IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received January 20, 2021, accepted February 1, 2021, date of publication February 10, 2021, date of current version February 19, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3058446

A MADM Location Privacy Protection Method Based on Blockchain

HUI WANG[1], CHENGJIE WANG[1], ZIHAO SHEN[1], KUN LIU[1], PEIQIAN LIU[1], AND DENGWEI LIN[2]

[1]School of Computer Science and Technology, Henan Polytechnic University, Jiaozuo 454000, China
[2]Office of Educational Administration, Jiaozuo University, Jiaozuo 454000, China

Corresponding author: Zihao Shen (hpuxxfzyjs@qq.com)

This work was supported in part by the National Natural Science Foundation of China (61300216).

ABSTRACT Location-based services make life easier, but they also involve privacy leakage issues. Many location privacy protection algorithms have been proposed to protect the privacy of users. However, these algorithms are usually based on theoretical data, and there are no actual user data to support studies of location privacy protection. To address this problem, we introduce a credit value, convert credit data from users into credit values using the multiple-attribute decision making (MADM) algorithm, store the credit values and transaction information from the anonymous zone construction process in conjunction with a blockchain, and propose a credit value reward and punishment mechanism that treats anonymous zone construction as a two-party game between the requestor and participant. In this game, a credit value reward and punishment mechanism is used to constrain undesirable behaviors. Through simulation experiments, it is verified that the method can be applied in practical scenarios, effectively constrain undesirable user behaviors, quickly construct anonymous zones, and reduce the probability of user location leakage issues.

INDEX TERMS Location-based services, blockchain, anonymous zone, MADM algorithm, credit value reward and punishment mechanism.

I. INTRODUCTION

With the rapid development of the mobile Internet and information technology, location-based services (LBSs) are widely used and have become an indispensable part of people's lives. Human life is closely integrated with smart mobile applications, and the development of location sensing technology such as data communication and sensor equipment in mobile intelligent terminals will enable the digitization of the geographical locations of people and objects [1]. A location-based service [2]–[3] is a value-added service that combines mobile communication technology and positioning technology to provide location-related services; based on the user's location and query content, it provides the user with various location-related services, such as point-of-interest retrieval, preference ranking, and life services (such as navigation and shopping).

While people enjoy the convenience of LBSs, their location privacy is at risk. Users submit their personal information to the location service provider (LSP) when they use an LBS to request information, and the LSP may illegally obtain personal information for the user, such as their home address, living habits, health information, and work information.

To solve the problem of location privacy protection in LBSs, Gruteser and Grunwald [4] proposed a spatiotemporal anonymity method and applied the k-anonymity model for location privacy protection. The basic idea of this method is that when users send a query request, they obtain the real positions of no fewer than k-1 participants to form an anonymous area and then submit the location of the anonymous area to the LSP to protect their real location [5]. Reference [6] proposed an algorithm based on the CliqueCloak method, which supports users in formulating K-values and preventing privacy leaks by studying edge information. Reference [7] noted that Bamba B *et al.* proposed the privacy grid method, introduced the concept of location diversity, and used a top-down method to divide a space into a grid to obtain an anonymous zone. All of the above K-anonymity methods need a centralized node to act as the central server. As the third-party server in the process of anonymous zone construction, once the central server is breached, the real location information of the users will be easily disclosed. Later,

The associate editor coordinating the review of this manuscript and approving it for publication was Muhammad Imran Tariq.

Chow *et al.* [8] proposed the distributed K-anonymity location privacy protection method, which uses the real locations of historical participants to assist the requestor in constructing an anonymous zone, and the requestor stores the participants' locations after each anonymous zone construction and then directly uses the recently stored participants' locations the next time it makes a request if the number of participants does not meet the location privacy protection needs in anonymous zone construction. To reduce the storage overhead of requestors, Ghinita *et al.* [9] used Hilbert curves to map the location information of requestors and participants from a two-dimensional space to a one-dimensional space and to store the one-dimensional location information of the users in the data nodes of a B+ tree to form K-anonymity zones based on the information of the nodes in the tree; however, when the number of participants is large, the requestors need to be aware that the root nodes of the B+ tree are retrieved one by one, thus significantly increasing the computational cost accrued by the requestor. To solve this problem, reference [10] noted that Kalnis *et al.* used a ring structure instead of the above structure to store the one-dimensional location information of the user, thereby allowing the requestor to quickly construct an anonymous zone. Cho *et al.* [11] suggested that the requestor should take the actual geographic position into account when posting information and that inaccurate geographic information may directly reveal the user's true information; therefore, they created geography that was as real as possible to improve the level of privacy regarding the user's location. Kim *et al.* [12] proposed a grid-based distributed K-anonymity location privacy protection scheme by using information entropy to measure the level of location privacy protection for the requesting user. Che *et al.* [13] proposed a two-way active distributed K-anonymity privacy protection scheme in which all users in the network actively provide their real locations to participate anonymously. Sun *et al.* [14] classified the real locations of all users in a network and proposed a distributed K-anonymity privacy protection scheme based on location tags. Hwang and Huang [15] and Zhang *et al.* [16] proposed that an anonymous zone should be constructed by obtaining the participants' real locations through social networks. Gupta and Rao [17] proposed a collaborative P2P communication model to establish trust among peers, effectively protect user location privacy and provide efficient operations.

Jia *et al.* [18] proposed a hybrid incentive mechanism that combines a blockchain and virtual credit, and it is useful in stimulating users to participate in anonymous cooperation. Yang *et al.* [19] noted that the original distributed K-anonymity privacy protection schemes assume that participants are honest and reliable. To address this problem, an auction incentive mechanism is proposed that allows multiple requesting users to obtain the true locations of the collaborating users through an auction, thus incentivizing users to participate in the construction of an anonymous zone. Yuan *et al.* [20] designed a winning bid determination rule using a greedy algorithm, which solves the problem that the above scheme is too sensitive in auctioning the number of participant locations that satisfy privacy protection needs in the construction of an anonymous zone considering the requestor's real location. Qiu *et al.* [21] used a combination of multiple private blockchains to disperse user transaction records, thereby providing enhanced location privacy protection for users. Li *et al.* [22] noted that both of the above schemes require the existence of a trusted auctioneer; otherwise, the location information for the requestor and collaborators is highly likely to be leaked to the LSP; they proposed a reputation incentive-based privacy protection scheme for distributed K-anonymity zones.

In summary, the existing K-anonymity location privacy protection schemes are based on theoretical data, and there are no actual user data to support the study of malpractice in location privacy protection, which affects the construction of the anonymous zone and can result in problems such as location leakage and location spoofing. Based on these issues, this paper proposes a blockchain-based MADM approach for location privacy protection, and the research is primarily performed in the following areas:

1) We introduce the concept of credit value, propose the MADM algorithm to convert credit data from users' lives into credit values, and propose a credit value reward and punishment mechanism to limit the adverse behaviors of the requestors and participants.
2) Based on the blockchain and the credit value reward and punishment mechanism, the transaction bill during the construction of the anonymous zone is stored in a public chain, and the credit value will be increased or decreased according to the different selection strategies of the requestors and participants and the changes in the credit values to limit the adverse behavior of the users and encourage them to actively participate in the construction of the anonymous zone.
3) Adequate experiments were conducted on the scheme to verify the practicality of the method. When a requestor uses the method to construct an anonymous zone, the requestor and participants are able to limit their own undesirable behaviors. That is, the participants provide real information to participate in the construction of the anonymous zone; the requestor does not reveal the real locations of the participants, thus creating a benign anonymous construction environment and enabling the efficient construction of the anonymous zone while reducing the user location leakage rate.

II. PREPARATORY KNOWLEDGE

A. RELEVANT DEFINITIONS

In this paper, the concept of credit value is introduced based on blockchain technology. A user's real-life credit (from Alipay, banks, shopping apps, etc.) is converted to credit value H through multiattribute decision making. The determination of this value depends on the actual credit situation of the user.

When assessing anonymity, the converted credit reference value H is compared with the privacy security measure value δ given by the system in the blockchain to make corresponding decisions. The relevant definitions are given below.

Definition 1: (The anonymous construction model M_{ANA}). The anonymous construction model is a 5-tuple model $M_{ANA} = (U, P, H, T, \delta)$, where $U = \{U_0, U_i\}$ is the set of requestors and participants, U_0 represents the requestor, and U_i represents the participant.

$P = \{P_0, P_i\}$ is the set of strategies used by both requestors and participants to construct an anonymous zone. $P_0 = \left\{p_0^1, p_0^2\right\}$ is a set of strategies for the requestor: p_0^1 indicates that requestor U_0, after receiving the location Loc_i of participant U_i, does not disclose it to a third party; p_0^2 indicates that requestor U_0 leaks information to a third party upon receipt of the location Loc_i of participant U_i. $P_i = \left\{p_i^1, p_i^2, p_i^3\right\}$ is a set of participant choices: P_i^1 indicates that participant U_i provides the true location Loc_i^{real} to requestor U_0; p_i^2 indicates that participant U_i does not provide this information to requestor U_0; and p_i^3 indicates that participant U_i provides false information Loc_i^{Phoney} to requestor U_0.

$H = \{H_0, H_i\}$ is the set of credit values for the requestor and participant. H_0 indicates the requestor's credit value, and H_i indicates the participant's credit value.

T is the timestamp of the moment when requestor U_0 sends the constructed anonymous zone; requestor U_0 and participant U_i correspond to a unique credit value H at each moment T.

δ is a privacy and security metric, and δ can be given as many different values to determine whether a user can participate in the construction of the anonymous zone by comparing these values to the credit value.

Definition 2: (Data reading function f). The reading function is $f\ (D) = (PL_{name}, UID, D, T)$, where PL_{name} denotes the name of the institution from which the data came.

$UID = \{N_0ID, U_iID\}$ is the set of user IDs; U_0ID is the requestor's ID; and U_iID is the participant's ID.

$D = \left\{D_{ij}\right\}$ is a set of indicator data values for each user agency, and D_{ij} represents the j-th institutional indicator value for the i-th user ($1 \le i \le m, 1 \le j \le n$); for example, D_{i1} is the first indicator value for the i-th user, and D_{1j} is the j-th indicator for the first user.

T is the timestamp associated with the time when the data are input into the read function.

Definition 3: (Data indicator values D_{ij}^Z). With the read function, one can obtain sets of data values $D = \left\{D_{ij}\right\}$ for different organizations and different users; assuming that m users are read and n agency indicator values are used, the indicator values for each user can form an indicator matrix $\left(D_{ij}\right)_{m\times n}$:

$$\left(D_{ij}\right)_{m\times n} = \begin{pmatrix} D_{11} & \cdots & D_{1n} \\ D_{21} & & D_{2n} \\ \vdots & D_{ij} & \vdots \\ D_{m1} & \cdots & D_{mn} \end{pmatrix} \tag{1}$$

To compare the data, a multiattribute decision method is applied to normalize the values and map them to the interval [0, 1]; then, the normalized indicator matrix is obtained from Equation (1):

$$\left(D_{ij}^Z\right)_{m\times n} = \begin{pmatrix} D_{11}^Z & \cdots & D_{1n}^Z \\ D_{21}^Z & D_{1n}^Z & \\ \vdots & D_{ij}^Z & \vdots \\ D_{m1}^Z & \cdots & D_{mn}^Z \end{pmatrix} \tag{2}$$

We set max (D_i) as the maximum value in column i of the indicator matrix and the minimum value in column j of the indicator matrix, with a 0-1 standard conversion for the indicator value. Corresponding conversions are required for different attribute indicators, as follows:

Efficiency indicator:

$$D_{ij}^Z = \frac{D_{ij} - \min\left(D_i\right)}{\max\left(D_i\right) - \min\left(D_i\right)} \tag{3}$$

Cost indicator:

$$D_{ij}^Z = \frac{\max\left(D_i\right) - D_{ij}}{\max\left(D_i\right) - \min\left(D_i\right)} \tag{4}$$

Fixed indicator, where the fixed value is B:

$$D_{ij}^Z = 1 - \frac{D_{ij} - B_j}{\max\left|D_{ij} - B_j\right|} \tag{5}$$

Definition 4: (Indicator weighting factor W). Given that the data weight coefficients for each of the different agency indicators are $W = (w_1, w_2, \ldots, w_n)$, the relative importance of indicator i to indicator j is given as r_{ij}, and we assume that r_{ij} is the approximate value of the ratio of the weight factor w_i for indicator i to the weight factor w_j for indicator j. Additionally, $r_{ij} \approx w_i/w_j$; this is the first pairwise comparison of the importance of the indicators. For n indicators, $C_n^2 = \frac{1}{2}n(n-1)$ comparisons need to be made, and the results of the pairwise comparisons of the n targets yield the matrix R:

$$\begin{aligned} R &= \begin{pmatrix} r_{11} & r_{12}\ldots & r_{13} & \\ r_{21} & r_{22} & \ldots & r_{23} \\ \ldots & \ldots & \ldots & \ldots \\ r_{31} & r_{32}\ldots & r_{33} & \end{pmatrix} \\ &\approx \begin{pmatrix} w_1/w_1 & w_1/w_2 & \ldots & w_1/w_n \\ w_2/w_1 & w_2/w_2 & \ldots & w_2/w_n \\ \ldots & \ldots & \ldots & \ldots \\ w_n/w_1 & w_n/w_2 & \ldots & w_n/w_n \end{pmatrix} \end{aligned} \tag{6}$$

According to the matrix R, the weight coefficient W for each indicator is obtained by the Lagrange multiplier method.

Lagrange multiplier (LMM):

$$L\left(x, \lambda\right) = f\ (x) + \sum_{k=1}^{l} \lambda_k h_k\ (x) \tag{7}$$

where λ_k is the Lagrange multiplier, λ, and K is a coefficient that is determined for each constraint.

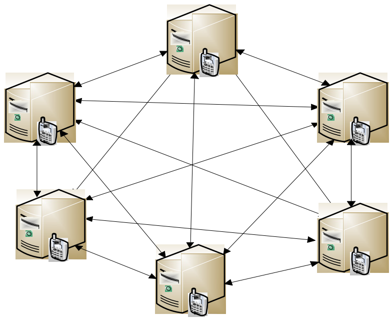

FIGURE 1. **P2P pair equality network structure.**

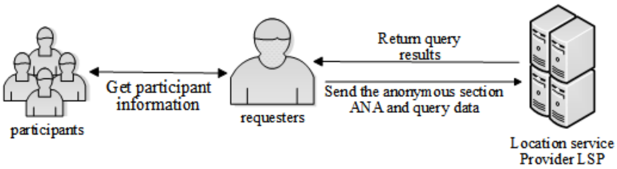
participants
Get participant information
requesters
Return query results
Send the anonymous section ANA and query data
Location service Provider LSP

FIGURE 2. **System structure.**

B. SYSTEM STRUCTURE

The system is structured as a peer-to-peer (P2P) network, as shown in FIGURE 1. The entire process, which requires no third-party intervention, consists of a requestor, participants and an LSP. When the requestor sends a query to the LSP, it also sends a collaboration request to the surrounding participants to obtain their real locations Loc_i^{real}, and after receiving the real locations $Loc_1, Loc_2, \ldots, Loc_n$ from participants $U_1, U_2, \ldots, U_n$, an anonymous zone ANA is constructed via a blockchain. The anonymous zone and query data are then submitted to the LSP. When the LSP authenticates the identity of the requestor, the submitted anonymous zone ANA and query data are retrieved, the query results are returned to the requestor, the feedback is filtered according to the actual location Loc_0^{real}, and accurate query results are obtained. This process is illustrated in FIGURE 2.

III. BLOCKCHAIN-BASED APPROACH TO MADM LOCATION PRIVACY PROTECTION

The existing distributed k-anonymity location privacy protection schemes have the following problems.

(1) Location leaks. After receiving the real location provided by the participant, a self-interested requester may disclose the location information to a third party, or a malicious user may be disguised as the requester to obtain the participant's real location, resulting in the location disclosure of the participant.

(2) Deception. After receiving the construction request from the requester, even if the participant is in a special area, because of self-interest, he or she may still provide a false location to the requester to improve his or her credit value so that he or she can successfully construct a greater anonymous area.

In this section, we define the anonymous zone construction model M_{ANA}, introduce the concept of credit value, and design a reward and punishment mechanism for user information leakage due to bad behaviors in the anonymous zone construction process. In the anonymous zone construction process, requestors and participants choose different strategies to maximize their own interests, which may result in revealing private locations and providing false location information, resulting in the discovery of requestor information or the disclosure of participant information. The proposed MADM algorithm converts credit data from users' real lives into credit values as an important constraint for users in constructing anonymous zones; a reward and punishment mechanism is used to constrain the bad behaviors of users in constructing the anonymous zone and to motivate them to actively participate in the construction of the anonymous zone to minimize the probability of user location leakage and protect location privacy.

A. MADM ALGORITHM

In anonymous zone construction, a requestor U_0 and participant U_i establish their behavior selection policies based on the user's credit value H. The credit value H is determined by the actual credit data for the user, which involves a data set, data preprocessing, and the weights of the data. Therefore, this method proposes transforming the actual credit data for a user with the MADM algorithm to calculate the credit value.

Based on Equation (4), after obtaining the data set, the value of each indicator D_{ij}^Z can be obtained after data normalization. Then, from Equation (5), the n targets can be compared in pairs to obtain the matrix R. From the matrix R, we obtain

$$\left\{\begin{array}{ll} r_{ij} = 1/r_{ji} & \\ r_{ij} = r_{ik} \cdot r_{kj} & (\forall i, j, k \in J) \\ r_{ii} = 1 & \end{array}\right\} \tag{8}$$

The relative importance of indicator i to indicator j is found as $\sum\limits_{i=1}^{n} r_{ij}$:

$$\sum_{i=1}^{n} r_{ij} = \frac{\sum\limits_{i=1}^{n} w_i}{w_j} \tag{9}$$

From Equation (9), we know that when $\sum\limits_{i=1}^{n} w_i = 1$, we have

$$w_j = \frac{1}{\sum\limits_{i=1}^{n} r_{ij}} \tag{10}$$

According to the least-squares method, we have

$$\sum_{i=1}^{n} w_i = 1$$

$$\min\{\sum\nolimits_{i=1}^{n} \sum\nolimits_{j=1}^{n} (r_{ij}w_j - w_i)^2\} \tag{11}$$

$$w_i > 0 i = 1, 2, \ldots, n$$

According to Equation (7), we have

$$L=\sum_{i=1}^{n}\sum_{j=1}^{n}(r_{ij}w_j-w_i)^2+2\lambda(\sum_{i=1}^{n}w_i-1) \tag{12}$$

$$\sum_{i=1}^{n}(b_{il}w_l-w_i)a_{il}-\sum_{j=1}^{n}(b_{lj}w_j-w_l)+\lambda=0,$$
$$l=(0,1,2,\ldots,n) \tag{13}$$

According to Equations (13) and $\sum_{i=1}^{n}w_i=1$, the weight coefficient $W=(w_1,w_2,\ldots,w_n)$ can be derived.

Based on the value of each indicator D_{ij}^{Z} and the weight coefficient W, we calculate the user's credit value H according to the weighted arithmetic average operator (WAA):

$$\begin{aligned}H\left(H_0,H_i\right)&=\frac{1}{n}WAA\left(D_{11},D_{21},D_{ij}\ldots,D_{mn}\right)\\&=\frac{1}{n}\sum_{j=1}^{n}w_jD_{ij}^{Z}\end{aligned} \tag{14}$$

The algorithm for calculating the credit reference value is given below.

Algorithm 1 MADM algorithm

```
Input: number of users m, number of institutions n.
Output: user credit data set S, credit value H.
Step 1 for each i in (1:m):
Step 2     for each j in (1:n): //Initialize m, n
Step 3       function f reads data;
Step 4     end;
Step 5 end;
Step 6 output S;
Step 7 use multiple-attribute decision making to calculate $\left(S_{ij}^{Z}\right)_{m\times n}$, $S_{ij}^{Z}$;
Step 8 use the least-squares method to obtain the matrix R, and then $R\overrightarrow{LSQLMM}W$
Step 9 calculate credit value H, $\left(S_{ij}^{Z}\right)_{m\times n}$, $S_{ij}^{Z}\overrightarrow{WAA}H$
Step 10 output H
```

The MADM algorithm uses the reading function and multi-attribute decision to convert the user's real life credit value into a credit reference value, which lays a theoretical foundation for the subsequent construction of users anonymous. Lines 1-6 of the algorithm represent that the model reads data through a read function loop to get set S. Lines 7-10 of the algorithm show that the data is transformed through multi-attribute decision-making, and the corresponding credit value of the user is calculated.

B. CREDIT VALUE REWARD AND PUNISHMENT MECHANISM

Definition 5: The credit value reward and punishment mechanism $G_h=\left(a^d,H\right)$ is a binary set in which $a^d=\left(a_0^d,a_i^d\right)$ is the d-th anonymous zone construction process and the strategies for requestor N_0 and participant N_i are a_0^d and a_i^d, respectively.

For the definition of H, see Definition 1.

This section introduces the reward and punishment mechanism for the credit value, which constrains the user's behavior through changes in the credit value according to different choices made by the user in the process of constructing the anonymous zone to protect the user's location privacy. Assume that during the construction of the d-th anonymous zone, the choice $a_0^{d(1)}$ means that requestor U_0 does not disclose the location Loc_i^d provided by participant U_i to a third party after receiving it; the choice $a_0^{d(2)}$ means that requestor U_0 discloses the location to a third party after receiving it from participant U_i; the choice $a_i^{d(1)}$ means that participant U_i provides the real location to requestor U_0; the choice $a_i^{d(2)}$ means that participant U_i does not provide the location to requestor U_0; and the choice $a_i^{d(3)}$ means that participant U_i provides a false location to requestor U_0. Then, the changes in credit values for requestor U_0 and participant U_i are as follows:

$$H_0=\begin{cases}H_0+\theta, & a_0^d=a_0^{d(1)}\\ H_0-\theta, & a_0^d=a_0^{d(2)}\end{cases} \tag{15}$$

$$H_i=\begin{cases}H_i+\theta, & a_i^d=a_i^{d(1)}\\ H_i, & (H_0<\delta)\,a_i^d=a_i^{d(2)}\\ H_i-\theta, & (H_0\geq\delta)\,a_i^d=a_i^{d(2)}\\ H_i-\theta, & a_i^d=a_i^{d(3)}\end{cases} \tag{16}$$

where θ denotes the measure of the change in the credit value H in anonymous zone construction, which is a given fixed value.

When $H_0>\delta$, participant H_i acts only when a request is received; otherwise, participant H_i does not respond. When $H_0\geq\delta$ but participant H_i does not provide location information, the participant is punished.

C. ANONYMOUS ZONE CONSTRUCTION PROCESS

This paper treats the anonymous zone construction process as a kind of transaction in which the identity information for both parties (ID, participant location information, credit value, etc.) is stored for each transaction in the form of a bill in the public chain of the blockchain, ensuring that transaction billing is irreversible and nonforgeable while enabling the decentralized sharing of information. The parties may use the transaction bill as evidence to verify the existence of bad behavior, such as requestor U_0 disclosing location information or participant U_i providing a false location; if it is proven that requestor U_0 has disclosed location information or participant U_i has provided a false location, as a punishment, the credit values of both will be reduced, thus affecting their ability to successfully construct an anonymous zone as a requestor.

In this paper, the reward and punishment mechanism plays an important role in the construction of an anonymous zone. Users decide whether to participate in the construction of an anonymous zone based on the corresponding credit value H, the privacy security measure δ, and the historical change in the credit value H. In addition, the change in the credit value H directly affects the probability of successfully constructing an anonymous zone, thus motivating users to actively participate in the maintenance of the blockchain. The anonymous zone is constructed as follows.

Step 1: Requestor U_0 sends an anonymous zone construction request Req to participant U_i in the network:

$$Req = \{U_0ID, H_0, O\left(Bill\right), T_{0-i}\ , sign_{sk-U_0ID}\left(Hchange_{U_0}\right) \tag{17}$$

$O\left(Bill\right)$ denotes the set of transaction statements generated during the construction process; T_{0-i} denotes the timestamp when requestor U_0 sends the anonymous zone construction request; $sign_{sk-U_0ID}$ denotes the private key of requestor U_0 in the blockchain; $sign_{sk-U_0ID}\left(Hchange_{U_0}\right)$ denotes the signature protection of $\left(Hchange_{U_0}\right)$ using the private key $sign_{sk-U_0ID}$; $\left(Hchange_{U_0}\right)$ denotes the change in the historical credit value of requestor U_0; and given that $(Hchange_U)$ is 0 or 1, $(Hchange_U) = 0$ means that H decreases, and $(Hchange_U) = 1$ means that H increases.

Step 2: After receiving a request to construct an anonymous zone from requestor U_0, participant U_i first looks at the message sent by requestor U_0, verifies its credit value, and looks up the history of credit value changes in the blockchain for that requestor U_0.

1) If $H_0 < \delta$, then participant U_i does not respond to the requestor's request;
2) If $H_0 \geq \delta$ and $\left(Hchange_{U_0}\right) = 1$, then participant U_i responds to the request and provides a transaction statement $Bill$:

$$\begin{aligned} Bill = \Big\{&U_0ID, H_i, T_{i-0}, Enc_{pk-U_0ID}\left(Loc_i^{real} \parallel T_{i-0}\right), \\ &sign_{sk-U_iID}\left(Enc_{pk-U_0ID}\left(Loc_i^{real} \parallel T_{i-0}\right)\right)\Big\} \end{aligned} \tag{18}$$

1) If $H_0 \geq \delta$ and $\left(Hchange_{U_0}\right) = 0$, participant U_i responds to the request and provides the transaction statement in Equation (18) while publishing a record Hch of the historical credit value changes of requester U_0 to the blockchain:

$$\begin{aligned} Hch = \Big\{&U_0ID, H_{i,} U_iID, \left(Hchange_{U_0}\right), T_{i-0}\ , \\ &sign_{sk-U_iID}\left(Hchange_{U_i} \parallel T_{i-0}\right)\Big\} \end{aligned} \tag{19}$$

where T_{i-0} denotes the time stamp at which the transaction is billed; $pk-U_0ID$ denotes the public key of requestor U_0 in the blockchain; $Enc_{pk-U_0ID}\left(Loc_i^{real} \parallel T_{i-0}\right)$ expresses the secret message of requestor U_0 after encrypting $Loc_i^{real} \parallel T_{i-0}$ with the public key; $Loc_i^{real} \parallel T_{i-0}$ denotes the true location of participant U_i at moment T_{i-0}; and $Hchange_{U_i} \parallel T_{i-0}$ denotes the change in the credit value of participant U_i at time T_{i-0}.

Step 3: After requestor U_0 receives the transaction $Bill$ provided by the participant, the requestor verifies the correctness of the signature information $sign_{sk-U_iID}\left(Hchange_{U_i} \parallel T_{i-0}\right)$ and the credit value H_i of participant U_i based on the participant's public key $PK - U_iID$ in the blockchain. If the validation fails, requestor U_0 does not use participant U_i's location Loc_i^{real} to construct an anonymous zone; if validation is successful, there are three possible scenarios:

1) $H_i < \delta$, so requestor U_0 does not use participant U_i's location Loc_i^{real} to construct an anonymous zone;
2) $H_i \geq \delta$ and $\left(Hchange_{U_i}\right) = 1$, so requestor U_0 uses participant U_i's location Loc_i^{real} to construct an anonymous zone;
3) $H_i \geq \delta$ and $\left(Hchange_{U_i}\right) = 0$, so requestor U_0 uses participant U_i's location Loc_i^{real} to construct an anonymous zone while providing a record of the historical credit value changes to the blockchain for participant U_i:

$$\begin{aligned} Hch = \Big\{&U_0ID, U_iID, \left(Hchange_{U_i}\right), T_{i-0}, \\ &\times sign_{sk-U_0ID}\left(Hchange_{U_0} \parallel T_{i-0}\right), \\ &\times Enc_{PK-U_0ID}\left(Loc_i^{real} \parallel T_{i-0}\right), \\ &\times sign_{sk-U_iID}\left(Enc_{pk-U_0ID}\left(Loc_i^{real} \parallel T_{i-0}\right)\right) \end{aligned} \tag{20}$$

During the construction of the anonymous zone, if steps 2-3) and 3-3) occur, the credit values H of requestor U_0 and participant U_i decrease before anonymous zone construction, and according to Equations (15) and (16), both exhibit undesirable behavior in such a case; according to the reward and punishment mechanism, as punishment, the credit values of both parties will be reduced during anonymous zone construction, as shown in Equation (21):

$$H = \begin{cases} H_0 = H_0 - \theta, & \left(Hchange_{U_0}\right) = 0 \\ H_i = H_i - \theta, & \left(Hchange_{Ui}\right) = 0 \end{cases} \tag{21}$$

When the above situation occurs multiple times, the credit values of both parties will satisfy $H < \delta$; as a result, these users cannot make requests or participate in the construction of an anonymous zone, so this mechanism is a good way to ensure that during the construction of an anonymous zone, requestors and users can trade in good faith for their own profit and actively participate in maintaining the blockchain. Through the above process, an anonymous zone can be successfully constructed when more than $K - 1$ eligible participants U_i provide information to requestor U_0, and the entire transaction is recorded in the public chain of the blockchain.

IV. SCHEME ANALYSIS

A. SECURITY ANALYSIS

The credit value reward and punishment mechanism introduced in this paper is based on a blockchain with a third-party service provider replaced by smart contracts [23]; this mechanism runs synchronously in all nodes of the public blockchain, has a peer-to-peer structure among nodes, and allows the distributed storage of transaction data. If some of the public blockchain nodes suffer from a distribution denial during a service attack, all transaction bills will remain available and be stored at other public blockchain nodes; additionally, the anonymous construction process will not be interrupted or stopped.

In anonymous zone construction, all users use a string of numerical accounts when transmitting information, as in Equation (17), and use an asymmetric key to encrypt the data to construct the anonymous zone, thus making it difficult for an attacker to decipher the encryption keys of all users and ensuring maximum information security. According to the credit value introduced in this paper, the user determines the credit value H after verifying the transmitted information using a secret key. This paper introduces the privacy and security metric δ. The transaction can be carried out when $H \geq \delta$. If it cannot be carried out and the construction of an anonymous zone fails, the proposed mechanism of rewards and punishments for credit values also maximizes the constraints related to bad user behavior.

The above case fully demonstrates the security of this method. The exchange of information between the two parties is encrypted and decrypted throughout the anonymous construction process, and the introduction of a trustworthiness value provides a guarantee that both the requestor and the participant have performed well in previous anonymous constructions and are actively maintaining the security of the blockchain. The solution prompts the participants to provide truthful information about themselves to the requestor while preventing the requestor from revealing their information, thus improving the quality of the service.

B. PRIVACY PROTECTION DEGREE

By incorporating k-anonymity technology, we assume that requester N_0 and participant N_i are ideal and that there are at least k-1 users with credit reference value $H \geq \delta$ in the network to participate in the construction of an anonymous area *ANA*. After requester N_0 receives the real locations $Loc_1^{real}, Loc_2^{real}, \ldots, Loc_{K-1}^{real}$ provided by participants N_i, equation (22) holds, indicating that the probability that the LSP can identify a real location in an anonymous area is no greater than *1/K*.

$$Nr_{LSP}\left[Loc_0^{real}|Area\left(Loc_1^{real}, Loc_2^{real}, \ldots, Loc_{K-1}^{real}\right)\right] \leq 1/K \qquad (22)$$

The construction process of anonymous areas is based on blockchains. All users communicate with pseudonyms to block the association of real information with users. The requestors and participants each have their own sets of public and private keys Enc_{pk-N_0ID}, $sign_{sk-N_0ID}$, Enc_{pk-N_iID}, $sign_{sk-N_iID}$, which are used to validate the information published by the requester before the participant provides information. Only when validation passes can the choice regarding sending information be made. When a requester receives participant information, he or she also uses the secret key to verify the information and make his or her choice. Transaction bills for the entire process are stored in the public chain, and as a result, the data are tamper and forgery proof, thus guaranteeing user location privacy to the greatest extent possible.

TABLE 1. Experimental parameters.

Parameter	Parameter specification	Parameter range
U_0	number of requesters	$20 \leq N_0 \leq 100$
U_i	number of participants	$20 \leq N_i \leq 100$
K	privacy demand value	$2 \leq K \leq 20$
δ	privacy and security metrics	$0.2 < \delta < 1$
H_0	requestor's credit value	$0 \leq H_0 \leq 1$
H_i	participant's credit value	$0 \leq H_i \leq 1$

V. EXPERIMENTS

The experiments use the Ethereum version 1.6.0 blockchain platform to build the anonymous zone and blockchain. Ethereum is the most commonly used blockchain platform that is open source and modular and provides smart contract functionality. The elliptic curve cryptography (ECC) encryption algorithm is chosen for cryptographic signature protection in the anonymous zone construction process; it is one of the most suitable cryptographic signature algorithms for mobile terminals. All experimental algorithms are implemented in Java, and the method is validated through a series of simulation experiments. The experimental environment includes an Intel(R) Core(TM) i7-9750U 2.60 GHz CPU, a 16 GB DDR3L at 1600 MHz, and a Windows 7 64-bit operating system. The detailed experimental parameters are shown in TABLE 1.

To effectively assess the advantages of this method, the user location privacy leakage rate is considered. The following formula is used to calculate the user location privacy leakage probability:

$$P(r) = \frac{m\left(change_{U_0} = 0\right) + m\left(change_{Ui} = 0\right)}{m\left(U_0 + U_i\right)} \times 100\% \qquad (23)$$

where $m\left(change_{U_0} = 0\right)$ is the amount of location information leaked by requester U_0 to participant U_i, $m\left(change_{Ui} = 0\right)$ is the amount of false location information provided by participant U_i to requester U_0, and $m\left(U_0 + U_i\right)$ is the total number of requesters U_0 and participants U_i.

A. THE EFFECT OF A USER'S CREDIT VALUE ON THE CONSTRUCTION OF AN ANONYMOUS ZONE

The effect of the credit values of requestor U_0 and participant U_i on the success rate of anonymous zone construction during the anonymous zone construction process is analyzed below. In this part of the experiment, the privacy and security metric is $\delta \in (0.2, 1)$, and the number of participants in the network is $\gg K - 1$. The experiment was repeated 100 times for

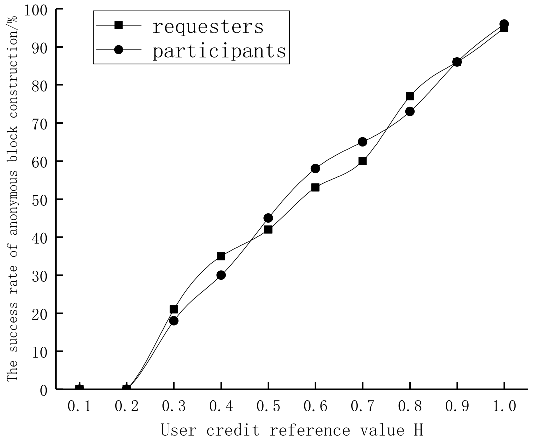

FIGURE 3. Influence of the user credit value on the success rate of anonymous zone construction.

users with different credit values, and the results are shown in FIGURE 3.

It follows from the experiment that for all users involved in anonymous zone construction, according to the concept of credit value introduced in this paper, the participants do not respond when requestor U_0's credit value $H_0 < \delta$, so the success rate of constructing an anonymous zone is zero, and the probability of successfully constructing an anonymous zone increases as H_0 continues to increase. For participant U_i, when the credit value $H_i < \delta$, the user cannot participate in the construction of the anonymous zone; that is, the probability of participating in the successful construction of an anonymous zone is zero. With the continuous increase in H_i, the number of users who can participate in the construction of the anonymous zone also increases, so the probability of successfully constructing the anonymous zone will continue to increase.

B. THE INFLUENCE OF PRIVACY AND SECURITY METRICS ON THE SCHEME

The impact of the privacy and security metric δ on the probability of a requestor revealing location information and the probability of a participant providing a false location are analyzed below. In this part of the experiment, it is assumed that during the anonymous zone construction process, the network is able to successfully construct an anonymous zone with the requestor credit value $H_0 \geq \delta$, the participant credit value $H_i \geq \delta$, and the number of participants $\gg K - 1$. The experiment was repeated 100 times for different δ values, and the results are shown in FIGURE 4 and FIGURE 5.

The experiments suggest that as the privacy and security metric δ increases, the probability of a requester revealing location information and the probability of a participant providing a false location decrease significantly; since the requestor satisfies $H_0 \geq \delta$ and $H_i \geq \delta$ in the anonymous zone construction process, H_0 and H_i are also relatively large when the value of δ is large, indicating that requestor U_0 and participant U_i behave well and are honest and reliable in the typical case of anonymous zone construction. It follows from the reward and punishment mechanism of the credit value in this method that requestor U_0, in order not to have their credit value reduced and to be able to continue to construct anonymous zones in the future, will not reveal the participant's true location information to a third party after receiving it, so the larger the privacy security metric δ is, the smaller the probability that the requestor will reveal the location information. Participant U_i, to prevent their credit value from being reduced and to be able to successfully construct anonymous zones as a requestor in the future, will provide true location information to the requestor, so the larger the privacy and security metric δ is, the less likely it is that the participant will provide a false location.

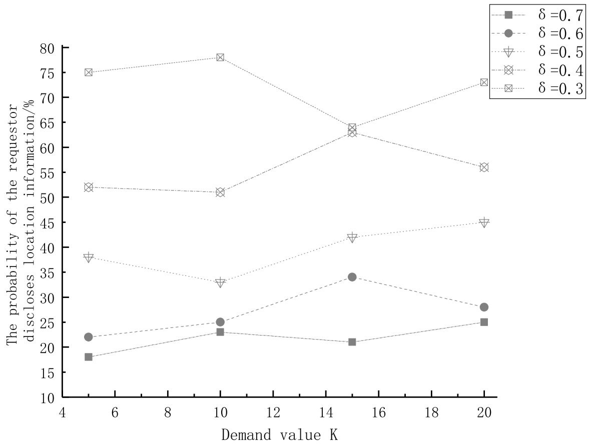

FIGURE 4. δ affects the probability that the requestor discloses location information.

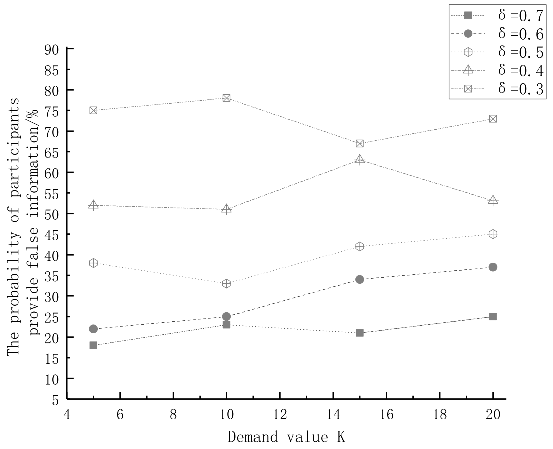

FIGURE 5. δ influences the probability that the participants provide false locations.

C. IMPACT OF THE NUMBER OF USER PARTICIPANTS ON THE SCHEME

In this part of the experiment, the effect of the number of users in the network on the probability of successfully constructing an anonymous zone is assessed. This experiment assumes that the requestor credit value $H_0 \geq \delta$ in the network. Additionally, $K = 5, 10, 15, 20$ reflects the need for privacy protection for requestor U_0, and the privacy and security metric δ is a

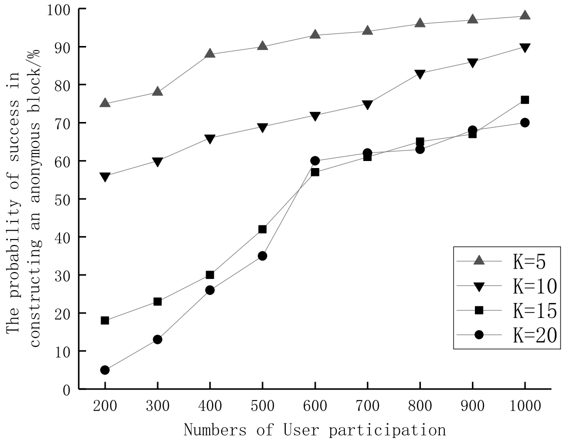

FIGURE 6. The influence of the number of participating users on the success rate of anonymous zone construction.

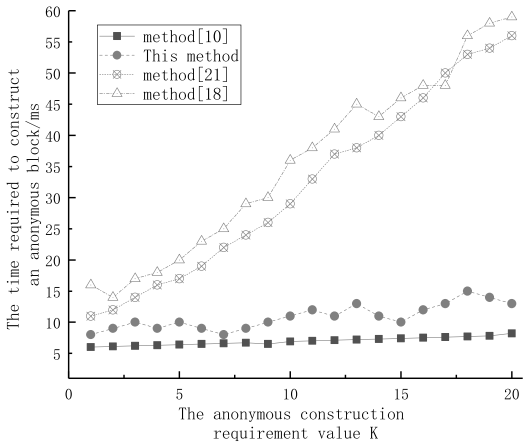

FIGURE 7. Time comparison for anonymous block construction.

fixed value; the experiment was repeated 100 times for each of the different K values, as shown in FIGURE 6.

The experiments showed that the probability of successfully constructing anonymous zones increases as the number of users in the network increases. With the credit value H and the privacy and security metric introduced, as the number of users in the network increases, the number of users who satisfy $H_i \geq \delta$ will increase, so the number of users who can participate in constructing an anonymous zone will increase, resulting in an increase in the probability that the requestor will successfully construct an anonymous zone using this scheme.

D. SCHEME COMPARISON

We assume that during the construction of the anonymous zone, the network is able to successfully construct the anonymous zone if the requestor's credit value H_0 satisfies $H_0 \geq \delta$, the participant's credit value H_i satisfies $H_i \geq \delta$, and the number of participants satisfies $\gg K - 1$. The practicality of this method is illustrated by comparing the time of anonymous zone construction and the probability of revealing the user location. The experimental results are shown in FIGURE 7 and FIGURE 8.

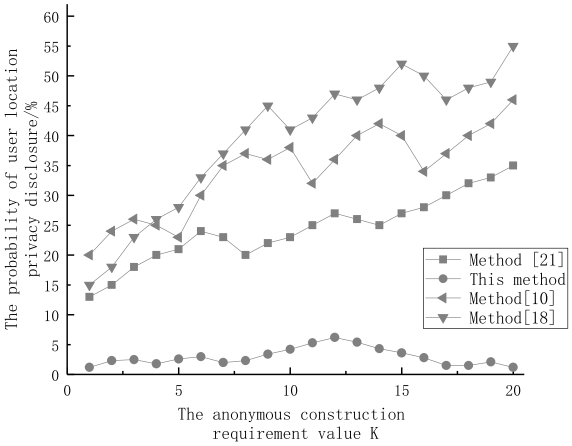

FIGURE 8. Comparison of the user location privacy disclosure probabilities.

Scheme [10] is based on a blockchain and treats the anonymous zone construction process as a game between the requesting user and the collaborating user; by verifying the actions of both in the chain as evidence of punishment, this method uses the historical user information during anonymous zone construction to directly constrain the anonymous zone situation; therefore, the time needed to construct the anonymous zone will be the same, but the privacy leakage rate for the user location may differ. The method proposed in this paper is slightly more time consuming compared to scheme [10] because during the anonymous zone construction process, each construction step involves the transformation from real data to credit values, and both the requestor and the participants need to verify the information with each other; however, the user location privacy leakage rate of this method is restricted to below 10%. Scheme [18] proposes a hybrid incentive mechanism that combines privacy protection and virtual credits, which is only effective in stimulating user participation. The scheme proposed in this paper has a significant advantage over scheme [18], not only in terms of the anonymous zone construction time but also in terms of user location privacy disclosure. Scheme [21] is based on the idea that a combination of multiple private blockchains can be used to disperse the user's transaction records, and each blockchain is associated with high time and cost requirements for the processes of uploading, extracting, and verifying the user information. The method proposed in this paper, in contrast to scheme [21], includes only one blockchain in the anonymous zone construction process, and while the information in the public blockchain needs to be verified, users who have misbehaved are identified; this process is much shorter than that in scheme [21], and the user location privacy leakage rate is comparatively lower.

The experimental results indicate that this method reduces the construction time for anonymous areas and greatly reduces the probability of user location leaks compared with the above methods. Although scheme [21] protects user privacy based on blockchains and guarantees that users can participate in anonymous construction, it does not restrict the bad or malicious behavior of users. The proposed method introduces credit values and a credit value reward and punishment mechanism based on blockchain technology. When a user exhibits bad behavior, the credit value of the user will be reduced, as shown in equations (15) and (16). When $H < \delta$, the user will not be able to participate in the construction of anonymous zones, thereby constraining the user's ability to successfully construct anonymous zones as a requestor. This constraint causes users to consciously abide by the rules and not leak information or provide false information, thus ensuring user location privacy and decreasing the probability of information leakage issues.

Based on the above analysis, by comparing the method proposed in this paper with the schemes mentioned in the literature [10], [18], [21], the method proposed in this paper can effectively restrain user misbehavior by shortening the construction time of the anonymous zone, thereby motivating participants to provide real information to participate in the construction of the anonymous zone, preventing the requestor from revealing the participants' real locations, reducing the leakage rate of the users' locations, and effectively protecting the user location privacy.

VI. CONCLUSION

This paper notes that existing algorithms are usually based on theoretical data without actual user data to support analyses of location privacy protection; thus, most studies cannot effectively assess the feasibility of user location privacy protection. To address this problem, this paper proposes a blockchain-based privacy protection method for the MADM algorithm, defines an anonymous zone construction model and gives the structure of the system; then, the MADM algorithm is used to convert the credit values of each platform from real user scenarios into a credit value, and this parameter is used as a constraint in the anonymous zone construction process to limit the bad behavior of users through a credit value reward and punishment mechanism. In addition, this paper describes the anonymous zone construction process in detail. The process is based on blockchain technology and stores transaction bills in the public chain, thus guaranteeing that the information is irreversible and nonfalsifiable. Finally, an analysis of the method and simulation experiments verified that the proposed approach can effectively limit the bad behavior of users when they construct anonymous zones, quickly construct anonymous zones while reducing the leakage rate of user locations, and effectively protect the privacy of user location information.

REFERENCES

[1] L. Ni, F. Tian, Q. Ni, Y. Yan, and J. Zhang, "An anonymous entropy-based location privacy protection scheme in mobile social networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2019, no. 1, pp. 1–19, Dec. 2019.

[2] S. Zhang, X. Li, Z. Tan, T. Peng, and G. Wang, "A caching and spatial k-anonymity driven privacy enhancement scheme in continuous location-based services," *Future Gener. Comput. Syst.*, vol. 94, pp. 40–50, May 2019.

[3] X. Li, Y. Zhu, and J. Wang, "Highly efficient privacy preserving location-based services with enhanced one-round blind filter," *IEEE Trans. Emerg. Topics Comput.*, early access, Jul. 5, 2019, doi: 10.1109/TETC.2019.2926385.

[4] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in *Proc. 1st Int. Conf. Mobile Syst., Appl. Services (MobiSys)*, 2003, pp. 163–168.

[5] W. Ni, M. Gu, and X. Chen, "Location privacy-preserving k nearest neighbor query under user's preference," *Knowl.-Based Syst.*, vol. 103, pp. 19–27, Jul. 2016.

[6] Y.-M. Ye, C.-C. Pan, and G.-K. Yang, "An improved location-based service authentication algorithm with personalized k-anonymity," in *Proc. China Satell. Navigat. Conf. (CSNC)*. Singapore: Springer, 2016, pp. 257–266.

[7] Y. Huang, Z. Huo, and X.-F. Meng, "CoPrivacy: A collaborative location privacy-preserving method without cloaking region," *Chin. J. Comput.*, vol. 34, no. 10, pp. 1976–1985, Oct. 2011.

[8] C.-Y. Chow, M. F. Mokbel, and X. Liu, "A peer-to-peer spatial cloaking algorithm for anonymous location-based service," in *Proc. 14th Annu. ACM Int. Symp. Adv. Geograph. Inf. Syst. (GIS)*, 2006, pp. 171–178.

[9] G. Ghinita, P. Kalnis, and S. Skiadopoulos, "PRIVE: Anonymous location-based queries in distributed mobile systems," in *Proc. 16th Int. Conf. World Wide Web (WWW)*, 2007, pp. 371–380.

[10] H. Liu, X. Li, B. Luo, Y. Wang, Y. Ren, and J. Ma, "Distributed K-anonymity location privacy protection scheme based on blockchain," *Chin. J. Comput.*, vol. 42, no. 5, pp. 942–960, 2019.

[11] H.-J. Cho, S. J. Kwon, R. Jin, and T.-S. Chung, "A privacy-aware monitoring algorithm for moving k-nearest neighbor queries in road networks," *Distrib. Parallel Databases*, vol. 33, no. 3, pp. 319–352, Sep. 2015.

[12] H.-I. Kim, Y.-S. Shin, and J.-W. Chang, "A grid-based cloaking scheme for continuous queries in distributed systems," in *Proc. IEEE 11th Int. Conf. Comput. Inf. Technol.*, Aug. 2011, pp. 75–82.

[13] Y. Che, Q. Yang, and X. Hong, "A dual-active spatial cloaking algorithm for location privacy preserving in mobile peer-to-peer networks," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2012, pp. 2098–2102.

[14] G. Sun, D. Liao, H. Li, H. Yu, and V. Chang, "L2P2: A location-label based approach for privacy preserving in LBS," *Future Gener. Comput. Syst.*, vol. 74, pp. 375–384, Sep. 2017.

[15] R.-H. Hwang and F.-H. Huang, "SocialCloaking: A distributed architecture for k-anonymity location privacy protection," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Feb. 2014, pp. 247–251.

[16] H. Zhang, Z. Xu, Z. Zhou, J. Shi, and X. Du, "CLPP: Context-aware location privacy protection for location-based social network," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2015, pp. 1164–1169.

[17] R. Gupta and U. P. Rao, "Achieving location privacy through CAST in location based services," *J. Commun. Netw.*, vol. 19, no. 3, pp. 239–249, 2017.

[18] B. Jia, T. Zhou, W. Li, Z. Liu, and J. Zhang, "A blockchain-based location privacy protection incentive mechanism in crowd sensing networks," *Sensors*, vol. 18, no. 11, p. 3894, Nov. 2018.

[19] D. Yang, F. Xi, and G. Xue, "Truthful incentive mechanisms for k-anonymity location privacy," in *Proc. 32nd IEEE Int. Conf. Comput. Commun.*, Apr. 2013, pp. 2994–3002.

[20] Y. Zhang, W. Tong, and S. Zhong, "On designing satisfaction-ratio-aware truthful incentive mechanisms for k-anonymity location privacy," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 11, pp. 2528–2541, Nov. 2016.

[21] Y. Qiu, Y. Liu, X. Li, and J. Chen, "A novel location privacy-preserving approach based on blockchain," *Sensors*, vol. 20, no. 12, p. 3519, Jun. 2020.

[22] X. Li, M. Miao, H. Liu, J. Ma, and K.-C. Li, "An incentive mechanism for K-anonymity in LBS privacy protection based on credit mechanism," *Soft Comput.*, vol. 21, no. 14, pp. 3907–3917, Jul. 2017.

[23] M. Debe, K. Salah, M. H. Ur Rehman, and D. Svetinovic, "Monetization of services provided by public fog nodes using blockchain and smart contracts," *IEEE Access*, vol. 8, pp. 20118–20128, 2020.

HUI WANG was born in Jiaozuo, Henan, China, in 1975. He received the Ph.D. degree in computer sciences and technology from Jilin University, in 2009. He is currently a Professor with the School of Computer Science and Technology, Henan Polytechnic University. His research interests include network security, information simulation, and intelligent information processing.

CHENGJIE WANG was born in Shandong, China, in 1993. He is currently pursuing the M.S. degree with the School of Computer Science and Technology, Henan Polytechnic University. His research interests include network and information security, location privacy, and artificial intelligence.

ZIHAO SHEN was born in Nanyang, Henan, China, in 1980. He received the Ph.D. degree in computer sciences and technology from Jilin University, in 2020. He is currently a Lecturer with the School of Computer Science and Technology, Henan Polytechnic University. His research interests include network and information security, information simulation, and intelligent information processing.

KUN LIU was born in Jiaozuo, Henan, China, in 1978. She received the M.S. degree from the Chongqing University of Posts and Telecommunications, in 2009. She is currently an Associate Professor with the School of Computer Science and Technology, Henan Polytechnic University. Her research interests include network and information security, and information simulation.

PEIQIAN LIU was born in Datong, Shanxi, China, in 1970. He received the Ph.D. degree in computer sciences and technology from the Beijing University of Posts and Telecommunications, in 2019. He is currently an Associate Professor with the School of Computer Science and Technology, Henan Polytechnic University. His research interests include network information security and intelligent information processing.

DENGWEI LIN was born in Wenxian, Henan, China, in 1972. He received the M.S. degree in computer sciences and technology from the East China University of Science and Technology, in 2008. He is currently a Professor with Jiaozuo University. His research interests include computer control, software development, and artificial intelligence.