Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 5426288, 9 pages
https://doi.org/10.1155/2022/5426288

Research Article

A Secured and Efficient Anonymous Roaming Scheme of Mobile Internet

Yao Cheng,[1] **Li Yue**,[1] **Naixia Duan**,[1] **and Chenglong Li**[2]

[1]*School of Information Engineering, Shaanxi Institute of International Trade & Commerce, Xi'an 712046, China*
[2]*School of Computer Science and Technology, Shandong Jianzhu University, Jinan 250000, China*

Correspondence should be addressed to Chenglong Li; chenglongli_sdu@163.com

Received 9 December 2021; Accepted 14 February 2022; Published 9 March 2022

Academic Editor: Xingsi Xue

An anonymous roaming scheme of mobile Internet was discussed in this paper aiming to improve the traditional authentication protocol that cannot satisfy the demand of user's identity authentication when the mobile terminal is roaming in mobile Internet. The authentication server of remote network will complete the identity legitimacy verification of mobile terminal with the help of the home network authentication server. A temporary identity is used to prevent user's anonymity protection from being tracked and eavesdropped, as well as other attacks, which can improve the confidential of user's identity and location considerably. This anonymous roaming scheme can achieve a high-level of safety efficiently. This will also satisfy the development of the network technology.

1. Introduction

The Internet of Things (IoT) realizes the ubiquitous connection between Things and Things, and between Things and people, and realizes the intelligent perception, recognition, and management of objects and processes. That is, IoT is an information carrier based on the Internet, which enables all objects that can be independently addressed to form an interconnected network.

With the rapid development of information network technology, the evolution of internet from wireless Internet to wireless mobile Internet has made the latter a development trend of the next generation network. Mobile Internet has the characteristics of dynamic topology, open link, and limited bandwidth. However, these features make it easier to intercept and monitor messages, and the mobile Internet faces security threats such as eavesdropping and replaying attacks; so, authenticating through a security portal becomes the top priority. Also, for IoT, the anonymous roaming authentication mechanism is a key technology to ensure communication security.

In the case of authentication server in the mobile Internet, the service is hoped to be provided to the legitimate users or the completely trusted users. The authentication protocol enables the authentication server and the mobile terminal (mobile terminal, MT) to realize a two-way anonymous authentication. To ensure the legitimacy of MT identity, for example, in [1], an anonymous identity authentication and key agreement scheme for global mobility network is proposed to realize mutual anonymous authentication between the two parties. In [2], a wireless anonymous authentication protocol is proposed to avoid the risk of using the same key for a long time. In [3], an identity-based anonymous wireless authentication scheme is proposed to solve the authentication problem of mobile users while roaming, and the security and anonymity of the scheme are analyzed in detail by using the characteristics of bilinear pairs and elliptic curves. In [4], to reduce message flows of traditional anonymous authentication schemes, a new kind of delegation-based scheme is proposed for wireless roaming networks. In [5], an improved secure anonymous authentication scheme using shared secret keys between home agent and foreign agent was proposed. A broadcast authentication protocol for smart grid communications was created in [6], and the security of proposed scheme was proved with the formal method. In [7], an

improved lightweight authentication protocol for wireless body area networks was created, and the security of the above scheme was proved in the random oracle. In the past few years, many constructions on the roaming authentication were created [8–14].

However, the partial roaming authentication protocol [1, 2] only completes the authentication between the authentication server and the MT for local communication. When MT roams away from the local network to enter the remote network, two-way anonymous authentication between MT and remote network authentication server cannot be realized. Although part of roaming authentication protocol [3–5] can satisfy the requirement of MT identity legitimacy authentication while roaming, the large amount of computation will result in a low efficiency. At the same time, MT will repeatedly apply for service after entering the remote network. Frequent authentication will increase the execution load of MT, reduce the efficiency of roaming mechanism, and threaten the security of privacy information such as MT identity.

In view of the above shortcomings of roaming authentication protocol, this paper proposes an anonymous roaming mechanism for mobile Internet. In this mechanism, when MT roams into a remote network, the remote network authentication server will be assisted by its local network authentication server. Simultaneously, the security of MT privacy information will be guaranteed. The remote authentication server issues roaming certificate for authenticated MT. MT can repeatedly apply for roaming service to remote network during the validity period of the certificate. Based on roaming certificate, remote authentication server can verify the identity of MT. The use of certificate improves the efficiency of the mechanism and reduces the computing load of mobile terminal.

The main innovation of this paper is its verification of the identity legitimacy of MT in roaming process, meanwhile ensuring the anonymity of MT identity, which improves the process's security and efficiency together, and makes up for the deficiency of traditional authentication protocol in identity anonymity and work efficiency while the MT is roaming.

2. Anonymous Roaming Mechanism of Mobile Internet

The mobile Internet is mainly composed of MT, home network authentication server (home network authentication server, hs), and remote network authentication server (remote network authentication server, rs). At the same time, it also includes the mobile Internet management center (management center, mc). The frame structure is shown in Figure 1.

The relevant variables and operations used in this paper are defined as follows:

ID_A is the identity or related network label of A; TID_A is the temporary identity generated by the home authentication server HS for A; Num_A is the random secret number selected by A; S is the secret number generated by the calculation; $\oplus$ is the exclusive OR operation ; $\|$ connector; KS_A is the private key of A; KP_A is the public key of A; $Cert_A$ is the certificate of A; and T_A is the timestamp generated by A.

$E(k, m)$ and $D(k, c)$ are symmetric key encryption/decryption algorithms; ENC (KS, m) and DEC (KP, c) are asymmetric key encryption/decryption algorithms; $H(m)$ is a hash function.

The authentication server of each network registers with the mobile internet management center MC, and the MC is responsible for managing the security and other matters of each authentication server. At the same time, the MC issues identity certificates to each authentication server $Cert_A = \{ID_A, KP_A, Date_A, LF_A, ENC(KS_{MC}, ID_A \| KP_A \| Date_A \| LF_A)\}$, where $Date_A$ is the date the certificate was signed and LF_A is the validity period of the certificate.

2.1. MT Registering Home Network. The MT applies for registration with the local network authentication server HS to complete its identity legality verification, and the HS generates a temporary identity for the legal MT.

(1) The MT sends a registration application to the HS

(2) The HS assigns a unique temporary identification number TID_{MT} to the legally qualified MT

First, the secret number SMT is generated by the Formula (1), namely,

$$S_{MT} = H(ID_{MT} || Num_{HS}). \quad (1)$$

Then, the temporary identity TIDMT for generating the MT is calculated by using Equation (2), namely,

$$TID_{MT} = S_{MT} ID_{MT} ID_{HS}. \quad (2)$$

The HS establishes the registration information $<ID_{MT}, S_{MT}, TID_{MT}, Num_{HS}>$ for the legally legged MT and hands over the temporary identity TID_{MT} to the MT for secure storage through the secure channel.

2.2. MT Anonymous Roaming Mechanism. After the MT is successfully registered, when the preroaming enters the remote network, the remote network authentication server RS will verify the identity of the MT denial identity based on the anonymous roaming mechanism. The specific application process is shown in Figure 2:

(1) After the MT generates the random number X_0, ID_{HS}, ID_{RS}, TID_{MT}, and the time stamp T_{MT} are encrypted with the public key of HS, that is, $M = ENC(KP_{HS}, ID_{HS} \| ID_{RS} \| TID_{MT} \| T_{MT})$, the messages ID_{HS}, ID_{RS}, T_{MT}, TID_{MT}, M, and X_0 and the message signature Sig_{MT} are encrypted together with the public key of RS, and the public key encryption ensures that only the authentication server of the target network can decrypt it

(2) RS verifies the integrity of the MT message based on the message signature followed by the verification of the freshness of the message's timestamp to prevent

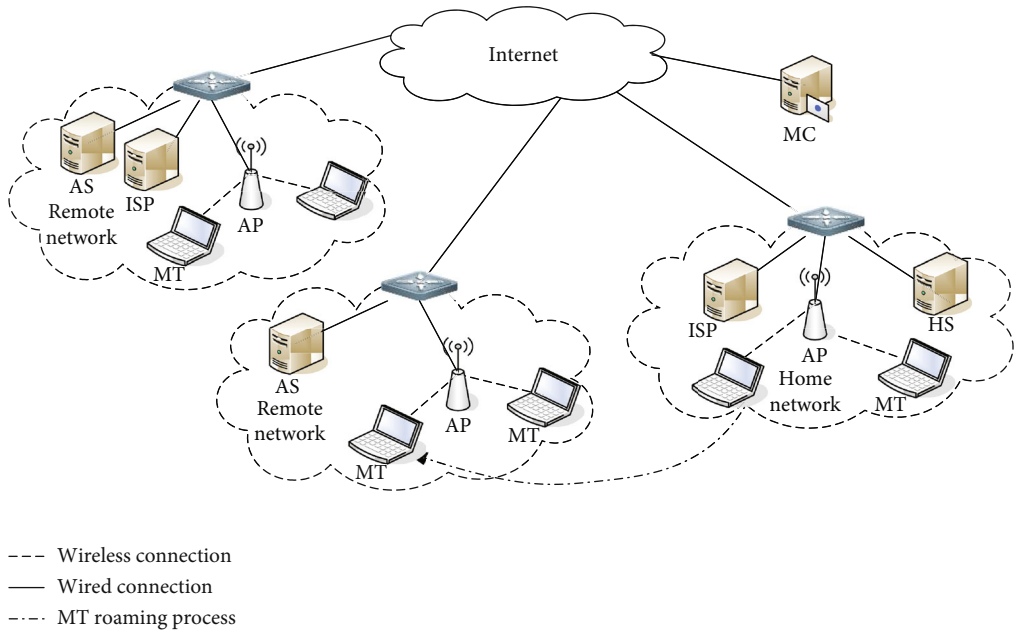

Figure 1: Mobile Internet roaming mechanism.

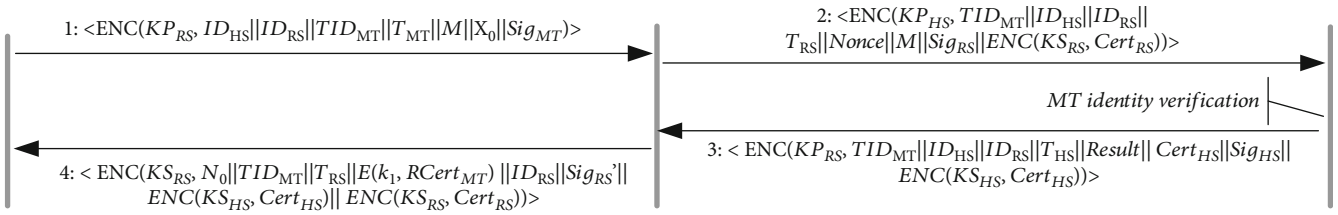

Figure 2: Anonymous roaming mechanism of MT.

the replay attack. If the verification is invalid, the roaming request of the MT will be rejected; otherwise, RS will encrypt the message TID_{MT}, ID_{HS}, ID_{RS}, T_{RS}, Nonce, ENC (PS_{RS}, $Cert_{RS}$), and M and then send them to HS together with the message signature after encrypting them with the public key

(3) HS verifies the validity of RS ID card and the validity of message integrity and the validity of the timestamp. If the verification fails, the execution will be terminated, and the roaming authentication mechanism will be withdrawn. Otherwise, after the HS decrypts the relevant messages, the identification of MT will be verified by formula (3). That is,

$$ID_{MT}{}' = TID_{MT}H(ID_{MT}||Num_{HS})ID_{HS}. \quad (3)$$

MT is an illegal user if $ID_{MT}{}' \neq ID_{MT}$, and HS terminates the operation; otherwise, HS encrypts the message TID_{MT}, ID_{HS}, ID_{RS}, T_{HS}, Result, ENC (PS_{HS}, $Cert_{HS}$), and Sig_{HS} with the public key of RS and sends it to RS.

(4) RS verifies the authenticity of the HS identity, the validity of the integrity of the message, and the validity of the timestamp. If not, the execution terminates and the operation exits; otherwise, the RS confirms the identity of the MT according to the relevant information and issues a roaming certificate $RCert_{MT}$ for the MT whose identity is legal

First, the RS selects the random secret number N0; then, the RS calculates the session key k1 = X0, N0. Finally, the RS sends the message TIDMT, IDRS, TRS, SigRS', N0, E(k1, RCertMT), ENC (KSHS, CertHS), and ENC (KSRS, CertRS) to the MT after encrypting them with the private key of the RS, where the private key encryption ensures that the roaming response message is sent by the RS.

Through the abovementioned two-round message interaction, the MT identity authentication is completed, and the negotiation between the MT and the RS session key is realized, wherein the session key is determined by the random secret number generated by the MT and the RS. That is, k $1 = X_0 \oplus N_0$. The MT uses the session key to ensure the security of the message in the roaming service process. That is, the MT security obtains the roaming certificate $RCert_{MT}$.

2.3. MT Applying for Service with Certificate. When MT obtains $RCert_{MT}$, it can apply for roaming to remote network authentication server RS many times during its validity

period. The process of MT applying for roaming within the validity period of $\mathrm{RCert}_{\mathrm{MT}}$ is shown in Figure 3.

(1) When MT applies for repeated roaming, it generates a random number X_i and calculates the temporary identity of the roaming application. That is,

$$\begin{aligned} \mathrm{TID}_{\mathrm{MT}_i} &= \mathrm{TID}_{\mathrm{MT}_{i-1}} \oplus N_{i-1} \oplus X_i, \\ \mathrm{TID}_{\mathrm{MT}_0} &= \mathrm{TID}_{\mathrm{MT}}, i = 1, 2, \cdots, n. \end{aligned} \tag{4}$$

MT computes the $E(k_{i-1}, \mathrm{RCert}_{\mathrm{MT}} \| X_i)$ and message signature, reads the message, and then sends the $\mathrm{Sig}_{\mathrm{MT}_i} TID_{MT_i}$, $e E(k_{i-1}, \mathrm{RCert}_{\mathrm{MT}} \| X_i)$, to RS.

(2) The RS verifies the freshness of the message and the integrity of the message. If the authentication fails, the roaming service request of the MT will be rejected; otherwise, the message $\mathrm{E}(\mathrm{k_{i\text{-}1}}, \mathrm{RCert_{MT}} \| \mathrm{X_i})$ will be decrypted by using the session key $k_i = X_i \oplus N_i$. If the MT holds a legal certificate, the RS will generate a random number n_i, and the session key $k_i = X_i \oplus N_i$ between the update and the MT will be updated

After the RS reads the timestamp, the message, $\mathrm{Sig}_{\mathrm{RS}_i}$, T_{RS_i}, and $E(k_{i-1}, N_i)$, will be sent to MT. MT uses Formula (5) to calculate the session key k_i:

$$k_i = X_i \oplus N_i, \tag{5}$$

in which $i = 1, 2, \cdots, n$. After the identity authentication between MT and RS has passed, the secure and anonymous communication between MT and RS can be carried out according to the anonymous communication model of mobile Internet in reference [6], which is not discussed in this paper.

2.4. Roaming Structure

2.4.1. Certificate Structure. Excessive application for roaming service will not only increase the authentication load of MT but also require that HS must always be online, which makes HS become the authentication bottleneck of the whole roaming mechanism. This paper uses the certificate mechanism to reduce the number of MT verification and to improve the efficiency of the HS. The basic information of the certificate is as follows: (1) validity: the effective time of the certificate, (2) the time of issuance: the time when the certificate is issued, (3) authorization object: the temporary identity TIDMT of the certificate holder, and (4) signature: signature information of RS.

2.4.2. Verification of Legitimacy. During the validity period of the roaming certificate, MT can apply for roaming service many times with the certificate and verify the authenticity of the roaming certificate through the following steps to judge the identity legitimacy of MT.

(1) Verify the identity of the issuer through signature information and check whether the contents of the certificate have been tampered simultaneously

(2) Verify the validity of the certificate based on the validity of the certificate and the time of issue

(3) Compute $\mathrm{TID_{MT}}' = \mathrm{TID}_{\mathrm{MT}_i} \oplus X_i \oplus X_{i-1} \oplus \cdots \oplus X_0 \oplus N_i \oplus N_{i-1} \oplus \cdots \oplus N_0$, verify whether $\mathrm{TID_{MT}} = \mathrm{TI\,D_{MT'}}\, I$ holds or not, and whether the person who holds the certificate is the applicant of it. If the above verification is passed, the MT holds true and valid legal certificate

3. Security Proof

3.1. CK Model. Bellare etal. [15] introduced modularization in 1998 to analyze the security of the protocol, which provides a theoretical basis for constructing a new provable secure key exchange protocol using reusable modules. Then, Canetti and Krawczyk further extended the method [16], which is called CK model.

Two attack models are defined in the ck model, that is, ideal model AM and real model UM. AM is authenticated as link modes. In this model, the attacker is passive and can invoke protocol running, capture protocol participants, query session key, expose, and test the session key. The um model is an unauthenticated link model. Thus, it can only faithfully deliver the same message once and cannot forge, tamper, or replay the message from an uncaptured participant. An UM model is an unverified link model. In addition to performing all attacks in the AM model, attackers can forge, tamper, and replay messages.

Definition 1. [16]. Let $\prod$ and $\prod'$ be n-side message driven protocols. $\prod$ runs in AM, and $\prod'$ runs in UM. If for any UM adversary U, there exists an AM adversary A, which makes AUTHA, $\prod$, and UNAUTHU, π' indistinguishable in calculation. Then, the simulation is called in um.

Definition 2. [16].

Compiler c is an algorithm whose input is a protocol description and output a protocol description.

If a compiler c has a protocol $c(\pi)$ to emulate in um for any protocol, the editor is called an authenticator. Define 3 [12] in session key security: if for any adversary A, when and only when the following properties are satisfied, the protocol is session key secure in AM.

Property 3. The uncaptured two parties obtain the same session key after participating in the entire agreement.

Property 4. If an adversary A performs a query attack, the possibility that it gets the correct session output value is not more than $1/2 + \varepsilon$, where ε is an ignorable decimal in the safety parameter range.

Theorem 5. [16]. *Assumes that λ is a message transmission authenticator, specifically, λ simulates a simple message*

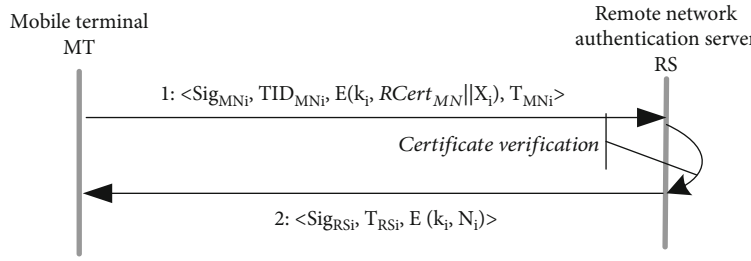

FIGURE 3: MT applies for roaming service with $\mathrm{RCert}_{\mathrm{MT}}$.

transfer protocol in um, assuming that c λ is a compiler defined on the basis of λ, and then c λ is an authenticator. Authenticator is a very important mechanism in modularization method, which can ensure that the security protocol in am can be transformed into security protocol in UM.

The messaging protocol sends a message from one participant to another. A protocol authenticator $c\ \lambda$ is a combination of several message transmission authenticators λ. If the protocol in AM has only one message flow, a message transmission authenticator λ can be used as the authenticator c λ. Otherwise, the simulated message transfer authenticator λ of the protocol message flow in AM can be combined together to act as the authenticator $c\ \lambda$. In [16], the basic methods of designing authentication and key agreement protocols based on the CK model are introduced in detail.

3.2. Roaming Protocols in AM. RS relies on the home authentication server HS to authenticate the identity legitimacy and platform credibility of MT. The process of the agreement is as follows:

(1) The access requests: The MT sends a roaming request message to the RS, which contains the identity of the relevant participant $\{\mathrm{TID}_{\mathrm{MT}}, \mathrm{ID}_{\mathrm{HS}}, \mathrm{ID}_{\mathrm{RS}}\}$

(2) The validity verification request: RS after receiving the roaming request of the MT, it is impossible to determine whether the MT is a legally authentic mobile terminal for the reason that the related information of the MT is not grasped, and the assistance authentication of HS is required. RS sends the MT legitimacy verification request $\{\mathrm{TID}_{\mathrm{MT}}, \mathrm{ID}_{\mathrm{HS}}, \mathrm{ID}_{\mathrm{RS}}, T_{RS}, \mathrm{Nonce}_{\mathrm{RS}}, \mathrm{Cert}_{\mathrm{RS}}, M, \mathrm{Sig}_{\mathrm{RS}}\}$ to the HS

(3) Legitimacy verification response: after HS receives the request message of RS's legitimacy verification, it first checks whether MT is a legitimate and trusted user and then checks whether RS is a legitimate remote network authentication server. If the above verifications are not passed, the protocol will be terminated and exits; otherwise, the information will be encrypted such as the result of the MT validity verification with the public key of rs, and the cipher text will send ENC x (-
$\mathrm{KP}_{\mathrm{RS}}, \mathrm{TID}_{\mathrm{MT}}\|\mathrm{ID}_{\mathrm{HS}}\|\mathrm{ID}_{\mathrm{RS}}\|T_{\mathrm{HS}}\|\ \mathrm{Result}\|\mathrm{Nonce}_{\mathrm{RS}}\|$
$\mathrm{ENC}\,(\mathrm{KS}_{\mathrm{HS}}, \mathrm{Cert}_{\mathrm{HS}})\|\mathrm{Sig}_{\mathrm{HS}})$ all the sighs to RS

(4) Roaming response: RS decrypts the cipher text message sent by hs using its own private key. RS verifies whether HS is a legitimate home network authentication server. After the verification has passed, it constructs the response message ENC (-
$\mathrm{KS}_{\mathrm{RS}}, N_0\|\ \mathrm{TID}_{\mathrm{MT}}\|T_{\mathrm{RS}}\|\ \mathrm{RCert}_{\mathrm{MT}}\|\mathrm{ID}_{\mathrm{RS}}\ \|\mathrm{Sig}_{\mathrm{RS}}{}'\|\mathrm{Nonc}$
$\mathrm{e}_{\mathrm{MT}}\ \|\ \mathrm{ENC}\,(\mathrm{KS}_{\mathrm{RS}}, \mathrm{Cert}_{\mathrm{RS}})\ \|\ \mathrm{ENC}\,(\mathrm{KS}_{\mathrm{HS}}, \mathrm{Cert}_{\mathrm{HS}}))$ and sends the message to MT

MT verifies that RS is a desired remote network authentication server based on identity certificate, and whether HS is a real home authentication server. Verification fails if the authentication fails.

Theorem 6. *The MT roaming protocol is secured in AM when the signature, asymmetric encryption, symmetric encryption, and other algorithms are secured and difficult to solve.*

It is proved that in AM, because the message participant is not captured by the enemy A during the protocol interaction, when the protocol is executed, MT and RS get the untampered X_0 and N_0.The calculated shared session keys are both $k_1 = X_0 \oplus N_0$. Therefore, the protocol satisfies the property of session key security 1.

It is assumed that the enemy a can distinguish the key agreement parameters from a random number of equal lengths by a probability p, which cannot be ignored. The probability upper limit of the unsymmetrical encryption algorithm to be breached is P_{ENC}. The enemy a can only get x0 and n0 by breaking the message encrypted with $\mathrm{PK}_{\mathrm{RS}}$ and $\mathrm{KS}_{\mathrm{RS}}$ and then perform XOR operation to get the session key. Because the random secret number N_0 generated by rs is transmitted by $\mathrm{KS}_{\mathrm{RS}}$ encryption, it is easy to be obtained by the enemy a. Thereby, the key point of the enemy is that X_0, which means A can only obtain the random secret number X_0 by breaking the ENC $(\mathrm{KP}_{\mathrm{RS}}, \mathrm{ID}_{\mathrm{HS}}\|\mathrm{ID}_{\mathrm{RS}}\|\ \mathrm{TID}_{\mathrm{MT}}\|\ T_{\mathrm{MT}}\ \|M\|X_0\ \|\mathrm{Nonce}_{\mathrm{MT}}\ \|\mathrm{Sig}_{\mathrm{MT}})$. Then, the probability of the random secret number X_0 being attacked by the adversary A at least is $\mathrm{PP}_{\mathrm{ENC}}$. If adversary a can obtain the random number $X_{0,}$ then there is $(1 - PP_{\mathrm{ENC}}) << PP_{\mathrm{ENC}}$ (that is PP_{ENC} is far greater than 1-PP_{ENC}), that is, $1/2 < < PP_{\mathrm{ENC}}$; so, both p and P_{ENC} cannot be ignored. This is contrary to the premise that asymmetric encryption algorithm is secure and difficult to solve. So, the

probability of the enemy a guessing the correct session key K1 is no more than $1/2 + \varepsilon$, in which ε is ignorable. And the protocol satisfies the property of session key security 2. The MT roaming protocol is session key secure in am.

In AM, because the enemy cannot forgery, tamper, and replay the message, they can only transmit the information produced by the legitimate participant. MT and RS get the identity legitimacy and platform credibility verification information without tampering. With the secure session key K_1 negotiated, roaming mechanism is secure in AM.

Proof of completion.

3.3. Authenticator Construction. This paper starts with HS authenticating MT, RS authenticating HS, and MT authenticating RS to construct authenticator. For the authentication information flow between RS and HS, and the authentication information flow between mt and RS a signature authenticator $\lambda_{\text{sig},\,T}$ based on timestamp is used, the security proof process of which is detailed in [16]. The specific interactive process of $\lambda_{\text{sig},T}$ is as follows: (1) A obtains timestamp ta, computes the signature sSig (m, T_A, B), and sends a message <m, Sig (m, T_A, B)> to B. (2) After receiving the message, b first checks the freshness of the timestamp ta and the correctness of the signature. If T_a is fresh and the signature is correct, b completes the authentication of a.

For the authentication message between hs and mt, because the message sent by mt is forwarded by rs, the message of mt authentication must be processed accordingly, which cannot directly send relevant real identity information, but also enable hs to verify the real identity of mt. Therefore, the identity-based anonymous authenticator $\lambda_{\text{ENC,TID},T}$ is used. Its security and anonymity proof are detailed in reference [9]. The specific interactive process of $\lambda_{\text{ENC,TID},T}$ is described as follows: (1) a registers to obtain tida. Use b's public key encryption to generate the ENC (KP_B, $m\|\text{TID}_A\|T_A$) and finally send tida, ENC (KP_B, $m\|\text{TID}_A\|T_A$) to B. (2) After B receiving the message, the cipher text message is decrypted to verify the validity of the TID_A. If the user is illegal, the execution will be terminated. Otherwise, the freshness of the timestamp will be checked. If the verification is passed, a passes the authentication of b.

3.4. Protocol in UM. First, the above authenticators $\lambda_{\text{sig},T}$ and $\lambda_{\text{ENC,TID},T}$ are applied to the am protocol message flow in Section 3.2 of this paper. Then, the authentication of mt is hidden without affecting the provable security of the protocol. This prevents an attacker from obtaining their true and valid identity information. Finally, the protocol in UM is optimized by using the method in [15], and the mt roaming protocol in UM shown in Figure 4 is obtained.

Theorem 7. *When the signature, asymmetric encryption and symmetric encryption algorithms are secure and difficult to solve, and the mt roaming mechanism is secure in um.*

Proof. It is proved that the mt roaming mechanism in UM can be automatically compiled according to the ck model because the authenticator used is provable and secure. Then, the anonymous roaming authentication mechanism is provable under the ck security model.

Completion of proof. □

Similarly, repeated roaming requests from mt certificates are also verifiable and secure.

4. Model Analysis

4.1. Anonymity Analysis

4.1.1. The Anonymity and Untraceability of Users. The real identity of the MT does not appear in communication and at the time of registration, it is replaced by the temporary identity TID_{MT}. Since only the HS are in possession of the secret number Num_{HS}, only HS can correctly verify the real identity ID_{MT} of the user through the expression (2) to ensure the anonymity of the MT identity. The different MT corresponds to a different temporary identity TID_{MT} and is generated by a different random number Num_{HS}. Any legal MT cannot calculate the temporary identity of the other MT through its own TID_{MT}.

Each time when a roaming is applied by the same MT, a different temporary identity TID_{MT} is used, which has an untraceable property.

MT encrypts the temporary identity TID_{MT} and passes it to RS, which realizes the anonymity of the user's real identity idMT to rs and the protection of his temporary identity. Even if the user's temporary identity TID_{MT} is compromised, the attacker can neither know the real identity of the user nor associate the intercepted temporary identity with it nor monitor the communication process of the user and track the message session. To sum up, the use of temporary identity to protect the anonymity of the user identity can effectively prevent attackers from tracking users, eavesdropping, and doing other attacks. This ensures the anonymity of user identity, location, and other privacy information. At the same time, it does not reduce the security of users.

4.1.2. Anonymity of Certificates. The roaming certificate can only report whether the identity of its holder is legal. It does not contain the configuration information of MT and its identity information, which means, the roaming certificate is anonymous, and the anonymity depends on the duration of valid authorization. The shorter the authorization time, the stronger the anonymity is. Meanwhile, the anonymity of the certificate is controllable, and controllability depends on the temporary identity information of the certificate holder. It allows only the same user to establish a roaming service. Specifically, it can only prove the identity legitimacy of the same user during the validity period of the certificate.

4.2. Safety Analysis. MT uses secret number SMT and identity information to calculate temporary identity TIDMT, by hash function. The confidentiality of SMT and the security of hash function ensure the unforgeability of TIDMT.

After the HS checks the freshness of the timestamp, it calculates the validity of the MT to identity its verification, i.e., RS completes the authentication of the MT with the help of HS, in which the message signature guarantees the

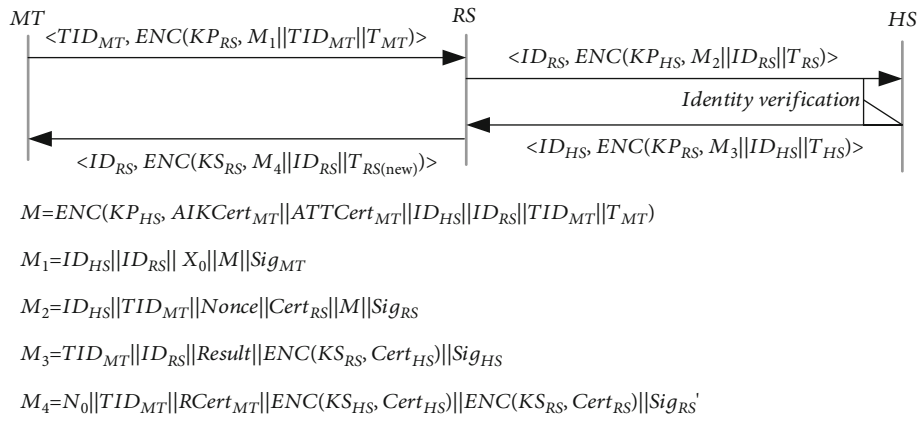

Figure 4: MT roaming protocol in UM.

integrity of the message, and the random number can prevent the replay attack.

When the MT repeatedly applies for service, the roaming certificate can prove the validity of the identity. Each time a different session key ki is generated, a one-time secret is realized, and the security is enhanced. Since Xi is selected by the MT and Ni is selected by the RS, ki is a one-time key. Neither party can calculate the generation separately, ensuring the fairness, freshness, and perfect presecrecy of the session key. Specially, PGF-JKNN-c got a dramatic 99.9%, which outperforms state-of-the-art methods.

Comparing the methods on the four data sets, we can observe that our proposed methods are better than other methods in three data sets (Indian Pines, KSC, and Salinas) except for University of Pavia data set. University of Pavia data set has the characteristics of few categories and low dimension, which are more suitable for SVM classifier. The SSKNN method performs poorly on KSC data set. That is because SSKNN is more fit able for regular shapes and large-scale shapes. Our proposed FPF-JKNN and GPF-JKNN are more robust to solve complex problems.

4.3. Performance Analysis

4.3.1. Calculation Efficiency. In the whole roaming authentication process, MT only needs one hash operation, one symmetric encryption operation, and one asymmetric encryption operation, while HS performs one asymmetric encryption operation and three hash operations. Rs performs two hash operations, one symmetric encryption, and two asymmetric decryption operations. The number of communication rounds between MT and RS and between RS and HS is one round. This scheme is comparable with [17, 18] in terms of computational overhead. The results are shown in Table 1.

4.3.2. Communication Efficiency. In the roaming mechanism, the first-round interaction verifies the identity legitimacy and platform credibility of MT. If the verification fails, HS and RS will terminate the interaction after the first round, which reduces the execution load of the protocol to a certain extent.

When the identity is legal and the platform is credible, MT applicants with certificates can apply for roaming service on a plurality of times. The use of the certificate mechanism improves the working efficiency of the roaming authentication mechanism, simultaneously effectively reduces the number of authentication times of the identity of the MT, and prevents the RS and HS from becoming a system bottleneck. In the repeated roaming process of the MT certificate holders, the authentication of the identity of the MT can be completed without the assistance of the HS by RS, the MT roaming authentication process for carrying out the 1-round message interaction is realized, and the communication time delay of the MT is reduced.

4.3.3. Storage Efficiency. The identity of MT is stored directly by HS. It is unnecessary for special trust center to store and manage it uniformly. MT only needs to store the necessary information, such as temporary identity. The anonymous roaming mechanism in this paper lightens the storage burden of MT.

4.4. Extensibility. With the rapid development of network technology, identity legality verification is no longer a necessary and sufficient condition for judging user security. However, it should be concerned with whether the terminal platform is trusted while condition for judging user security. However, it should be the identity is legal. The credibility of the platform is a necessary condition for user security, which promotes the rise and development of trusted computing technology. With the development of trusted computing technology, the mobile trusted module (MTM) [19, 20] specification is intended to be established on mobile terminals. The security mechanism protects the user's private information and sensitive data and builds a secure and reliable mobile trusted terminal. It is only necessary to add the credibility verification information of the user terminal platform in the authentication message of this document, and the HS can verify the credibility of the MT platform according to the platform credibility verification strategy, so that the anonymous roaming requirement of the terminal in the trusted computing environment can be satisfied.

Table 1: Comparison of computing overhead by entity.

Operation	Our scheme	Literature [17]	Literature [18]
Hash operation (MT/HS/RS)	1/3/2	7/10/4	5/3/4
Symmetric encryption and decryption(MT/HS/RS)	2/0/2	2/2/2	☆
Asymmetric encryption and decryption(MT/HS/RS)	1/1/2	☆	2/0/2
XOR operation (MT/HS/RS)	0/2/0	5/3/1	☆
Exponent arithmetic (MT/HS/RS)	☆	2/0/2	☆
Chaotoc-maps (MT/HS/RS)	☆	☆	6/2/1
Number of information exchanges(MT-RS/RS-HS)	2/2	2/2	2/2

Note: ☆ indicates that this scheme does not use the operation.

Similarly, the anonymous roaming mechanism of this paper can also be applied to roaming communication and tariff service of mobile user equipment in 3G network environment. RS provides services for MT and charges. If MT pays the fees once on every roaming, it will bring inconvenience. In the MT roaming identity authentication process, the RS charges service fee to the HS, and the HS charges the MT again. Since the HS assists the RS to complete the identity authentication of the MT during the roaming process, the MT cannot deny the cost incurred by the roaming..

5. Conclusion

The traditional authentication protocol cannot meet the identity authentication requirements of the mobile terminal roaming service. This paper proposes a mobile Internet anonymous roaming mechanism to improve this disadvantage. When the mobile terminal applies for the roaming service, the remote network authentication server completes the identity verification of the mobile terminal with the assistance of the home network authentication server. The use of temporary identity to achieve user anonymity protection not only makes remote networks and attackers unable to know the user's true identity but also ensures the confidentiality of private information such as user identity and location. The identity is associated with the existing communication information, which can ensure the nontrackability of the private information such as the user identity and location, and effectively prevents attackers from performing attacks such as tracking and eavesdropping on the user. The proposed mechanism does not reduce the process' security during the implementation of the anonymous roaming of mobile terminals. It has the characteristics of security, anonymity, and extensibility.

As the certificate will bring additional storage pressure to the terminal, the next step will be to further study the efficient roaming authentication mechanism under the mobile Internet and design a certificate-free one-round message interactive roaming authentication mechanism.

In the next stage, we will further study the roaming authentication mechanism with better performance based on the conclusions on the sensor distribution [21, 22], performance scheduling [23, 24], etc.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The paper was supported by the Science and Technology Project for the Universities of Shandong Province (No. J18KB171), Natural Science Foundation of China under Grant 62102235, Natural Science Foundation of Shandong Province under Grant ZR2020QF029, and Doctoral Fund of Shandong Jianzhu University under Grant XNBS1811. This work was also supported by the Computer Vision and Image Processing Technology Team Construction Project for the Shannxi Institute of International Trade & Commerce.

References

[1] M. Gupta and N. S. Chaudhari, "Anonymous two factor authentication protocol for roaming service in global mobility network with security beyond traditional limit," *Ad Hoc Networks*, vol. 84, pp. 56–67, 2019.

[2] W. Li, S. Zhang, Q. Su, Q. Wen, and Y. Chen, "An anonymous authentication protocol based on cloud for telemedical systems," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 8131367, 2018.

[3] T. Gao, F. Peng, and N. Guo, "Anonymous authentication scheme based on identity-based proxy group signature for wireless mesh network," *EURASIP Journal on Wireless Communications and Networking*, vol. 2016, no. 1, 2016.

[4] C. Jiang, S. L. Wu, and K. Gu, "New kind of delegation-based anonymous authentication scheme for wireless roaming networks," *International Journal of Network Security*, vol. 20, no. 2, pp. 235–242, 2018.

[5] K. Park, Y. Park, Y. Park, A. Goutham Reddy, and A. K. Das, "Provably secure and efficient authentication protocol for roaming service in global mobility networks," *IEEE Access*, vol. 5, pp. 25110–25125, 2017.

[6] S. Aghapour, M. Kaveh, and D. Martín, "An ultra-lightweight and provably secure broadcast authentication protocol for smart grid communications," *IEEE Access*, vol. 8, pp. 125477–125487, 2020.

[7] V. Kumar, M. Ahmad, A. Kumari, S. Kumari, and M. K. Khan, "SEBAP: a secure and efficient biometric-assisted authentication protocol using ECC for vehicular cloud computing," *International Journal of Communication Systems*, vol. 34, no. 2, 2021.

[8] U. Chatterjee, D. Mukhopadhyay, and R. S. Chakraborty, "3PAA: aprivatePUFprotocol foranonymousauthentication," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 756–769, 2021.

[9] B. A. Alzahrani, A. Irshad, A. Albeshri, K. Alsubhi, and M. Shafiq, "An improved lightweight authentication protocol for wireless body area networks," *IEEE Access*, vol. 8, pp. 190855–190872, 2020.

[10] G. Zhang, D. Fan, Y. Zhang, X. Li, and X. Liu, "A privacy preserving authentication scheme for roaming services in global mobility networks," *Security and Communication Networks*, vol. 8, no. 16, 2859 pages, 2015.

[11] S. A. Chaudhry, A. Albeshri, N. Xiong, C. Lee, and T. Shon, "A privacy preserving authentication scheme for roaming in ubiquitous networks," *Cluster Computing*, vol. 20, no. 2, pp. 1223–1236, 2017.

[12] X. Li, A. K. Sangaiah, S. Kumari, F. Wu, J. Shen, and M. K. Khan, "An efficient authentication and key agreement scheme with user anonymity for roaming service in smart city," *Personal and Ubiquitous Computing*, vol. 21, no. 5, pp. 791–805, 2017.

[13] V. Odelu, S. Banerjee, A. K. Das et al., "A secure anonymity preserving authentication scheme for roaming service in global mobility networks," *Wireless Personal Communications*, vol. 96, no. 2, pp. 2351–2387, 2017.

[14] J. L. Tsai and N. W. Lo, "Provably secure anonymous authentication with batch verification for mobile roaming services," *Ad Hoc Networks*, vol. 44, pp. 19–31, 2016.

[15] M. Bellare, R. Canetti, and H. Krawczyk, "A modular approach to the design and analysis of authentication and key exchange protocols (extended abstract)," in *Proceedings of the Thirtieth Annual ACM Symposium on the Theory of Computing*, pp. 419–428, Dallas Texas USA, 1998.

[16] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," in *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 453–474, Springer, Berlin, Heidelberg, 2001.

[17] M. Karuppiah, S. Kumari, X. Li et al., "A dynamic ID-based generic framework for anonymous authentication scheme for roaming service in global mobility networks," *Wireless Personal Communications*, vol. 93, no. 2, pp. 383–407, 2017.

[18] Q. Xie, H. Bin, X. Tan, and D. S. Wong, "Chaotic maps-based strong anonymous authentication scheme for roaming services in global mobility networks," *Wireless Personal Communications*, vol. 96, no. 4, pp. 5881–5896, 2017.

[19] M. Kim, H. Ju, Y. Kim, J. Park, and Y. Park, "Design and implementation of mobile trusted module for trusted mobile computing," *IEEE Transactions on Consumer Electronics*, vol. 56, no. 1, pp. 134–140, 2010.

[20] A. Soltani-Farani, H. R. Rabiee, and S. A. Hosseini, "Spatial-aware dictionary learning for hyperspectral image classification," *IEEE Transactions on Geoscience and Remote Sensing*, vol. 53, no. 1, pp. 527–541, 2015.

[21] X. Xue and C. Jiang, "Matching sensor ontologies with multi-context similarity measure and parallel compact differential evolution algorithm," *IEEE Sensors Journal*, vol. 21, no. 21, pp. 24570–24578, 2021.

[22] X. Xue, X. Wu, C. Jiang, G. Mao, and H. Zhu, "Integrating sensor ontologies with global and local alignment extractions," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 6625184, 10 pages, 2021.

[23] X. Xue and J. Zhang, "Matching large-scale biomedical ontologies with central concept based partitioning algorithm and adaptive compact evolutionary algorithm," *Applied Soft Computing*, vol. 106, article 107343, 2021.

[24] X. Xue and J. Chen, "Matching biomedical ontologies through compact differential evolution algorithm with compact adaption schemes on control parameters," *Neurocomputing*, vol. 458, pp. 526–534, 2021.