Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 1847890, 9 pages
https://doi.org/10.1155/2018/1847890

*Research Article*

# The Research of Mobile Location Privacy Protection Access Control Method Based on Game Theory

**Lijuan Zheng**[1], **Linhao Zhang**[1], **Meng Cui**[1], **Ning Cao**[2], **Jianrui Ding**[3], **Leul Yalemshet**[1], **Tsepo Nyakonda**[1], **and Shepard Musasike**[1]

[1]*School of Information Science and Technology, ShiJiazhuang Tiedao University, ShiJiazhuang 050043, China*
[2]*College of Information Engineering Qingdao Binhai University, Qingdao 266555, China*
[3]*Harbin Institute of Technology, School of Computer Science and Technology, Harbin 150001, China*

Correspondence should be addressed to Lijuan Zheng; zhenglijuan@stdu.edu.cn

Received 28 April 2018; Accepted 1 November 2018; Published 12 December 2018

Guest Editor: Jian Shen



In recent years, the Internet of things has developed rapidly. And the location-based service (LBS) is becoming more and more extensive. Service providers hold a large number of users' information. In order to improve the quality of service, service providers increasingly use big data technology to provide more accurate services for users. At the same time, it aggravates the information disclosure of users' privacy. From the perspective of the service provider, a mobile location privacy access control method based on game theory is proposed to solve the access control problem of mobile location privacy information. Firstly, the weight coefficient is set according to the location privacy influence factors, and then the access control threshold is calculated according to the privacy location leakage situation of the mobile location. Different visitor levels are set according to the threshold. In the process of access control, the prejudgement of the access behaviour is performed, and then the privacy information amount of the information requested for access is calculated according to the weights of the different information. Compare the result with the threshold and get the access control strategy. The strategy set is selected based on strategy matrix of game theory and thresholds are adjusted based on the calculation returns of strategy matrix. The effectiveness and practicability of the method are verified through the security analysis.

## 1. Introduction

In recent years, the Internet of things (IoT) has developed rapidly, and applications based on the IoT have gradually emerged [1]. It involves military, industry, agriculture, power grid and water networks, transportation, logistics, energy conservation, environmental protection, medical care and healthcare, smart home appliances, and so on [2]. In the IoT, applications based on location services are also increasingly widespread. Location-based services provide location services to the user by determining the geographical location of the mobile device, which can easily lead to leakage of user location privacy. For example, a single point location will be changed in real time when a user requests a location service. An unauthorized visitor accesses an application server to obtain user location information. After obtaining a certain amount of information, the location privacy information can infer the user's track information, resulting in leakage of user location privacy information which will also lead to attacks against users [3]. The continuous development of big data technology also brings greater development space for enterprises [4]. More and more location-based service providers can make data mining based on existing user data to improve user experience. JP Tang et al. studied the platform through intelligent traffic data sensing information processing platform and used the existing traffic big data to improve the intelligent traffic service [5]. The leakage of private information greatly affects the user's service experience. Solving the problem of privacy information protection in the application process of Internet of things is one of the necessary conditions for the wide application of the Internet of things [6].

The user's mobile location privacy information is divided into single point location privacy information and trajectory privacy information. Single point location privacy refers to an independent location point related to private information. Different from single point location privacy, the track mainly refers to the order of the position information of a moving object in chronological order. Trajectory privacy focuses on the temporality of location information. The mobile location privacy contains single point location privacy and trajectory privacy, which refers to the temporality, spatiality, and frequency characteristics of location information.

This paper proposes a mobile location privacy access control method based on game theory aiming at the leakage of privacy information in the mobile location of Internet of things users. It controls the privacy information access behaviour according to the specified location privacy information access policy from the perspective of the service provider. The access control can guarantee the server to make a dynamic response to illegal access behaviour about privacy information. At the same time, according to tolerance setting, avoid the indirect leakage of mobile location and privacy information caused by the superposition of information.

## 2. Research Status

IoT location privacy protection has received more and more attention in recent years, and the related research work has achieved a lot of results. It is mainly aimed at the query and release of location information. Related location privacy protection technologies include location anonymous technologies, among which application research of k-anonymous technology proposed by Samarati and Sweeney is the most widely used [7]: encryption technologies, such as secure multiparty computing technology, homomorphic encryption technology, fake convergence node protocol, and RFID privacy protection technology [8]. IoT location privacy protection technology has gradually matured, but protection technology related to mobile location privacy is still in its infancy. The existing methods are mostly based on the traditional anonymization, fuzzy, and cryptography. Wang YJ et al. proposed a real incentive mechanism based on location privacy protection in mobile crowdsourcing systems under the online network environment. The improved two-stage auction algorithm based on trust degree and privacy sensibility is proposed. The differential privacy based on Gauss white noise is applied to k-anonymity to prevent user location information leakage [9]. Zhang HT. et al. proposed novel online spatial temporal k-anonymity method for location privacy protection from sequence rules-based inference attacks. It predicts the destination location from the privacy-sensitive sequence rules excavated from large scale anonymous datasets. This method extends the original sequence database of anonymous datasets. It adopts specific generalization and avoidance principles to gradually hide privacy-sensitive rules and resist reasoning attacks [10]. There is also someone in conjunction with other technologies for privacy protection research. Huguenin K. et al. use machine learning methods to predict the user's motivation to check-in and quantify utility implications to protect location privacy [11]. Based on mobile cloud computing, Gong Y. et al. proposed a framework to protect location privacy when assigning tasks to mobile devices, allowing mobile devices to contribute resources to the ad hoc mobile cloud without revealing location information [12]. Mobile location privacy involves trajectory privacy information. There are three main aspects of protection technology for trajectory privacy: fuzzification, release suppression, and addition of fake data. Zhao P. et al. proposed ILLIA to solve location injection attacks. On the basis of exploring the similarity of user mobility in continuous LBS queries, a trust-based k-anonymity scheme is developed. ILLIA can defend against LIA without knowing how to manipulate false locations in advance, while still maintaining high-quality services [13]. Suppression method is often used in trajectory privacy protection. Al-Hussaenik et al., based on the (K, C) L standard, used the local and global suppression methods to avoid attackers obtaining track privacy information [14]. The fake data method is also widely used in track privacy protection. Gao Sheng et al. disturb the actual trajectory data to generate false trajectory data and then added it to the original trajectory data [15]. Su Qing et al. proposed a hierarchical role-based access control method for location privacy protection on mobile terminals and defined access permissions through secondary role definitions [16]. Related researchers have introduced game theory for privacy protection, but these methods are still in deep exploration [17]. In addition, the access control method for the service information provider to private information is not perfect. In order to improve the service quality, data mining and cloud computing technologies are used, but the privacy protection of the user privacy data is not controlled.

Game theory is not only a new branch of modern mathematics, but also an important discipline in operations research. It is a mathematical theory and method for studying the phenomena of struggle or competition [18]. Game theory has many applications in security, privacy, and wireless networks. It is a new research method to solve the problem of privacy protection based on game theory. Unlike traditional privacy protection methods, privacy protection methods based on game theory describe participants' benefits and costs, simulate their rational choice process through mechanism design and development strategy, and find the best solution for each party by analysing game equilibrium. There are many privacy protection models based on game theory that have been proposed in succession, such as the privacy protection model based on game theory proposed by Zhang Yixuan [19]. A game theory analysis for location privacy protection based on P-destination in mobile social networks is proposed by Bidi Ying and Amiya Nayak [20]. Consider users that collaborate with each other in the anonymous group and choose game strategies to provide their own data for other users so as to obtain desired services. The research methods for mobile location privacy are not perfect, and the issues of point location privacy and trajectory privacy are gradually exposed, which will also be the new direction of the research on privacy protection model based on game theory in the future.

## 3. Mobile Location Privacy Protection Scheme Based on Game Theory

This article starts with the characteristics of mobile location privacy and establishes a mobile location privacy access control model based on game theory. It implements dynamic control and protection of mobile location privacy information through access control.

*3.1. Basic Concepts.* Single point location refers to sensitive location information with frequency characteristics generated by individual activities. For example, someone who often appears at a certain location at a certain moment, such as family location, work place. The position information $D$ may be represented as $D = \{u_i, (x_i, y_i, t_i)\}$. The privacy information of a single point of location can easily expose a person's fixed position. Once the disclosure is captured by criminals, the security threat to individuals is extremely high. Therefore, it is necessary to prevent attackers from obtaining such sensitive information.

Trajectory privacy refers to a series of sequential and frequent sensitive location information generated by individual activities, such as where persons are, where they are during a certain period of time, and what activity area is. The track information $T$ can be represented as $T = \{u_i, (x_1, y_1, t_1), (x_2, y_2, t_2), (x_3, y_3, t_3), \ldots, (x_n, y_n, t_n)\}$. According to the trajectory privacy, it is easy to deduce personal habits, action route preferences, and even infer private information such as home address and work place. Therefore, it is necessary to prevent malicious attackers from obtaining such sensitive information.

In the position indication, id indicates the user identifier, $t_i$ indicates the time of the user position information, and $(x_i, y_i)$ indicates the two-dimensional position information of the user at time $t_i$.

Historical access record refers to the visitor's access record to a user's privacy information.

*3.2. Problem Description*

*3.2.1. Location Privacy Leakage Caused by Information Superposition.* The location information itself contains abundant temporal and spatial information, and the single location information has no substantial value, but the superposition of information can make the information integrated to obtain more valuable and specific information. Currently, due to the increasing location services, a large amount of user location information has been generated. Many enterprises and scientific research institutions have obtained a lot of analysis results related to user habits through the research and analysis of a large number of location information. Many of the location information are intrinsically related, especially for personal location information analysis, which can easily expose the user's privacy.

The model calculates the maximum tolerance of privacy information leakage by weighting the time, space, and frequency factors of the user's mobile location and restricts the amount of access to private information of the visitor.

*3.2.2. Location Server Cannot Identify Malicious Access Behaviour and Implement Access Control.* The user's location request information and real-time location information are stored on the location server. Malicious visitors can gain certain access rights through certain means and access the user's location record information. When the gained information is gradually increased, the amount of private information is also increasing. It is difficult for the server to detect such malicious behaviour and make timely response measures.

The above two key issues can be summarized as follows:

①Information superposition can cause indirect leakage of mobile location privacy.

②Identification of access behaviour and real-time dynamic control realized by the location server.

Different levels of thresholds are set for different visitors to solve the problem of dynamic access control.

This article focuses on privacy protection based on game theory for mobile location privacy. It mainly studies the characteristics of mobile location privacy and proposes a model suitable for protecting mobile location privacy access control using game theory in combination with current privacy information protection methods.

*3.3. Model Structure Design.* There are three parts in the model: the strategy execution part, the strategy deployment part, and the historical visit record. And there are five modules in total.

①Request acquisition module: module obtains a request for privacy information from a visitor request, and then it extracts critical information from access.

②Key information extraction module: it integrates visitor's mobile location privacy information request.

③Visitor's historical visit record module of mobile location privacy information: it records each visitor's historical mobile location privacy information request and provides reference for the threshold calculation module.

④Threshold calculation module: it sets the privacy location information threshold based on the game theory by the existing factor weight. Module performs weighted calculation based on historical record feedback results and feeds it back to the decision execution module.

⑤Decision execution module: it executes feedback made through the game strategy.

The design composition is shown as in Figure 1.

The basic element of model is as follows.

User set: $user = \{u_1, u_2, \ldots, u_n\}$, represented as a collection of all users who own information in the system.

The visitor set: $visitors = \{v_1, v_2, \ldots, v_n\}$, represented as a collection of all visitors in the system.

Access the role set: $roles = \{r_1, r_2, \ldots, r_n\}$, represented as a hierarchical collection of visitors in the system.

The system operation set: $operate = \{op_1, op_2, \ldots, op_n\}$, represented as a collection of response actions for the system for access requests.

*3.4. Scheme Design*

*3.4.1. Factor Weight Setting.* Firstly, it is necessary to analyse the key factors of privacy protection in mobile location. It

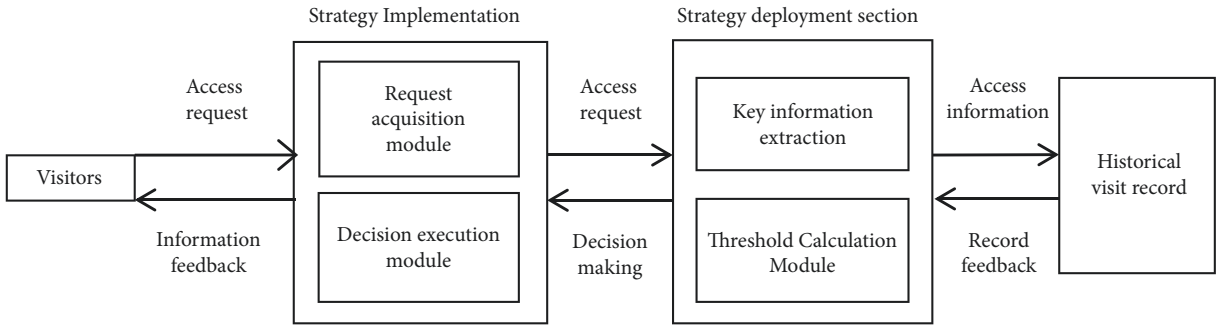


Figure 1: Access control method design composition.

performs weighted calculations and comparisons for time, space, and frequency. Summarizing the weight of each factor and then the weight setting suitable for this model is obtained. According to the result, the amount of information is calculated. Whether to respond to the access behaviour of location privacy information is decided based on the calculation results about the amount of information. The weight values of time, space, and frequency factor are set to be $w_t$, $w_s$, $w_f$.

*3.4.2. Game Theory Strategy Implementation Plan.* The scheme uses the noncooperative game theory related technology to control the visitors' behaviours. The recent behaviours of all visitors will be recorded and calculated for the degree of privacy mastered by the visitors. The server sets a threshold for the users' mobile location privacy information as the standard for that server controls visitors' access behaviour. Besides, the standard can also be regarded as the maximum value for allowing the visitor to grasp user's mobile location privacy information. When it is exceeded, the privacy of mobile users' location will be disclosed.

Assuming that the weighted result of accessing private information is *ac-R*, according to the single point location information $D = \{u_1, (x_1, y_1, t_1)\}$ given above, the time and space information can be known, and the frequency information can be obtained based on the historical access records. After integrating the three factor information, the weighted results of visit are calculated according to the following.

$$\begin{aligned} ac - R_{point} = &-\mathrm{w}_t P(x_t)\log_2 P(x_t) \\ &-\mathrm{w}_s P(x_s)\log_2 P(x_s) \\ &-\mathrm{w}_f P(x_f)\log_2 P(x_f) \end{aligned} \tag{1}$$

This equation aims at the request behaviour of single point location privacy information, calculates the amount of request information according to different factor request information conditions, and sums to obtain the amount of private information of this access behaviour.

According to track information $T = \{u_1, (x_1, y_1, t_1), (x_2, y_2, t_2), (x_3, y_3, t_3), \ldots, (x_n, y_n, t_n)\}$, the weighted result of accessing private information is obtained as follows.

$$ac - R_{trace} = -\sum_{i=1}^{k} \frac{1}{n}\log_2 \frac{1}{n} \tag{2}$$

This equation is for access behaviour of tracking private information. The number of single points contained in the track information is $n$. The number of location points for the request access behaviour is $k$, and $ac\text{-}R_{trace}$ indicates the amount of private information that the access behaviour can obtain.

*3.4.3. Threshold Setting Scheme.* This threshold is mainly composed of three factors: time, space, and frequency. Through analysis and summary of the impact of each factor on the privacy of the users' mobile location, the weights are calculated according to the result setting factors. The weighted result is calculated by the strategy deployment module for different weighted mobile location privacy information. Once the degree of visitor's privacy mastery exceeds the initial threshold, privacy information is no longer provided to the visitor. The threshold is set as *ac-threshold*. The formula for calculating the threshold is shown in

$$\begin{aligned} ac - threshold = &-\mathrm{w}_t P_1 \log_2 P_1 - \mathrm{w}_s P_2 \log_2 P_2 \\ &- \mathrm{w}_f P_3 \log_2 P_3 \end{aligned} \tag{3}$$

Suppose that the value of the access information extracted from the historical access record is *ac-V*. Whether to allow the visitors to access the privacy information of users' mobile location is determined by comparing *ac-threshold* with *ac-V+ac-R*. If *ac-threshold* is more than *ac-V+ac-R*, access is allowed; if *ac-threshold* is less than *ac-V+ac-R*, access is denied.

*3.4.4. Dynamic Access Control Scheme.* Scheme sets different access permissions for different visitors and judges whether the visitor has malicious access intention based on the access behaviour. Then it classifies the malicious access intentions as single point location privacy and trajectory privacy. This solution is designed to set access rights for the server's managers with different levels and applications of location privacy access behaviours.

Combine the visitor's recent history records and this visit request to determine the intention of the request and suppose the requested location information is $\{v_1, (u_1, x_1, y_1, t_1), (u_2, x_2, y_2, t_2) \ldots\ldots, (u_n, x_n, y_n, t_n)\}$. If the visitor's visit is successful, the recent visit record, location information $(x, y)$, and time information $t$ have more than 3 records with

Table 1: Game strategy matrix table.

| System | Visitors | |
|---|---|---|
| | Goodwill visit (G) | Malicious visits (E) |
| Allow access (P) | Ssin-ac, Fper-ac | -Sevil-ac, Fper-ac |
| Access denied (R) | -Ssin-ac, 0 | 0, -Fre-ac |

Table 2: System threshold adjustment parameters table.

| | System threshold adjustment parameters |
|---|---|
| -Sevil-ac | -Sevil-ac |
| -Ssin-ac | Ssin-ac |

similar information at a single day; then it is judged as a single point of privacy malicious visit. If there are more than 6 access records at the above single point and the time t for a single-day access record is time-series, then it is determined as the trajectory privacy malicious access behaviour. According to the system operation set $operate = \{op_1, op_2, \ldots, op_n\}$, in this model, four kinds of system operations are set up, that is, the system's permission and denial of access operations in the case of visitor's goodwill access and the system's permission and denial of access operations in the case of visitor's malicious access.

The game-theoretic strategy matrix is set as Table 1. The system revenue is divided into good-faith access revenue to *Ssin-ac* and malicious access revenue to *Sevil-ac*. Visitors' income is allowed access revenue to *Fper-ac* and denied access revenue to *Fre-ac*.

The system first makes early judgments on access behaviour, executes access control through late threshold comparisons, and then combines the previous judgment results with the access control execution results. Referring to the strategy matrix, the system revenue and visitor income are summarized; then adjust the corresponding system thresholds and visitor's permission through the revenue summary and make model access control more accurate. When the system revenue is positive, the system threshold is not adjusted. Instead ofwhen the system revenue is negative, the system threshold adjustment parameters are shown in Table 2.

## 4. Security Theoretical Analysis

*4.1. Adversary Model.* There are two types of visitor types: goodwill visitors and malicious visitors.

Instead of visiting a single user in depth and trying to get the user's identity information, goodwill visitors only access location information related to their needs.

A malicious visitor may attempt to obtain more user privacy information, including accessing more user records or attempting to obtain more location information for the same user record.

Malicious visitors can have the following capabilities:

(A) Information other than identity information about the user can be obtained.

Table 3: Privacy information transaction set table.

| Transaction set number | Event collection |
|---|---|
| E1 | {t p f s} |
| E2 | {p f b s} |
| E3 | {t f b s} |
| E4 | {t p b s} |
| E5 | {t f s} |
| E6 | {t p f b s} |

(B) An access request can be issued regardless of the type of access information.

(C) User partial location privacy information (less than the system-defined threshold) can be obtained.

*4.2. Factor Weight Analysis.* Supposing a user's location information transaction set is organized and a conclusion can be made using theories related to data mining association rules, the results are shown in Table 3.

t represents time information (assuming $t$ = 21:00), $p$ represents location information, $f$ represents frequency information (assuming $f$ is the situation where frequency is greater than 5), $b$ represents background knowledge, and $s$ represents the situation of privacy leakage (assuming $s$ is the home address information disclosure situation).

According to Table 3, there are 6 transactions, $E = \{E_1, E_2, E_3, E_4, E_5, E_6\}$, the item set $I = \{t, p, f, b, s\}$, and $E\ (t, s)$ represents the transaction that has both event $t$ and event $s$.

According to data mining related knowledge, $support_{x,y} = N_{E(x,y)}/N_E$, $confidence_{x,y} = N_{E(x,y)}/N_{E(x)}$, $N_{E(x,y)}$ represents the number of transaction containing both events $x$ and $y$, and $N_{E(x)}$ represents the number of transactions containing event $x$. Something can be obtained as follows:

$$\text{Rule } t \text{ —>} s,\ support_{t,s} = 5/6,\ confidence_{t,s} = 1.$$

$$\text{Rule } p \text{ —>} s,\ support_{p\ s} = 2/3,\ confidence_{p,s} = 1.$$

$$\text{Rule } f \text{ —>} s,\ support_{f,s} = 5/6,\ confidence_{f,s} = 1.$$

The proportion of time factor $w_t = support_{t,s}/(support_{t,s} + support_{t,s} + support_{t,s}) = 0.357$. Similarly, the weight coefficient $w_t = 0.357$, $w_p = 0.286$, $w_f = 0.357$.

From the above analysis and calculation results, it can be seen that time, location, and frequency factors account for different proportions of location privacy information. That is, information sensitivity is different. The method of this scheme can distinguish the weights of different influencing factors of location privacy information and express them in numerical form.

*4.3. Access Hypothesis Analysis*

*4.3.1. Prior Judgment of Access Behaviour.* First, when a visitor accesses private information, the access control system firstly retrieves the historical access record and guesses whether the access behaviour is legal to the privacy of single point or trajectory privacy according to the historical access. If there is no history access record, the system will think of it as

Table 4: Threshold setting table.

| Visitors | Single point privacy threshold | Trajectory privacy threshold |
|---|---|---|
| First level | 0.654 | 0.764 |
| Second level | 0.818 | 0.955 |
| Third Level | 0.981 | 1.146 |

point location privacy access by default. According to role set $roles = \{r_1, r_2, \ldots, r_n\}$, the total level of visitors is 3, and the number of records that visitors in each level can visit increases by levels. The first-level visitors can access 4 records. The second-level visitors can access 5 records, and the third-level visitors can access 6 records. If this condition is satisfied, it will be judged as normal goodwill access behaviour. If this condition is not satisfied, it will be judged as malicious access behaviour.

The threshold is set for different visitors. The single point location data contains thirty records, and the track data is taken 24 times a day. According to the analysis of test, when the single point location privacy disclosure is more than five records, the sensitive information of the user is considered to be leaked; when the trace data disclosure is more than 5 pieces, the privacy information of the user is considered to be leaked. The threshold setting table is shown in Table 4.

*4.3.2. Visit by Peer Visitors.* Assume that visitors A and B are first-level visitors. A and B visit the same single point privacy information of a mobile user. The query information is $\{v_A, (u_1, x_1, y_1, t_1), v_B, (u_1, x_1, y_1, t_1)\}$, set the visitor A's history access record value as $ac\text{-}V(A) = 0.432$ and visitor B's history access record value as $ac\text{-}V(B) = 0.537$.

According to (1) we can get the following.

$$\begin{aligned} ac\text{-}R_{point}(A) &= 0.153 \\ ac\text{-}R_{point}(B) &= 0.153 \\ ac\text{-}V(A) + ac\text{-}R_{point}(A) &= 0.585 \\ ac\text{-}V(B) + ac\text{-}R_{point}(B) &= 0.690 \end{aligned} \tag{4}$$

The first-level visitor's access single point privacy threshold $ac\text{-}threshold_1$ is 0.654. According to $ac\text{-}threshold_1$ being more than $ac\text{-}V(A) + ac\text{-}R_{point}(A)$, $ac\text{-}threshold_1$ is less than $ac\text{-}V(B) + ac\text{-}R_{point}(B)$. Visitor A's privacy information access request can be answered while visitor B's privacy information access request is denied.

*4.3.3. Visit by Different Levels Visitor.* Assuming visitor C is a first-level visitor, visitor D is a second-level visitor. They visit the same trajectory privacy information of a mobile user, and the query information is $\{v_C, v_D, (u_2, x_2, y_2, t_2), (u_2, x_3, y_3, t_3)\}$; set the history access record value of visitor C as $ac\text{-}V(C) = 0.373$ and the historical access record value of visitor D as $ac\text{-}V(D) = 0.576$.

According to formula (2) we can get the following.

$$\begin{aligned} ac\text{-}R_{trace}(C) &= 0.382 \\ ac\text{-}R_{trace}(D) &= 0.382 \\ ac\text{-}V(C) + ac\text{-}R_{trace}(C) &= 0.755 \\ ac\text{-}V(D) + ac\text{-}R_{trace}(D) &= 0.958 \end{aligned} \tag{5}$$

The value of the first-level visitor's access trajectory privacy threshold $ac\text{-}threshold_1$ is 0.764, and the value of the second-level visitor's access threshold $ac\text{-}threshold_2$ is 0.955; then according to condition, $ac\text{-}threshold_1$ is more than $ac\text{-}V(C)$ plus $ac\text{-}R_{trace}(C)$ and $ac\text{-}threshold_2$ is less than $ac\text{-}V(D)$ plus $ac\text{-}R_{trace}(D)$. Visitor C's privacy information access request can be answered while visitor D's privacy information access request is denied.

From the above calculation and analysis, we can see that, for the same access request of the peer visitors, the access control model can make different decisions according to different historical access records. For the same access request of nonpeer visitors, the access control model can also make a more appropriate judgment based on historical access records. There are no fixed restrictions on the visitors' access behaviour, but the protection of location privacy information can still be achieved. And the information entropy theory focuses on the calculation of information amount of the whole information set. Applying this theory in access control is easy to lead to missing the information of single access. The system prejudgment method set by this model can make up for this defect, and, as a reference condition of the game strategy matrix, it also can help to adjust the access control model.

## 5. Game Strategy Analysis

*5.1. Threshold Adjustment.* The adjustment parameter of the system is $Ssin\text{-}ac = Sevil\text{-}ac = 0.1$.

(1) Assume that visitor E is a first-level visitor. He accesses the track privacy information of a mobile user. The query information is $\{v_E, (u_1, x_1, y_1, t_1), (u_1, x_2, y_2, t_2)\}$. Suppose visitor E's historical access record value is $ac\text{-}V(E) = 0.472$. According to the prejudgment criteria, E can access up to four records as a first-level visitor. So E's access request meets the goodwill visit standard.

$$\begin{aligned} ac\text{-}R_{trace}(E) &= 0.299 \\ ac\text{-}V(E) + ac\text{-}R_{trace}(E) &= 0.771 \end{aligned} \tag{6}$$

The first-level visitor's access threshold is $ac\text{-}threshold_1 = 0.764$, so $ac\text{-}threshold_1 < ac\text{-}V(E) + ac\text{-}R_{trace}(E)$. Visitor E's request of privacy information access can be denied. It satisfies the situation that the goodwill visitor be refused to access by system in the policy matrix. At this time, the benefit of the system is negative, which satisfies the adjustment condition of system parameter. According to Table 2, adjust the parameter as *Ssin-ac*. After adjustment, the system threshold is adjusted to $ac\text{-}threshold_1 + Ssin\text{-}ac = 0.774$. At this point, adjust this policy to allow the access requests of E.

(2) Assume that visitor F is a first-level visitor. He accesses the track privacy information of a mobile user. The query information is $\{v_F, (u_1, x_1, y_1, t_1), (u_1, x_2, y_2, t_2), (u_1, x_3, y_3, t_3), (u_1, x_4, y_4, t_4), (u_1, x_5, y_5, t_5)\}$, and suppose visitor F's historical access record value is $ac\text{-}V(F) = 0.285$. According to the prejudgment criteria, as a first-level visitor, F can access up to four records, so F's access request cannot meet the goodwill visit standard and will be judged as malicious access.

$$\begin{aligned} ac\text{-}R_{trace}(F) &= 0.471 \\ ac\text{-}V(F) + ac\text{-}R_{trace}(F) &= 0.756 \end{aligned} \tag{7}$$

The first-level visitor's access threshold is $ac\text{-}threshold_1 = 0.764$, so $ac\text{-}threshold_1 > ac\text{-}V(F) + ac\text{-}R_{trace}(F)$. Visitor F's request of privacy information access can be responded. It satisfies the situation that the malicious visitor be allowed to access by system in the policy matrix. At this time, the benefit of the system is negative, which satisfies the adjustment condition of system parameter. According to Table 2, adjust the parameter as *Sevil-ac*. After adjustment, the system threshold is adjusted to $ac\text{-}threshold_1\text{-}Sevil\text{-}ac = 0.754$. At this point, adjust this policy to deny the access requests of F.

*5.2. Game Theory Analysis.* When a visitor conducts a malicious visit, the gain of visitor is divided into *Fre-ac* and *–Fre-ac* according to the system whether access is allowed. At the same time, the system's gain is divided into *-Sevil-ac* and 0. On the contrary, when the visitor carries out a goodwill visit, the gain of visitor is divided into *Fper-ac* and 0 while the gain of the system is divided into *Ssin-ac* and *-Ssin-ac*, according to whether the system access is allowed. This is the game of incomplete information.

Assume that the probability of a visitor who performs a good visit is $x$ and a malicious visit is $1\text{-}x$. Assuming that the system can accurately identify the visitor's access intent, the probability of the system allowing access is also $x$, and the probability of denying access is $1\text{-}x$. The combination of system and visitor strategies is $S_1 = (P, G)$, $S_2 = (P, E)$, $S_3 = (R, G)$, $S_4 = (R, E)$. The visitor's income value *income* is shown in

$$\text{Income} = \sum_{k} \text{income}_k(S_k)\, p_f \tag{8}$$

$Incomek(S_k)$ is the gain when selecting the $S_k$ strategy; $p_f$ is the probability of choosing the $k$ strategy. According to the above assumptions, (9) is as follows:

$$\text{Income}_f(G) = x * \text{Fper} - ac \tag{9}$$

*Incomef(G)* is the expected value of income when the visitor makes a good visit;

$$\text{Income}_f(E) = x * \text{Fper} - ac + (1 - x)(-\text{Fre} - ac) \tag{10}$$

*Incomef(E)* is the expected value of income when a visitor visits maliciously;

$$\text{Income}_s(P) = x * \text{Ssin} - ac + (1 - x)(-\text{Sevil} - ac) \tag{11}$$

*Incomes(P)* is the expected value of the income when the system adopts an allowed access strategy;

$$\text{Income}_s(R) = x(-\text{Ssin} - ac) \tag{12}$$

*Incomes(R)* is the expected value of the income when the system adopts the deny access policy.

*Informef(G)> Incomef(E)* can be derived from (9) and (10). That is, regardless of the probability of a good-faith visit of the visitor, the visitor's good-faith access behaviour will have a greater expected total return value than a malicious visit. So the visitors should choose good-faith visits as they wish to maximize their own interests.

In order to ensure the normal services of system location access, the system should try its best to meet visitors' access needs and ensure that privacy information is not revealed, it should satisfy the following: *Incomes(P)* is larger than *Incomes(R)*. It is shown as

$$x * \text{Ssin} - ac + (1 - x)(-\text{Sevil} - ac) > x(-\text{Ssin} - ac) \tag{13}$$

When $x$ is more toward the value of 1, the fuller condition is established in (13). That is to say, when the visitor adopts a good-faith access behaviour, the system's profit expectation also tends to be maximum.

From this, it can be concluded that good-faith access behaviour taken by visitors and access allowed by the systems can be seen as the Nash equilibrium strategy. And, at this point, both parties can get the most benefit.

From the analysis of the first two parts, we can see that the game theory strategy matrix set by this model can adjust the threshold parameters when the system strategy is deviant, so that the system can make more appropriate judgments. This makes the model access control to be better for location privacy information and ensures the dynamic of access control. At the same time, considering the first case, this paper argues that the threshold cannot be adjusted every time to avoid being used by malicious visitors to increase the threshold and reduce the system access control conditions. It ensures the stability of the system.

## 6. Comparative Analysis

Most of the existing mobile location privacy protection methods are for location information publishing and query operations, but these methods still cannot fully protect user location privacy information. For example, the (K, C) L privacy standard and its improvement methods are mainly to protect location privacy information against location trajectory tracking attacks. The continuous anonymity and its related improvement methods are mainly to protect the privacy of trajectory reconstruction attacks. The method proposed in this paper controls the amount of information accessed by normal visitors and attackers using the standard of information volume, so the attacker can only obtain limited private information and the difficulty of tracking and reconstructing attacks is increased.

Existing mobile location privacy protection methods have their own advantages, but, with the development of big data environment, they also have many drawbacks. For example,

Table 5: Comparative analysis table.

| | Considering different information factors | No curing access operation is required | Strategic adjustment mechanism |
|---|---|---|---|
| This model | √ | √ | √ |
| [9] | × | × | √ |
| [12] | × | × | × |
| [14] | × | × | × |
| [16] | × | √ | × |
| [20] | × | √ | × |

anonymity is effective for single-private data, but it cannot avoid the privacy leakage caused by the joint reconstruction attacks of multiple data sources. At the same time, there are many privacy protection methods for emerging technologies. For example, the location privacy protection development model and task allocation strategy in mobile cloud computing of ad hoc networks are proposed in [12]. A truthful incentive mechanism to protect location privacy in mobile crowdsourcing system is proposed in document [9]. And location service providers have a lot of user privacy information. Some service providers use existing data for data mining. However, they did not conduct more comprehensive access control over private data, which led to internal data leakage or external attack access leakage. The method proposed in this paper is mainly aimed at access control of data in the above two kinds of privacy leakage, and a game theory strategy matrix is introduced. It can complement the existing mobile location privacy protection method from the perspective of a location service provider and improve the effectiveness of location privacy protection and data utilization.

Compared with the game analysis of location privacy protection based on P-destination proposed in literature [20], the game theory is applied to the defence strategy game between the attacker and the system to maximize the system benefits. The location privacy protection method based on game theory proposed in literature [16] uses game theory to embody the behaviour of user cooperation in probability. The scheme proposed in this paper not only considers the execution of policy and the prediction of visitor behaviour, but also pays attention to the control of the amount of information that the visitor grasps and the adaptability of the scheme. Game theory strategy matrix adopted in this paper participates in the access control parameter adjustment, which is more conducive to the realization of dynamic and accurate and feasible access control strategies. So the scheme is more secure. Because this method does not identify and control collusion attacks, it can resist simple collusion attacks because of its restriction on the amount of information of visitors.

In Table 5, we compare and summarize three aspects: location privacy influencing factor, access operation, and adjustment mechanism.

## 7. Concluding Remarks

This paper provides a new access control method for single point location privacy access and trajectory privacy access in mobile location and achieves dynamic access control by setting visitor level and threshold for accessing privacy information. After security analysis, this method has certain practicality and scientificity.

## Data Availability

The data used to support the findings of this study are included within the article.

## Disclosure

An earlier version of this study was presented as a conference paper in ICCCS 2018: International Conference on Communication and Computing Systems.

## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## Acknowledgments

This research was partially supported by Hebei Education Department (QN2015231, QN2017132), Beijing Key Laboratory of Security and Privacy in Intelligent Transportation, Beijing Jiaotong University, Research and Practice of Higher Education Teaching Reform of Hebei Education Department (no. 2016GJJG112), Doctoral Scientific Research Foundation of Shijiazhuang Tiedao University (Z991015137), and Natural Science Foundation of Hebei Province (no. F2017210161, no. F2018210109).

## References

[1] J. Kaur and K. Kaur, "A fuzzy approach for an IoT-based automated employee performance appraisa," *Computers Materials and Continua*, vol. 53, no. 1, pp. 24–38, 2015.

[2] M. Guo, S. B. Zhang, and X. D. Li, "Research on location privacy protection technology in IoT," *Journal of Chinese Computer Systemspp*, no. 9, pp. 1961–1965, 2017.

[3] M. Rong, X. H Chen, and H. Liu, "Research on user privacy measurement and privacy protection in mobile crowdsensing," *Netinfo Security*, no. 8, pp. 1671-1122, 2018.

[4] C. R. Wu, E. Zapevalova, and Y. W. Chen, "Time optimization of multiple knowledge transfers in the big data environment," *Computers Materials and Continua*, vol. 54, no. 3, pp. 269–285, 2015.

[5] J. P Tang and L. Li, "Big data sensing information processing platform for intelligent traffic," *Applied Mechanics Materials*, vol. 667, pp. 324–327, 2014.

[6] H. T. Chi, *Location Privacy Protection Based on Location Service*, Xidian University, 2014.

[7] P. Samarati and L. Sweeney, *Protecting Privacy when Disclosing Information: k-Anonymity and Its Enforcement through Generalization and Suppression*, 1998.

[8] C. Yin, J. Xi, R. Sun, and J. Wang, "Location privacy protection based on differential privacy strategy for big data in industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3628–3636, 2018.

[9] Y. Wang, Z. Cai, X. Tong, Y. Gao, and G. Yin, "Truthful incentive mechanism with location privacy-preserving for mobile crowdsourcing systems," *Computer Networks*, vol. 135, pp. 32–43, 2018.

[10] H. Zhang, C. Wu, Z. Chen, Z. Liu, and Y. Zhu, "A novel online spatial-temporal k-anonymity method for location privacy protection from sequence rules-based inference attacks," *PLoS ONE*, vol. 12, no. 8, 2017.

[11] K. Huguenin, I. Bilogrevic, J. S. Machado et al., "A predictive model for user motivation and utility implications of privacy-protection mechanisms in location check-ins," *IEEE Transactions on Mobile Computing*, vol. 17, no. 4, pp. 760–774, 2018.

[12] Y. Gong, C. Zhang, Y. Fang, and J. Sun, "Protecting location privacy for task allocation in ad hoc mobile cloud computing," *IEEE Transactions on Emerging Topics in Computing*, vol. 6, no. 1, pp. 110–121, 2018.

[13] P. Zhao, J. Li, F. Zeng et al., "ILLIA: enabling k-Anonymity-based privacy preserving against location injection attacks in continuous LBS queries," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1033–1042, 2018.

[14] K. Al-Hussaeni, B. C. M. Fung, and W. K. Cheung, "Privacy-preserving trajectory stream publishing," *Data & Knowledge Engineering*, vol. 94, pp. 89–109, 2014.

[15] S. Gao, J. Ma, W. Shi, G. Zhan, and C. Sun, "TrPF: A trajectory privacy-preserving framework for participatory sensing," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 6, pp. 874–887, 2013.

[16] Q. Su and Y. Z Li, "Research of privacy protection method based on access control," *Journal of Yanbian University*, vol. 42, no. 1, pp. 69–74, 2016.

[17] D. D. Zhou, W. W. Li, and Y. Q. Sun, "Survey on game theory based privacy protection," *Journal of Chinese Computer Systems*, vol. 36, no. 12, pp. 2696–2700, 2015.

[18] S. K. Zhang and Y. D. Zhang, *Methods of Modern Game Theory and Mathematics in Economic*, Dongbei University of Finance and Economics Press, 2016.

[19] Y. X. Zhang, J. S. He, B. Zhao, and N. F. Zhu, "A privacy protection model based on game theory," *Chinese Journal of Computers*, vol. 39, no. 3, pp. 615–627, 2016.

[20] B. Ying and A. Nayak, "Location privacy-protection based on p-destination in mobile social networks: A game theory analysis," in *Proceedings of the 2017 IEEE Conference on Dependable and Secure Computing*, pp. 243–250, Taiwan, August 2017.