networks. *Mathematical & Computer Modelling, 55*(1–2), 214–222.
15. Wen, F., Susilo, W., & Yang, G. (2014). A robust smart card-based anonymous user authentication protocol for wireless communications. *Security & Communication Networks, 7*(6), 987–993.
16. Das, A. K. (2013). A secure and effective user authentication and privacy preserving protocol with smart cards for wireless communications. *Networking Science, 2*(1–2), 12–27.
17. Kang, M., Rhee, H. S., & Choi, J. .-Y. (2011). Improved user authentication scheme with user anonymity for wireless communications. *IEICE Transactions on Fundamentals of Electronics Communications & Computer Sciences, E94–A*(2), 860–864.
18. Karuppiah, M., & Saravanan, R. (2015). A secure authentication scheme with user anonymity for roaming service in global mobility networks. *Wireless Personal Communications, 84*(3), 2055–2078.
19. Karuppiah, M., Kumari, S., Li, X., Wu, F., Das, A. K., Khan, M. K., Saravanan, R., & Basu, S. (2017). A dynamic id-based generic framework for anonymous authentication scheme for roaming service in global mobility networks. *Wireless Personal Communications An International Journal, 93*(2), 383–407.
20. Gope, P., & Hwang, T. (2016). Lightweight and energy-efficient mutual authentication and key agreement scheme with user anonymity for secure communication in global mobility networks. *IEEE Systems Journal, 10*(4), 1370–1379.
21. Zhou, T., & Xu, J. (2011). Provable secure authentication protocol with anonymity for roaming service in global mobility networks. *Computer Networks, 55*(1), 205–213.
22. Gope, P., & Hwang, T. (2016). An efficient mutual authentication and key agreement scheme preserving strong anonymity of the mobile user in global mobility networks. *Journal of Network & Computer Applications, 62*(C), 1–8.
23. He, D., Ma, M., Zhang, Y., Chen, C., & Bu, J. (2011). A strong user authentication scheme with smart cards for wireless communications. *Computer Communications, 34*(3), 367–374.
24. Wu, F., Xu, L., Kumari, S., Li, X., Das, A. K., Khan, M. K., Karuppiah, M., & Baliyan, R. (2016). A novel and provably secure authentication and key agreement scheme with user anonymity for global mobility networks. *Security & Communication Networks, 9*(16), 3527–3542.
25. Xu, G., Liu, J., Lu, Y., Zeng, X., Zhang, Y., & Li, X. (2018). A novel efficient maka protocol with desynchronization for anonymous roaming service in global mobility networks. *Journal of Network and Computer Application, 107*, 83–92.
26. Chaudhry, S. A., Albeshri, A., Xiong, N., Lee, C., & Shon, T. (2017). A privacy preserving authentication scheme for roaming in ubiquitous networks. *Cluster Computing, 20*(2), 1223–1236.
27. Lee, H., Lee, D., Moon, J., Jung, J., Kang, D., Kim, H., & Won, D. (2018). An improved anonymous authentication scheme for roaming in ubiquitous networks. *Plos One, 13*(3), e0193366.
28. Fraz, B. A., ul, H. K. M., Anwar, G., Ashraf, C. S., Imran, K., Usman, A. M., & Khurram, K. M. (2018). A lightweight and secure two factor anonymous authentication protocol for global mobility networks. *Plos One, 13*(4), e0196061.
29. Lee, C. C., Lai, Y. M., Chen, C. T., & Chen, S. D. (2016). Advanced secure anonymous authentication scheme for roaming service in global mobility networks. *Wireless Personal Communications, 94*(3), 1–16.
30. Chen, R., & Peng, D. (2017). An anonymous authentication scheme with the enhanced security for wireless communications. *Wireless Personal Communications, 97*, 2665–2682.
31. Niu, J., & Li, X. (2012). A novel user authentication scheme with anonymity for wireless communications. *Security & Communication Networks, 7*(10), 1467–1476.

32. Madhusudhan, R., & Shashidhara. (2018). A secure and lightweight authentication scheme for roaming service in global mobile networks. *Journal of Information Security & Applications, 38*, 96–110.
33. Wu, F., Li, X., Xu, L., Kumari, S., & Sangaiah, A. K. (2018). A novel mutual authentication scheme with formal proof for smart healthcare systems under global mobility networks notion. *Computers & Electrical Engineering, 68*, 107–118.
34. Li, J., Zhang, Z., Hui, L., & Zhou, Z. (2020). A novel message authentication scheme with absolute privacy for the internet of things networks. *IEEE Access, 8*, 39689–39699.
35. Aydin, Y., Kurt, G. K., Ozdemir, E., & Yanikomeroglu, H. (2020). A flexible and lightweight group authentication scheme. *IEEE Internet of Things Journal, 7*(10), 10277–10287.
36. Kumar, M. R., & Parthasarathy, V. (2020). A secure fuzzy extractor based biometric key authentication scheme for body sensor network in internet of medical things. *Computer Communications, 153*, 545–552.
37. Deebak, B. D., & Al-Turjman, F. (2020). Smart mutual authentication protocol for cloud based medical healthcare systems using internet of medical things. *IEEE Journal on Selected Areas in Communications, 39*(2), 346–360.
38. Ying, Z., Chiou, S. Y., & Liu, J. (2016). Improvement of a privacy authentication scheme based on cloud for medical environment. *Journal of Medical Systems, 40*(4), 1–15.
39. Jangirala, S., Das, A. K., Wazid, M., & Vasilakos, A. V. (2020). Designing secure user authentication protocol for big data collection in IoT-based intelligent transportation system. *IEEE Internet of Things Journal, 8*(9), 7727–7744.
40. Bansal, G., Chamola, V., Kumar, N., Guizani, M., & Sikdar, B. (2020). Lightweight mutual authentication protocol for v2g using physical unclonable function. *IEEE Transactions on Vehicular Technology, 69*(7), 7234–7246.
41. Alladi, Tejasvi, Naren, Gaurang Bansal, Chamola, Vinay, & Guizani, Mohsen. (2020). Secauthuav: A novel authentication scheme for UAV-ground station and UAV-UAV communication. *IEEE Transactions on Vehicular Technology, 69*(12), 15068–15077.
42. Alladi, T., Chamola, V., Naren, & Kumar, N. (2020). Parth: A two-stage lightweight mutual authentication protocol for UAV surveillance networks. *Computer Communications, 160,* 81–90.
43. Alladi, T., Naren, N., & Chamola, V. (2020). Harci: A two-way authentication protocol for three entity healthcare IoT networks. *IEEE Journal on Selected Areas in Communications, 39*(2), 361–369.
44. Adu-Gyamfi, D., Zhang, F., & Takyi, A. (2021). Anonymising group data sharing in opportunistic mobile social networks. *Wireless Networks, 27*(3), 1477–1490.
45. Wang, D., & Wang, P. (2014). On the anonymity of two-factor authentication schemes for wireless sensor networks: Attacks, principle and solutions. *Computer Networks, 73*(C), 41–57.
46. Xiong, L., Sangaiah, A. K., Kumari, S., Fan, W., & Khan, M. K. (2017). An efficient authentication and key agreement scheme with user anonymity for roaming service in smart city. *Personal & Ubiquitous Computing, 21*(12), 1–15.
47. Hwang, L., & Xie, Q. (2019). Security enhancement of an anonymous roaming authentication scheme with two-factor security in smart city. *Neurocomputing, 347*(28), 131–138.
48. Gope, P., Islam, S. H., Obaidat, M. S., Amin, R., & Vijayakumar, P. (2017). Anonymous and expeditious mobile user authentication scheme for glomonet environments. *International Journal of Communication Systems, 31*(2), e3461.
49. Gope, P. (2016). Energy efficient mutual authentication and key agreement scheme with strong anonymity support for secure ubiquitious roaming services. In *11th International conference on availability, reliability and security (ARES)* (pp.247–252).
50. Arshad, H., & Rasoolzadegan, A. (2017). A secure authentication and key agreement scheme for roaming service with user anonymity. *International Journal of Communication Systems, 30*(18), e3361.
51. Hu, B., Xie, Q., Bao, M., & Dong, N. (2014). Improvement of user authentication protocol with anonymity for wireless communications. *Kuwait Journal of Science, 41*(1), 155–169.
52. He, D., Chen, C., Chan, S., & Bu, J. (2013). Strong roaming authentication technique for wireless and mobile networks. *International Journal of Communication Systems, 26*(8), 1028–1037.
53. Juels, A., & Brainard, J. (1999). Client puzzles: a cryptographic countermeasure against connection depletion attacks. In: *Proceedings of the Network and Distributed System Security Symposium, NDSS 1999* (pp. 151–165). San Diego, California, USA.
54. Burrows, M., Abadi, M., & Needham, R. (1990). A logic of authentication. *ACM Transactions on Computer Systems, 8*(1), 18–36.
55. Abadi, M., Blanchet, B., & Comon-Lundh, H. (2009). Models and proofs of protocol security: A progress report. In: *Computer Aided Verification, 21st International Conference, CAV 2009* (pp. 35–49), Grenoble, France.
56. Kilinc, H. H., & Yanik, T. (2014). A survey of sip authentication and key agreement schemes. *IEEE Communications Surveys & Tutorials, 16*(2), 1005–1023.

Rui Chen received the Ph.D. degree in computer science and technology from Sichuan University in 2018, Chengdu, P. R. China. Now he is an associate professor of the College of Computer Science, Sichuan Normal University, Chengdu, P. R. China. His current interests include design and analysis of security protocols and handover authentication of wireless network etc.

Yongcong Mou received the M.S. degree in operational research and cybernetics from Sichuan Normal University in 2011. Now she is an lecturer of the Sichuan Water Conservancy Vocational College, Chengdu, P. R. China. Her current interests include analysis and prove of security protocols etc.

Min Zhang received Ph.D. degree in Sichuan Province Key Lab of Signal and Information Processing at Southwest JiaoTong University, Chengdu, P. R. China. His research focuses on Network & Information security and authentication protocol etc.