2022 IEEE 22nd International Conference on Software Quality, Reliability and Security (QRS)

Identity Authentication Strategy of Mobile Crowd Sensing based on CFL

Lin Wang[1], Fangxiao Li[2], Yunfei Xie[2], and Leyi Shi[1,2,*]
[1]College of Oceanography and Space Informatics,China University of Petroleum, QingDao, China
[2]College of Computer Science and Technology,China University of Petroleum, QingDao, China
shileyi@upc.edu.cn, 773628999@qq.com, 1720488013@qq.com, 1182326676@qq.com
*corresponding author

***Abstract*—In order to protect information privacy and ensure user information security, in view of the obvious centralization of the existing identity authentication technologies such as Public Key Infrastructure(PKI) and Identity-Based Encrypted(IBE), this paper proposes an efficient authentication strategy that applies Cryptography Fundamental Logics(CFL) identity authentication technology to Mobile Crowd Sensing(MCS) system, which can complete the authentication between Task Publisher, Cluster Head and Task Participant without the participation of a third-party center. Firstly, this paper introduces to use CFL technology to solve the problem of identity authentication relying on the central server; Secondly, an algorithm combined with MCS system is proposed to solve the decentralization of authentication process; Finally, the Average System Response Time and System Throughput of the three technologies are obtained through simulation experiments, analyzed and compared. The result shows that: this strategy has obvious advantages, it can faster and more secure the identity authentication.**

***Keywords*—Mobile Crowd Sensing, Privacy-preserving, Cryptography Fundamental Logics, BAN logic, clustering**

I. Introduction

The Mobile Crowd Sensing [1] is based on a wireless sensor network [2] through the use of sensors built-in mobile intelligent devices to achieve a broader, more convenient, more thorough, more private, and more comprehensive sensing service, which can greatly promote the development of the Internet of Everything [3] and smart cities [4]. However, privacy leakage and other problems in the MCS system will affect and restrict its future development and large-scale deployment application. The security and privacy-preserving [5] issues in the MCS are the key to whether participants can actively participate. For examples, an app needs to detect the traffic flow in a certain area within a certain period of time, and it will publish tasks in that area and recruit task participants. If participants want to earn incentives, they need to submit their location information in exchange for rewards; a task publisher wants to obtain photos from all angles of a building in a certain area in a certain period of time, and then gives appropriate incentives according to the quality of the photos presented. If the MCS system task is to be carried out smoothly, the task publisher must first authenticate the identity of the user who wants to participate in the task, so as to ensure the privacy, information security, location security and data security of both parties. This can not only protect the privacy of the task participants, but also enable the task publisher to avoid attacks by some malicious users.

MCS is a human-centered perception and data collection [6] mode, requires participants to provide the location, time, sensor type, identity, bidding, data, and other information, which involves participants' location privacy, trajectory privacy, data privacy, identity privacy, etc. Therefore, compared with traditional wireless sensor networks, privacy-preserving is a major problem faced by MCS, and privacy-preserving issues run through all stages of the MCS mission cycle [7]. Generally speaking, a large number of task participants and reliable perceptual data are the basic requirements for achieving reliable perceptual services, and the primary task is to solve the problem of identity authentication. Only by ensuring that the identity is sufficiently secure can more participants be attracted to participate in the task. In addition, the MCS system needs to have a complete and strong incentive mechanism to ensure the interests of both task publishers and task participants. It can neither make task participants provide data without rewards, nor make task publishers suffer replay attacks from malicious users, which will lead to excessive occupation of system resources and reduce system reputation; If you want to attract more participants to participate in the perception task and obtain high-quality data, the task publisher needs to provide enough incentives to attract participants as far as possible; The MCS system also needs to develop a task specific quantitative plan for data quality, so that the higher the data quality provided by the task participants, the higher the quantitative score, and the more incentives they will get.

However, the existing PKI [8] authentication technology needs a certificate generation center in the registration process, a certificate authentication center in the verification stage, and IBE [9] authentication technology needs the participation of the Private Key Generator in the whole process, which all have obvious centralization problems.

Motivated by CFL identity authentication [10], a new identity based certificate authentication system, compared with PKI, IBE and other traditional authentication methods, it has the characteristics of high security strength, low calculation cost, less certificate delivery times, and the most important thing is that the authentication process does not require third-party intervention, which is more suitable for MCS systems.

The main contributions of this paper are summarized as follows:

- This paper puts forward the method of ”clustering”to reduce the certification pressure of task publishers, which makes MCS faster, safer and easier. Within the specified task area, the task area is randomly divided into several small areas, and a cluster head is randomly selected in each small area to verify the identity of participants

2693-9177/22/$31.00 ©2022 IEEE
DOI 10.1109/QRS57517.2022.00024

and collect participant data for transmission to the task publisher.

- This paper put the CFL card issuing center on the cloud,which proposed to solve the problem of relying on the central server in the registration stage, and an algorithm is proposed to combine with the MCS identity authentication to realize the decentralization problem in the verification process, and Time Stamp Technology is used to label the registration, verification and revocation stages of certificates to resist replay attacks.
- This paper's experiment is compared with PKI and IBE in terms of communication cost, calculation cost, average system response time, system throughput.

The rest of this paper is organized as follows:

In Section 2, we investigate the relate work of MCS and identity authentication technology. Section 3 introduces the pre-knowledge of this paper. The system model and authentication process are defined in Section 4. In section 5, we can get the formal analysis of the authentication protocol by BAN logic, security analysis, and verify the effectiveness of this strategy through simulation experiments. We conclude this paper in Section 6.

II. Related Work

With the popularity of mobile intelligent devices, it is becoming more and more convenient to obtain multiple information through them, and the resulting privacy leakage is also becoming easier. Mobile Crowd Sensing task is essentially a Spatial Crowdsourcing task [11], it means that Mobile Crowd Sensing task allocation must consider the location of task participants and the time when they can perform the perception task. Since the task requirements involve the privacy of the task publisher, and the configuration information of the task participants includes the privacy of the participants, according to the privacy-preserving task allocation scheme, the privacy of several entities can be protected, which can be divided into one-way privacy-preserving task allocation scheme and two-way privacy-preserving task allocation scheme.Although the scheme [12], [13] proposed by Shu et al. and Wu et al. the task allocation of two-way privacy-preserving is realized by proxy reencryption, the scheme proposed by them requires additional servers such as proxy servers or fog nodes. In the privacy-preserving protocol, adding servers will increase the number of entities that leak privacy. To reduce the risk of privacy disclosure, Shu et al. proposed a privacy-preserving task allocation scheme [14] without proxy server through secret sharing technology. Wu et al. proposed a reliable privacy-preserving task allocation scheme [15] using blockchain technology in consideration of the untrustworthy problem of the central server. Wu et al. used anonymous signature technology to protect the identity privacy of task participants [16]. Li et al. used reputation mechanism to evaluate data reliability, and then designed a mechanism to protect identity privacy [17]. Qiu et al. introduced k-anonymity technology into the data evaluation scheme [18] to protect the identity privacy of task participants.

Rao N et al. [19] pointed out the key challenge of deploying PKI system in resource limited industrial control systems, pointing out the direction of PKI research in the field of industrial control. Dan B et al. designed IBE authentication protocol [20] to solve the complex problem of PKI certificate management, using identity as the key generation meta set directly and creating the mapping between user identity and key. Gentry C et al. used lattice to construct IBE scheme in document [21], but it was proved that it was not as light-weight IBE [22], [23] scheme constructed using elliptic curve and bilinear pair designed by researchers recently. The above researchers continue to lighten the function authentication to promote its application and development in the field of industrial control and the Internet of things. Later, in view of the problem that the rights of central authentication such as PKI and IBE are too concentrated, Lindell y et al. [24] proposed a multi-party cooperative elliptic curve digital signature algorithm, which uses the homomorphic attribute in the homomorphic encryption algorithm to complete the signature authentication of both parties. Later, researchers also proposed a variety of ECDSA [25], [26] to achieve decentralized authentication, but the signature process of this scheme still depends on multiple communications between both sides, and the authentication efficiency is limited by large communication cost.

In view of the above problems, this paper proposes an identity authentication strategy of Mobile Crowd Sensing based on CFL.

III. Pre-Knowledge

CFL authentication system is a certificate authentication system based on identification, which is proposed on the basis of PKI authentication system and IBC authentication system.

A. Basic principles of CFL

The basic key pair of the CFL authentication system includes the identification key pair generated by the certificate generation center and the working key pair generated by the certificate generation center.

Verification process as show in Fig 1: generate the user's working key pair, then apply to the CFL certificate generation center for a certificate and submit their own working public key and other information, issue the CFL certificate to the client, and the client sends the dynamic CFL certificate to the verifier for certificate verification, and finally return the verification result.

B. Product-of-Exponential cryptographic algorithm

In this paper, we use an identity based product-of-exponential cipher algorithm as the basic cipher algorithm of identity key pair. Next, the process of generating the identity key pair by using the product-of-exponential cryptographic algorithm is given: Select two large prime numbers with the same scale p and q, let $n = p^*q$. Let $p_1 = (p-1)/2$ and $q_1 = (q-1)/2$ and require that $p_1, q_1, (p_1-1)/2, (q_1-1)/2$ are all prime numbers. By placing the data of SKB and PKBin the array, the stop sequence composed of the output

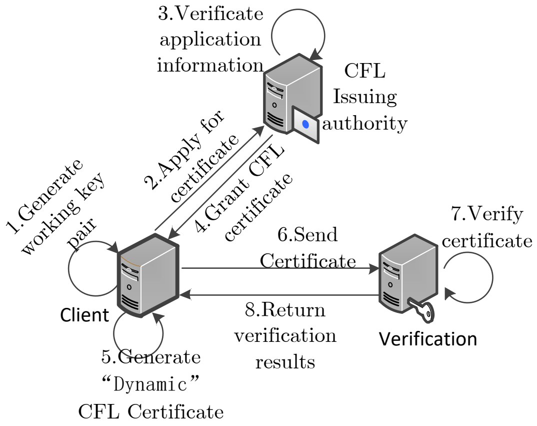
3.Verificate application information
CFL Issuing authority
2.Apply for certificate
4.Grant CFL certificate
1.Generate working key pair
6.Send Certificate
7.Verify certificate
Client
8.Return verification results
Verification
5.Generate “Dynamic” CFL Certificate

Figure 1. CFL verification process

sequence of the hash function H is selected. Let the output of H be n bits,satisfying $s \mid N$ and let $N = st$, output the sequence $h = \{h_0, h_1, \cdots, h_{t-1}\}$, where $h_i, i = 0, 1, \cdots, t-1$ is the number of s bits.

Let SKB $= \left\{d_0, d_1, \cdots, d_{t\times(2^s-1)}\right\}$, PKB $= \left\{e_0, e_1, \cdots, e_{t\times(2^s-1)}\right\}$, and e_i, d are prime numbers with two diverse numbers less than $\log_2 j(n)/t$,which are selected from the multiplication group of the Residual class ring. The multilinear function is set to:

$$f_{H(\mathrm{ID})}(\mathrm{SKB}) = f_h\left(d_0, d_1, \cdots, d_{t\times(2^s-1)}\right) = \prod_{i=0}^{t-1} d_{\sum_{j=0}^{i} h_j} \bmod \varphi(n) = \mathrm{IDSK} \tag{1}$$

The Dual Function:

$$f_{H(\mathrm{ID})}(\mathrm{PKB}) = f_h\left(e_0, e_1, \cdots, e_{t\times(2^s-1))}\right. = \prod_{i=0}^{t-1} e_{\sum_{j=0}^{i} h_j} = \mathrm{IDPK} \tag{2}$$

Among them $e_i d_i \equiv 1 \bmod \varphi(n)$, (1)(2)in the formula, note $s(i) = \sum_{j=0}^{i} h_j, i = 0, 1, \ldots, t-1$, which is the stop going sequence, used to control and select the private key base or the public key base, and corresponds to $h = \{h_0, h_1, \cdots, h_{t-1}\}$ one-to-one. We call (1) and (2) the transformation of multilinear functions.

The public key and private key of the product of exponential type public key cryptographic algorithm are composed of the product of multiple exponents, which breaks through the single exponential structure of the public key and private key of RSA cryptographic algorithm. For CFL authentication, it is not feasible for an attacker to obtain the private key base SKB by using the public key base PKB and the intercepted certificate content.

IV. Modeling and Process

A. MCS System Model

The system model of this paper is shown in the Fig 2 below. Different from common MCS system model, this system model comprises Task Publishers, Task Participants, and Cluster Heads randomly selected from task participants. A task publisher may be a person, a device, or a center that integrates verifying participants' identity, signing certificates, storing certificate information, and publishing tasks; Task Participants are composed of people who have mobile intelligent devices and want to participate in tasks and get incentives.

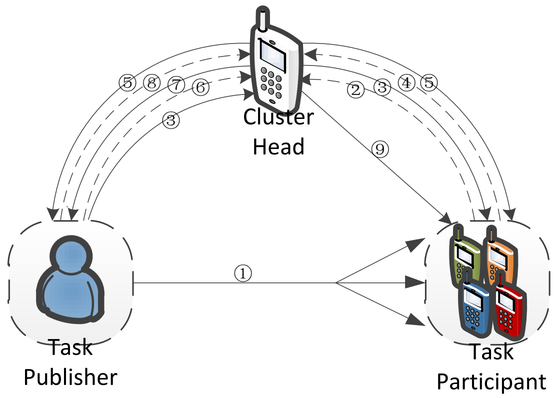

Figure 2. System schematic diagram

In this scene, since the scope of the task is limited, the number of people who can participate in the task can be unlimited, so when the Task Publisher publishes the task, the corresponding incentive interval will also be published. In a fixed geographical area, one of the neighboring participants is randomly selected as the Cluster Head to serve as a transit station for collecting the data of the neighboring participants in a small range. Still, the specific data content is not obtained.

In the system, the Task Publisher posts the perceptual tasks and obtains reliable perceptual data from the Task Participants. The Cluster Head is randomly selected by Task Participants in the specified area, and its role is as a guarantor. On the one hand, it prevents participants from providing low-quality data to affect the incentive mechanism of the system, and on the other hand, it prevents publishers from refusing to pay after obtaining reliable data. Task Participants are responsible for collecting perceptual data according to task requirements and earning rewards according to reliable data provided by themselves:

1. Task Publishing: the Task Publisher publishes tasks and budgets, and selects task participants who voluntarily participate in the specified area;
2. Select cluster head: divide the specified area into several small areas. In each small area, randomly select one participant from the participants as the Cluster Head, responsible for collecting the reliability evaluation and incentive of the publisher, and responsible for the identity authentication and data acquisition of the participants in its area;
3. Identity authentication: the Task Publisher performs CFL identity authentication on the Cluster Head, and the Cluster Head performs CFL identity authentication on the participants in its area;

4. Evaluation request: the Task participants transmit data to cluster heads and send reliability evaluation requests;
5. Notification of evaluation result: the cluster head evaluates the reliability request and sends the evaluation result to both parties;
6. Prepayment incentive: The Task Publisher advances the reward to the Cluster Head;
7. Data transfer: after receiving the advance payment, the Cluster Head sends the data to the Task Publisher;
8. Data confirmation: the Task Publishers verifies the reliability of the data, quantifies the data quality, and sends the final reward parameter to the Cluster Head;
9. Pay remuneration: if the data transmitted by the Task Participants passes the data reliability evaluation of the Task Publisher, the Cluster Head will pay the Task Participants the actual remuneration according to the final remuneration parameters.

B. Signature of certificate

When a user node accesses the Cluster Head or the certificate needs to be updated, the Cluster Head signs and distributes the certificate for the new cluster point or the cluster point that needs to update the certificate, which is the signing process of the certification as show in Fig 3. This section takes the Cluster Head signing the certificate for participant A as an example and mainly includes the following steps:

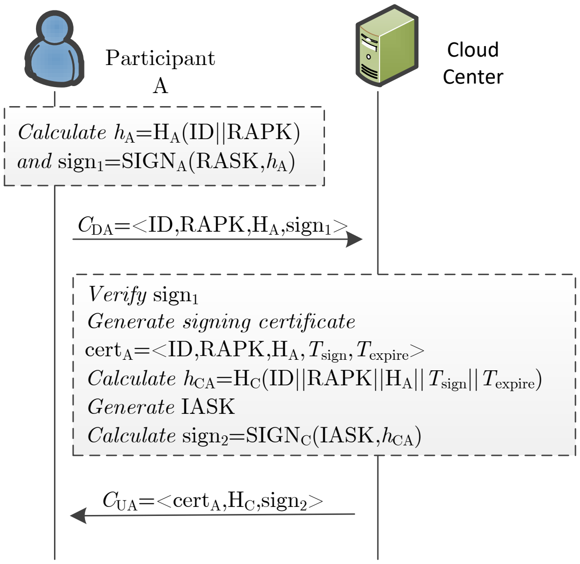
Participant A
Cloud Center
Calculate h_A=H$_A$(ID||RAPK) *and* sign$_1$=SIGN$_A$(RASK,h_A)
C_{DA}=<ID,RAPK,H$_A$,sign$_1$>
Verify sign$_1$
Generate signing certificate
cert$_A$=<ID,RAPK,H$_A$,T_{sign},T_{expire}>
Calculate h_{CA}=H$_C$(ID||RAPK||H$_A$||T_{sign}||T_{expire})
Generate IASK
Calculate sign$_2$=SIGN$_C$(IASK,h_{CA})
C_{UA}=<cert$_A$,H$_C$,sign$_2$>

Figure 3. Signing process

S1 Participant A generates an ID according to its own identity information and generates a group of working public and private key pairs (RASK, RAPK) according to the working cryptographic algorithm.

S2 Participant A uses its own hash function H_A to calculate $\mathrm{h_A} = \mathrm{H_A}(\mathrm{ID}||\mathrm{RAPK})$. Then, participant A sends $\mathrm{C_{DA}} =< ID, \mathrm{RAPK}, \mathrm{H_A}, \mathrm{sign}_I >$. The signature algorithm $SING_A$ is used to encrypt $\mathrm{h_A} = \mathrm{H_A}(\mathrm{ID}||\mathrm{RAPK})$

S3 The cloud center verifies the digital signature $sign_I$. Ensure the authenticity and uniqueness of participants' identities. If the verification is passed, continue to perform the following steps; Otherwise, the authentication is terminated. After the verification of the authentication request is passed, the cloud center returns a certificate C_{UA} to participant A, and the generation process is shown in $1) \sim 5)$:

1) The Cloud Center first determines the signing time Tsign and the cancel time Texpire of the certificate to obtain the certificate $cert_A$ $=< \mathrm{ID}, \mathrm{RAPK}, \mathrm{H_A}, Tsign, Texpire >$;
2) The management center obtains the control information: $h_{CA} = H_C(ID||RAPK||H_A||Tsign||Texpire)$;
3) The management center generates the identification private key IASK of cluster point a through multilinear transformation according to the H_{CA} and the private key base SKB;
4) The management center uses the signature algorithm $SIGN_c$ to encrypt H_{CA} with the identification private key IASK as the key, and calculates $sign_2$= $SIGN_c(IASK, h_{CA})$;
5) After attaching H_C and $sign_2$ to the certificate to be signed $cert_A$, a legal signed certificate C_{UA} $=<$ certA, H_C, $sign_2$ $>$ will be issued to participant A.

After obtaining the certificate, participant A stores the certificate locally. After the Cloud Center sends the certificate to participant A, it records the certificate signing information.

C. Network access authentication

Network access authentication refers to the authentication process of the Cluster Head access Task Publisher or a participant accessing the Cluster Head in the MCS system. This paper takes the process of participant A accessing the MCS system as an example. When participant A wants to access the MCS system and establish a connection with Cluster Head B, participant A needs to send the certificate to Cluster Head B for verification as shou in Fig 4. The verification process is divided into the following steps:

S1 When the participant A uses the certificate, the Time Stamp T_1 is generated according to the current time, and the random number J_1 is randomly generated. The participant A uses its own signature hash function H_A, calculate $Z_A = H_A\left(ID||RAPK||T_1||J_1\right)$ and uses its signature algorithm $SIGN_A$ to get the signature $sign_3 = SIGN_A\left(RASK, H_A\left(ID||RAPK||T_1||J_1\right)\right)$ Participant A generates a certificate $\mathrm{C}_A = \langle C_{UA}, T_1, J_1, sign_3 \rangle$;

S2 After Cluster Head B receives the certificate from participant A, Cluster Head B calculates $\mathrm{H_A}\left(\mathrm{ID}||\mathrm{RAPK}||\mathrm{T_1}||\mathrm{J_1}\right)$, uses rap as the public key for verification, and uses the verification algorithm $Verify_A$ corresponding to $SIGN_A$ to verify whether $Verify_A(RAPK, sign_3,\ H_A(ID||RAPK||\ T_1||J_1))$;

S3 After step 2 is passed, the Cluster Head B inputs $certA$ into H_C to obtain the control information H_{BA} input

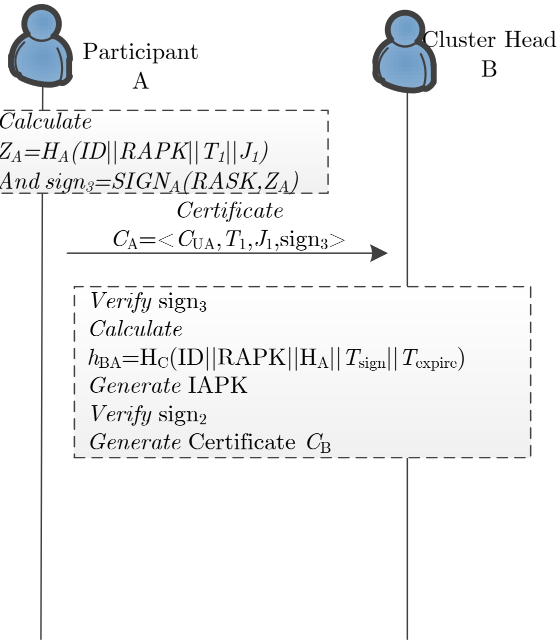
Participant
A
Cluster Head
B
Calculate
$Z_A=H_A(ID||RAPK||T_1||J_1)$
And $sign_3=SIGN_A(RASK,Z_A)$
Certificate
$C_A=<C_{UA},T_1,J_1,\mathrm{sign}_3>$
Verify sign_3
Calculate
$h_{BA}=\mathrm{H_C}(\mathrm{ID}||\mathrm{RAPK}||\mathrm{H_A}||T_{\mathrm{sign}}||T_{\mathrm{expire}})$
Generate IAPK
Verify sign_2
Generate Certificate C_B

Figure 4. Certification process

by the multilinear function; According to the public key base PKB disclosed by H_{BA} and the Cloud Center, the identification public key $IAPK$ of participant $A$is generated through the multilinear function transformation of formula (2);

S4 After Cluster Head B generates IAPK, Cluster Head B calculates $H_C(cert_A)$ according to $cert_A$ and H_C in the certificate C_A. Cluster Head B uses $IAPK$ as the public key for checking and verifies $Verify_C$(IAPK,$sign_2$,$H_C(cert_A)$).

Since both of the participant A and the Cluster Head B were moving, after a period of time of communication, the distance between the two sides might exceed the distance of the communication. At this time, the connection between the participant A and the Cluster Head B would be broken, and the participant A need to choose another Cluster Head within the scope of communication and reconnect the network and verify it to reconnect the MCS system.

D. Revocation of the certificate

The Task Publisher and every Participant and Cluster Head all stored certificate revocation lists(CRL) in the local memory. CRL provided a central management method to inform the other network node when a node's certificate was canceled. The Task Publisher was responsible for maintaining and updating the CRL and announcing it in many ways. The Participant would update their CRL according to the update of the CRL. In the following cases, the system node needed to withdraw the certificate

1 The Certificate Arrives At The Revocation Time. The content of the certificate signed by the Task Publisher for the user node of the MCS system includes the signing time and the revocation time. When the revocation time is reached, the cloud center will revoke the certificate and update the CRL. After the certificate is revoked, the user node reapplies for the certificate from the Cloud Center;

2 The Participant Leaves The Current Coverage Domain. Since the participant is mobile, it may leave the original Cluster Head to cover its coverage area. At this time, the participant needs to find a new Cluster Head again. Take participant A as an example. When participant A leaves the coverage area of its current Cluster Head B due to movement, the Current Cluster head B needs to revoke the certificate it signed for participant A. At this time, the current Task Publisher updates the CRL, then publishes a message to all participant nodes in the coverage area claiming that the certificate signed by participant A is invalid, and publishes the same message to all Cluster Heads, and then the other Cluster Heads forward the message to all participant nodes in the coverage area. The participant node receiving the message adds the certificate of participant A to its CRL. When the participant A enters the coverage area of the new Cluster Head C, it will re apply for the certificate from the new Cluster Head;

3 The Participant Private Key Leakage. Once the working private key RASK currently used by a participant node is leaked for some reason. The participant node must declare to the Cluster Head that the certificate is invalid at the first time. Then the Cluster Head forwards the certificate revocation statement to other participant nodes and other Cluster Heads in the current coverage domain, and then forwards it to all other nodes in the system.

According to all existing nodes in the network, the locally stored CRL is regularly updated, and a new invalid certificate is added to the CRL according to the received revocation message. When performing authentication between the participant and the Cluster Head, the Cluster Head first checks whether the participant certificate has exceeded the validity period and whether it appears in its own CRL. After ensuring that the certificate has not exceeded the validity period and has not been invalidated, the subsequent network access authentication process is performed. The same is true between Task Publishers and Cluster Heads.

V. Strategy Analysis

A. BAN logic analysis

BAN logic, which can take formal describe to the authentication protocol and take formal analysis to the authentication protocol according to the hypothesis. Although the formal analysis of BAN logic can not consider the security defects caused by encryption and operating environment during the specific implementation of the strategy, it can prove the security of the strategy at the level of theoretical analysis and is widely used for the formal analysis of authentication security protocol. In this section, the MCS authentication strategy based on CFL authentication is formally described, and its security is formally analyzed and proved.

Formal analysis of authentication between Participants and Cluster Heads

1) Formal description: Message 1: participant A → Cluster Head $C :< \mathrm{ID, RAPK,}\ H_A, \mathrm{sign}_1 >$

Message 2: Cluster Head → participant A A: $<$ ID, RAPK, $\mathrm{H_A}, T_{\text{sign}}\ , T_{\text{expire,}}\ , \mathrm{Hc_c}, \mathrm{sign}_2 >$

Let $I_0 = \langle\ \mathrm{ID, RAPK,\ H_A}\rangle, I_1 = \langle T_{\text{sign}}\ , T_{\text{expire,}}\ \mathrm{H_C}, \mathrm{sign}_2\rangle$

2) Protocol target: Participant $A \mid\equiv I_1$

3) Initial assumptions::

1 Participant $A \mid\equiv A \overset{I_0}{\rightleftharpoons} C$
2 Participant $A \triangleleft \{I_0, I_1\}$
3 Participant $A \mid\equiv \#(I_1)$
4 Participant $A \mid\equiv C \Rightarrow I_1$

4) BAN Logic Deduction: From the initial assumption 1,2, it can be deduced according to the message meaning rules:

$$\frac{A \mid\equiv C \overset{I_0}{\rightleftharpoons} A, A \triangleleft \{I_0, I_1\}}{A| \equiv C| \sim (I_0, I_1)} \tag{3}$$

From the initial assumption 3,it can be deduced according to the freshness of the news:

$$\frac{A \mid\equiv \#(I_1)}{A \mid\equiv \#(I_0, I_1)} \tag{4}$$

From 3, 4, it can be deduced according to the temporary verification rule:

$$\frac{A| \equiv C| \sim (I_0, I_1), A \mid\equiv \#(I_0, I_1)}{A| \equiv C| \equiv (I_0, I_1)} \tag{5}$$

From Eq5 according to the belief rule:

$$\frac{A| \equiv C| \equiv (I_0, I_1)}{A| \equiv C| \equiv I_1} \tag{6}$$

rom the assumptions 4 and Eq6, it can be deduced according to the governing rule:

$$\frac{A \mid\equiv C \Rightarrow I_1, A| \equiv C \mid\equiv I_1}{A \mid\equiv I_1} \tag{7}$$

The above logic proves the Protocol target, and the participant A trusts the validity and authenticity of the certificate signed by the Cluster Head, thereby trusting the identity of the Cluster Head. The same is true for Cluster Heads and Task Publishers.

B. Security analysis

1) Decentralized self certification: This strategy continues the characteristics of CFL technology to certificate centralization, mainly reflected in the following two aspects: 1. Enerating a signature key pair based on the public-private key base and the identity ID: Different from the process of private key signature by CA in PKI system, CFL certificate generation center uses the identity ID of the registration node and the private key base SKB to generate the corresponding identification private key IASK based on the multilinear function. The verifier can also directly generate the identification public key IAPK for verification through the public key base PKB and the identity ID of the other party. This signature public-private key generation method does not involve the private key of the certification center, and eliminates the dependence of the certificate generation on the private key of the certification center. It can avoid the leakage of the private key of the certification center and reduce the possibility of identity forgery of the certificate generation center. 2. Third party is required to participate in the verification stage: PKI and IBE authentication require CA back certification and KGC to issue key pairs to complete the identity authentication of both parties, which belongs to a typical central authentication mechanism. However, the strategy in this paper does not involve any third party in the authentication process. Only by exchanging and verifying each other's dynamic certificates, the two parties can independently realize the identity authentication of the other party, which reduces the communication cost in the authentication process, and can also prevent the people in the middle attack launched by the dishonest third party entity on the authentication process.

TABLE I
COMPARISON OF COMMUNICATION COST OF EACH SCHEME

Scheme	Registration stage	Verification phase	Total communication cost
PKI	$2RC$	$2RC + 2RV$	$4RC + 2RV$
CFL	$2RC$	$2RV$	$2RC + 2RV$
IBE	$3RC$	$2RV$	$3RC + 2RV$

2) Defense Replay Attacks: The strategy in this paper uses time stamps technology to resist replay attacks. When the certificate sender sends the certificate to the authenticator, it needs to add the time stamp T1 and the random number J1 to the content of the certificate, and then send the time stamp T1, the random number J1 and other parameters to the authenticator after signing. Due to the freshness of T1 and J1, when the attacker replays the intercepted certificate to the verifier, the verification fails. Effectively preventing replay attacks.

C. Performance Analysis

1) Communication Cost: This section compares the communication cost of the strategy proposed in this paper with other relevant schemes. The registration phase includes the user submitting the relevant identity information to the certificate generation center, and the certificate generation center generates the corresponding certificates and random numbers. The authentication stage is the authentication process of the user. Let RC be the remote communication between the device and the authentication center, including the communication cost with the certificate generation center (CGC) and the authentication center (CA), and RV be the communication cost between the user nodes (Cluster Heads and Participants). The table compares the communication cost of the strategy in this paper with that of other schemes.

It can be seen from the Table I that the communication cost of the strategy in this paper is the same as that of the scheme IBE and is superior to that of the scheme PKI. Because in this scheme, the Inter Cluster authentication or the authentication between the Cluster Head and the Task Publisher does not

TABLE II
COMPARISON OF CALCULATION COST OF EACH SCHEME

Scheme	Registration stage	Verification phase	Total communication cost
PKI	2H+2PM+1PA+RNG	4H+6PM+3PA+RNG	6H+8PM+4PA+2RNG
CFL	2H+7PM+3PA+2RNG	H+7PM+3PA	3H+14PM+6PA+2RNG
IBE	2RNG+6H+4PM	3PM+PA+6H	12H+7PM+PA+2RNG

TABLE III
SERVER CONFIGURATION

Configuration	Cloud Server	Local Server
Processor	Intel Xeon Platinum 8255C @ 2.50GHz	Intel(R) Core(TM) i7-7500U CPU @ 2.70GHz 2.90 GHz
Memory	4GB	8G
Network card	Tencent VirtIO Ethernet Adapter	Intel Dual Band Wireless-AC 3165
Location	Bei Jing,Shang Hai	QingDao

require the participation of the CA, the communication cost can be effectively reduced.

2) Calculation Cost: Generally speaking, the calculation cost of the certificate based authentication scheme is greater than that of the symmetric encryption based authentication scheme, but it is better than the symmetric encryption based authentication scheme in terms of security and application scope.

Next, the calculation cost of the three schemes are compared and analyzed. First, the calculation costs of the three schemes are theoretically compared and analyzed by counting the number of cryptographic operations used in the protocol. H is defined as a hash operation, PM is a point multiplication operation on an elliptic curve, PA is a point addition operation on an elliptic curve, and RNG is a random number calculation.The average time of different cipher calculations calculated by Kilic et al. Based on the PBC library is: 0.0023ms for H, 2.226ms for PM, 0.0288ms for PA, and 0.539ms for RNG. In the theoretical comparison experiment, the number of hash operations is counted when the security parameter is 256. The specific comparison is shown in the Table II.

As can be seen from the above table, the PM operation coefficient of CFL is larger than PKI and IBE, so in general, the calculation cost of CFL is larger than PKI and IBE.

3) Experimental test: This section will compare with other schemes in the references through specific experimental tests. In the authentication system of MCS system based on CFL, the total throughput and total response time of the system in the registration phase and the verification phase are mainly completed through experimental tests. The Cloud Server and Local Server information of the experimental environment are showed in Table III.

In the experimental test, the secp256k1 elliptic curve standardized by NIST is used as the benchmark. SM3 is used for security parameters and hash functions, and SM2 is used for signature and verification functions. The test program is based on the open source cryptography library Bouncy Castle to realize the calculation on the elliptic curve. It is written in Java language and developed on the PC side. The cloud server is Tencent cloud server. The main operating environment is as follows:

In this experiment, without considering the network delay, we tested three schemes respectively. The test tool is Apache JMeter, and the seed key length is 128 bit. Each group of data is taken as the average value of 20 rounds of experimental data. The specific comparative experimental results are shown in the figures. As can be seen from the above table, the PM operation coefficient of CFL is larger than PKI and IBE, so in general, the calculation cost of CFL is larger than PKI and IBE.

It can be seen from the Fig 5 that the system throughput of the three schemes increases gradually with the increase of the number of registered participants. The system throughput of the CFL scheme proposed in this paper is higher than that of the PKI scheme and much higher than that of the IBE scheme. It can be seen from the Fig 6 that the three schemes all increase with the increase of the number of users, of which CFL has the least system response time and IBE has the most system response time. In the identity authentication system of the actual MCS system, the user generally performs one registration and one verification. After the verification, the data is transmitted within the specified time and range. If it exceeds the specified time, the data will be invalid. If it exceeds the coverage area of the Cluster Head, it needs to be reregistered

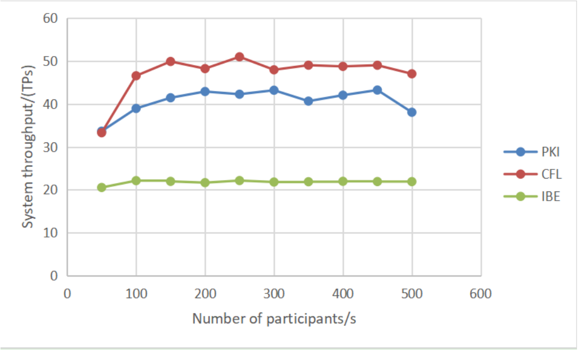

Figure 5. System throughput

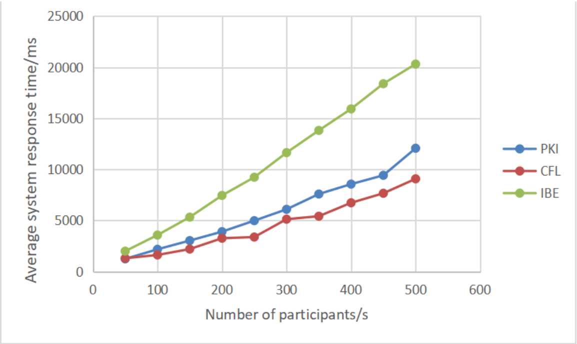

Figure 6. Average system response time

and verified with the new Cluster Head.

VI. Conclusion

Aiming at the characteristics and security requirements of MCS, this paper Identity authentication strategy of Mobile Crowd Sensing based on CFL. This strategy realizes three parts of identity authentication, and the whole process does not need the participation of a third-party center; On this basis, this paper analyzes the security and efficiency performance of the authentication strategy, and uses BAN logic formal analysis method to analyze the security of the strategy in detail. The results show that this policy can achieve the expected security objectives, effectively reduce the number of third-party servers, prevent replay attacks and other attack means, and ensure the efficient and safe operation of the system. On the basis of ensuring security, the communication cost and calculation cost are reduced, and the authentication efficiency is improved.

Acknowledgment

This work was funded by the Natural Science Foundation of Shandong Province under Project ZR2019MF034, in part by the National Natural Science Foundation of China (NSFC) under grant No. 62111530052.

References

[1] Nguyen T N, Zeadally S. Mobile crowd-sensing applications: Data redundancies, challenges, and solutions[J]. ACM Transactions on Internet Technology (TOIT), 2021, 22(2): 1-15.

[2] Huanan Z, Suping X, Jiannan W. Security and application of wireless sensor network[J]. Procedia Computer Science, 2021, 183: 486-492.

[3] Miraz M H, Ali M, Excell P S, et al. A review on Internet of Things (IoT), Internet of everything (IoE) and Internet of nano things (IoNT)[J]. 2015 Internet Technologies and Applications (ITA), 2015: 219-224.

[4] Ghazal T M, Hasan M K, Alshurideh M T, et al. IoT for smart cities: Machine learning approaches in smart healthcare—A review[J]. Future Internet, 2021, 13(8): 218.

[5] Sun Z, Wang Y, Cai Z, et al. A two-stage privacy protection mechanism based on blockchain in mobile crowdsourcing[J]. International Journal of Intelligent Systems, 2021, 36(5): 2058-2080.

[6] Taherdoost H. Data Collection Methods and Tools for Research; A Step-by-Step Guide to Choose Data Collection Technique for Academic and Business Research Projects[J]. International Journal of Academic Research in Management (IJARM), 2021, 10(1): 10-38.

[7] Zhang D, Wang L, Xiong H, et al. 4W1H in mobile crowd sensing[J]. IEEE Communications Magazine, 2014, 52(8): 42-48.

[8] Diaz-Sanchez D, Marin-Lopez A, Mendoza F A, et al. TLS/PKI challenges and certificate pinning techniques for IoT and M2M secure communications[J]. IEEE Communications Surveys & Tutorials, 2019, 21(4): 3502-3531.

[9] Unal D, Al-Ali A, Catak F O, et al. A secure and efficient Internet of Things cloud encryption scheme with forensics investigation compatibility based on identity-based encryption[J]. Future Generation Computer Systems, 2021, 125: 433-445.

[10] LAN S B, LI P X, DAN L X. CFL-based Industrial Control System Authentication Communication Scheme[J]. Journal of Computer Applications, 0.

[11] Gummidi S R B, Xie X, Pedersen T B. A Survey of Spatial Crowdsourcing[J]. ACM Transactions on Database Systems, 2019, 44(2):8:1–8:46.

[12] Shu J, Jia X, Yang K, et al. Privacy preserving task recommendation services for crowdsourcing[J]. IEEE Transactions on Services Computing, in press.

[13] Wu H, Wang L, Xue G. Privacy aware task allocation and data aggregation in fogassisted spatial crowdsourcing[J]. IEEE Transactions on Network Science and Engineering, 2020, 7(1):589–602.

[14] Shu J, Yang K, Jia X, et al. Proxyfree privacy preserving task matching with efficient revocation in crowdsourcing[J]. IEEE Transactions on Dependable and Secure Computing, in press.

[15] Wu Y, Tang S, Zhao B, et al. BPTM: Blockchain Based Privacy Preserving Task Matching in Crowdsourcing[J]. IEEE Access, 2019, 7:45605–45617.

[16] Wu H, Wang L, Xue G, et al. Enabling Data Trustworthiness and User Privacy in Mobile Crowd-sensing[J]. IEEE/ACM Transactions on Networking, 2019, 27(6):2294–2307.

[17] Li Q, Cao G. Providing privacy aware incentives in mobile sensing systems[J]. IEEE Transactions on Mobile Computing, 2016, 15(6):1485–1498.

[18] Qiu F, Wu F, Chen G. Privacy and quality preserving multimedia data aggregation for participatory sensing systems[J]. IEEE Transactions on Mobile Computing, 2015, 14(6):1287–1300.

[19] RAO N, SRIVASTAVA S, SREEKANTH K S. PKI Deployment Challenges and Recommendations for ICS Networks[J]. International Journal of Information Security and Privacy, 2017, 11 (2): 38-48.

[20] DAN B, FRANKLIN M. Identity-Based Encryption from the Weil Pairing J. Siam Journal on Computing, 2003, 32(3): 586-615.

[21] WATERS B. Efficient identity-based encryption without random oracles [C] // Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2005: 114–127.

[22] GENTRY C, PEIKERT C, VAIKUNTANATHAN V. Trapdoors for hard lattices and new cryptographic constructions [C] // Proceedings of the 40th Annual ACM Symposium on Theory of Computing. New York: ACM, 2008: 197-206.

[23] SARVABHATLA M, VORUGUNTI C S. A secure and robust dynamic ID-based mutual authentication scheme with smart card using elliptic curve cryptography [C] // Proceedings of the Seventh International Workshop on Signal Design and its Applications in Communications. Piscataway: IEEE, 2015: 75-79.

[24] KIM S Y, KIM H, LEE D H. An efficient id-based mutual authentication secure against privileged-insider attack [C] // Proceedings of the fifth International Conference on IT Convergence and Security. Piscataway: IEEE, 2015: 1-4.

[25] LINDELL Y. Fast secure two-party ECDSA signing [C] // Proceedings of the 2017 Annual International Cryptology Conference. Cham: Springer, 2017: 613-644.

[26] DOERNER J, KONDI Y, LEE E, et al. Secure two-party threshold ECDSA from ECDSA assumptions [C] // Proceedings of the 2018 IEEE Symposium on Security and Privacy. Washington. DC: IEEE Computer Society, 2018: 980-997.