JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 33, 965-978 (2017)
DOI: 10.6688/JISE.2017.33.4.7

Privacy Protection Model Based on Digital Envelope and Dummies for Location-Based Services

JIAN XU[1,3], SI-JIA ZHAO[2] AND FU-CAI ZHOU[1]
[1]*Software College*
Northeastern University
Shenyang, 110169 P.R. China
[2]*School of Computer Science and Statistics*
Trinity College Dublin
Dublin, Dublin 2 Ireland
[3]*State Key Laboratory of Information Security, Institute of Information Engineering*
The Chinese Academy of Sciences
Beijing, 100093 P.R. China
E-mail: xuj@mail.neu.edu.cn

With the rapid development of smart city, location-based services (LBS for short) have become an important part of intelligent transportation which is the basic infrastructure of smart city. However, when users enjoy LBS, they have to send their real time location to location service provider, which allows users to face the risk of release location privacy at any time. In order to protect the location privacy, a privacy protection model based digital envelope and dummies is proposed. We use distributed peer to peer structure, which does not require the third-part anonymous server, to improve the efficiency of the location communication and set different location privacy protection methods for single point query and track query in order to adapt the diversity for different environment of location privacy protection. With the combination of digital envelope and false location technology, we add noise to basic location information to improve the security of location data. The experiments results showed that the proposed scheme is efficient, and that the location privacy can be also protected.

Keywords: smart city, location-based services, privacy, digital envelope, dummies

1. INTRODUCTION

In 2009, IBM first proposed the concept of "Smarter Planet", suggested the government to invest in a new generation of intelligent infrastructure. The idea quickly gets response and has led to the boom of construction of smart city within the scope of the whole world. Smart city [1, 2] is an advanced form of urban informationilization after Digital City and Smart City, and also a deep integration of informationilization, industrialization and urbanization. Moreover, smart city is a result of the combination of Internet, big data, mobile networks, cloud computing and Internet of Things [3-7]. In essence, smart city is a new model that gathers the wisdom of the human being, gives "objects" with intelligence, and mixes people and objects in a perfect and dynamic way to achieve the optimization of urban development. Simply speaking, smart city is to make full use of information technology providing better service and ensure sustainable urban development. Thus, information and data have become the "brain" of a smart city and let the

Received July 11, 2016; revised August 7, 2016; accepted August 30, 2016.
Communicated by Zhe Liu.

connation of smart city continue to expand around the core of serving people. As a main part of smart city, Intelligent Transportation can avoid traffic congestion; achieve reduction of energy emission which attracts wide attention, including government, companies and academia [8, 9].

Intelligent transportation is one of the important signs of social intelligence developing. It is also a main focus that information technology encourages the development of social intelligence. Intelligent Transportation System (ITS for short) is an approach that uses wireless communication, computer, automatic control, satellite positioning and other advanced technologies to improve the existing road facilities and create a new interactive way among human, vehicles and road. That is to say, ITS collects real-time information, including traffic information and service information, and transfers it to each user after processing by the traffic management center. Then users can select traffic routes and transportation depending on the actual situation. Management department can also manage vehicle and road timely to reach a maximum traffic facilities utilization rate, alleviate traffic congestion, shorten the delivery time, reduce transportation costs and environmental pollution.

Location-Based Services (LBS for short) [10, 11] is the basis of intelligent transportation and has a huge user group. LBS integrates various technologies, including equipment location technology, wireless communication technology and geographic information management, in order to provide personalized service to users which related to them current location [12]. In other words, the personalized service is based on the mobile users' geographical location during the process. Intelligent equipment mainly through two ways to collect location of moving subjects (1) Build-in positioning equipment, such as GPS and Wi-Fi in phones and car navigations, can directly capture accurate position of specified subjects at any time, and release location information through a variety of ways. For example, some new applications of mobile social network [13] can release users' position at any time [14]. (2) Wearable devices that widely used recently can capture acceleration, optical images and other data which can be used to determine the users' location information after processing [15].

While LBS bring great convenience to us, it also brings a lot of threats and challenges to people's privacy. Due to the complexity of the smart city, the privacy of people who involve in becomes more complex. Privacy means personal data that cannot be interference, illegal collection and use. Privacy right is one of the basic rights today which involves the collection, transmission, storage and process of personal data. Therefore, LBS privacy protection has become a hot research topic no matter in the industry or in academia. In 2003, Beresford first proposed the concept [16] of location privacy, which opened a precedent for the study of LBS privacy protection. Since then, LBS privacy protection has increasingly become a research hot topic in the field of information technology. Ghinita summarizes the location privacy from two aspects of private query and anonymous trace, but it does not involve private metrics and query privacy [17]. Krumm focused on the anonymity, privacy preserving techniques and some privacy violation algorithms based on the location data set, but it does not involve the system structure and query privacy [18]. Huo Zheng *et al.* study from the traditional relational data privacy protection to temporal and spatial orientation, then analyse and compare the key technologies of trajectory privacy protection in data publishing and trajectory privacy protection in LBS, but it not relates to query privacy [19]. Shin *et al.* summarized the LBS pri-

vacy threat model, analyze and compare various LBS privacy protection technology and metrics, but the system structure and the protection of technology are not comprehensive [20]. Durr *et al.* used the method of coordinate transformation to segment the user's accurate position into a number of finite precision positions that achieves the security management of location information, but it does not involve private metrics and query privacy [21]. Huang Yi *et al.* proposed a collaborative user anonymous zone of privacy protection method named Co-Privacy [22]. It reaches the effect of *k*-anonymity without sacrificing the user's quality of service, and improves the overall performance of the anonymous system, simplifies the query processing, but it does not involve privacy measure.

At present, most of the researches of location privacy use a single protection method, such as dummies or encryption method. However, these methods are also given some problems, including a lower degree of privacy preserving, a high overhead of computing and communication, needing a third-party organization and so on. Therefore, we propose a privacy protection model based on digital envelope and dummies (PPM-DED for short) for LBS. In the second part of this paper, we give the formal definition of the model, the model description and the key algorithms in the model. The third part is the analysis of security and performance of the model, and in the final, we give a summary of this paper.

2. PRIVACY PROTECTION MODEL BASED ON DIGITAL ENVELOPE AND DUMMIES

2.1 Formal Definition

Before giving the formal definition of the model designed in this paper, we first give the definition of location privacy.

Definition 1: Privacy refers to the information that individuals, organizations or institutions and other entities does not mean to be known by external, such as personal interests, political beliefs, company's financial situation and so on.

Definition 2: Personal Privacy is generally refers to the information that data owner is not willing to disclose the confidential and sensitive information, such as hobbies, health status, income level, religious beliefs and political inclinations. And definition of limitation is different led to the definition of privacy differ. In general, any information that can be identified, but the individual is not willing to reveal it can be considered as a personal privacy.

Definition 3: Location Privacy is a special kind of personal privacy, refers to the information that directly related to personal sensitive information when connected to the LBS query, like the accessible location is sensitive, and other personal sensitive information deducted from location, such as hobbies, health situation, religion *etc.* Individual locations include the location of its present or past visit. Therefore, the location privacy relates to (1) whether the user is accurate positioning; (2) whether the user's sensitive personal information is inferred from the position where he ever accessed. Thus, location privacy protection is not only necessary to protect the user's past and present position

from exploiting, but also to prevent an attacker to infer the user's location via other sensitive personal information.

2.2 Model Description

This paper proposed a location privacy protection model based on digital envelope and dummies which uses the distributed peer to peer structure, as distributed peer to peer structure has high effectiveness and does not require third-party anonymous server. It can distributed data to each node which improves the stability of the system.

Definition 4: User's Basic Information (*UBI*) represented by two-tuple, formally represents each user's information as

$$UIB = (id, u, p)$$

in which, *id* is user ID that randomly created by system, *u* is user name, *p* is user's password.

Definition 5: LBS Query usually represented by four-tuple, formally represents each LBS query as

$$LQ = (u, loc, t, c).$$

In which, *u* is user name related to *UBI*, *loc* is user's current location coordinates, *t* is current query time, *c* is user's query content.

Definition 6: Track Position is represented as

$$T = \{(x_1, y_2, t_2), (x_2, y_2, t_2), \ldots, (x_n, y_n, t_n)\}$$

in which, $(x_i, y_i, t_i)(i = 1, \ldots, n)$ represents a moving object at time t_i on position (x_i, y_i), t_i is the time.

Definition 7: Spatial Heterogeneity Original track T at time t_i is (x_i, y_i, t_i), and the location of dummy track T' is (x'_i, y'_i, t'_i), so the spatial heterogeneity of this position is $SH(T, T') = \sqrt{1+(t_i - t'_i)^2((x_i - x'_i)^2 + (y_i - y'_i)^2)}$, and the spatial heterogeneity of this track is $TotalSH(nT, nT') = \sum SH(nT, nT')$.

Definition 8: Location privacy protection model can be defined as three-tuple (S, A, P), S is the set of participants, A is the set of encryption algorithm, P is the set of protocols.

$S = \{U, DB, LBS, USC, LSC\}$, in which, $U = (u_1, u_2, \ldots, u_n)$ is the set of mobile terminal users; *DB* is a database for storing information; *LBS* is location based server that providing location services; *USC* is the built-in security processor for client; *LSC* is the built-in security processor for location based server.

$A = \{3DESEn, 3DESDe, RSAEn, RSADe\}$, in which, 3*DESEn* is encryption algorithm for location data, 3*DESD*e is decryption algorithm for cipher text of location data, *RSAEn* is encryption algorithm for key in digital envelope and *RSADe* is decryption al-

gorithm for key to decrypt cipher key.

P = {*Que*, *Per*, *Fal*}, in which, *Que* is three-party protocol among *U*, *DB* and *LBS*, used to query location information; *Per* is encryption protocol for data transmission between *U* and *LBS*; *Fal* is the false track protocol which is used to add noise for *U*'s query.

Definition 9: Untraceability refers to the low probability of analyzing *u*'s track through public information and *LQ*(*u*) query.

Definition 10: Irrelevance refers to the low probability of interrelation between user u_i and query *LQ*(*u*).

Fig. 1 descripts the model structure of location privacy protection based on digital envelope and dummies. In this model users communicate with location based serve through mobile network, *U* has location query send function and display location function; *LBS* has geographic information database and storage data function; *DB* mainly storages *LBS* data which is stored as ciphertext.

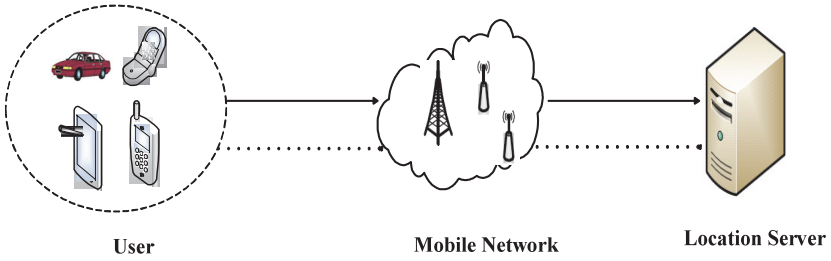


Fig. 1. The model structure of location privacy protection.

Our model contrary to defect that location service query relies on third-party anonymous server to protect location privacy, via user and LBS to process the query information which apportions the computing into two part, improving the efficiency of information processing.

(1) Initialization

DB_{uer}, DB_{ori}, DB_{Loc} represents user basic information database, original location database, encrypted location database.

DB_{user} = {Rec[1], Rec[2], …, Rec[n]}, Rec[i] represents record i in DB_{user}, $1 \le i \le n$.
DB_{ori} = {Rec[1], Rec[2], …, Rec[n]}, Rec[i] represents record i in DB_{ori}, $1 \le i \le n$.
DB_{Loc} = {Rec[1], Rec[2], …, Rec[n]}, Rec[i] represents record i in DB_{Loc}, $1 \le i \le n$.

(2) Query process

Location query includes two steps: interaction between *U* and *DB* and interaction between *DB* and *LBS*. When *U* sends a request message to *LBS*, the *DB* in server receives position and then *LBS* extract this message from *DB* to search in geography database and send back to *DB*; *U* match the data on *DB* and decrypts the message to get the exact position. Wherein, *DB* plays data storage capabilities throughout the process.

(3) Process of creating false position

User proposes $LQ(u)_{ori}$ query, the system generates random noise value *rand* according to range of noise that user specified, then adding noise value *rand* into original query $LQ(u)_{ori}$ and get $LQ(u)_{fake}$. By calculating the distance between original position and false position to judge whether this point matches the standard of create false position, if so, add it to the location database; on the contrary, to regenerate.

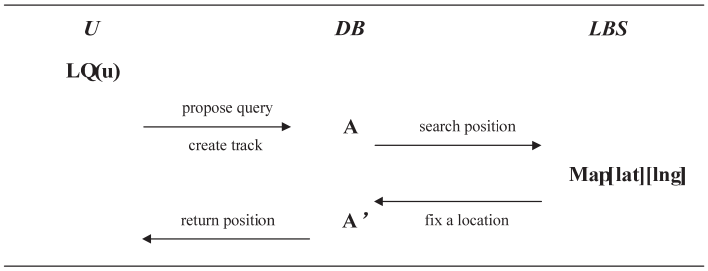


Fig. 2. Que protocol.

Algorithm 1: False position generation algorithm

Input: personal location I, request message q, the range of creating false position ($\sigma_{\min}$, $\sigma_{\max}$).

Output: send anonymous area, including false position and real position, to LBS. When $t = 0$, create false position, that is, create false position for starting point.

01: $A_0 = (x_0, y_0)$, user's real location at time $t = 0$

02: $B_0 = (x'_0, y'_0) = Random(A_0)$, false position created around A_0

03: $C_0 = dist(A_0, B_0) = \sqrt{(x_0 - x_0)^2 + (y_0 - y_0)^2}$ distance between real position and false position

04: if ($C_0 \in (\sigma_{\min}, \sigma_{\max})$), if C_0 meets the requirement of distance, return this position to location data set

05: return C_0

06: *else*($C_0 \notin (\sigma_{\min}, \sigma_{\max})$), then goto step 2, if C_0 does not meet the requirement, return to step 02.

Algorithm 2: Dummies track generation algorithm

Input: personal location I, request message q, the range of creating false position ($\sigma_{\min}$, $\sigma_{\max}$).

Output: send anonymous area, including false position and real position, to LBS.

when $t = 0$, create false position, that is, create false position for starting point.

01: $A_0 = (x_0, y_0)$, user's real location at time $t = 0$

02: $B_0 = (x_0, y_0) = Random(A_0)$, false position created around A_0

03: $C_0 = dist(A_0, B_0) = \sqrt{(x_0 - x_0)^2 + (y_0 - y_0)^2}$, distance between real position and false position

04: if ($C_0 \in (\sigma_{\min}, \sigma_{\max})$), if C_0 meets the requirement of distance, return this position to location data set

05: return C_0

06: *else*($C_0 \notin (\sigma_{\min}, \sigma_{\max})$), then goto step 02, if C_0 does not meet the requirement, return

to step 02

07: repeat step 02 to step 06 until create enough amount of positions Creating false position at $t = 1$, $i \geq 1$. In this case, the module not only considers the distance, but also thinks over whether the track is similar with the original one.

08: $A_1 = (x_1, y_1)$, user's real location at time $t = 1$

09: $B_1 = ((x'_1, y'_1) = Random(A_1)$, false position created around A_1

10: repeat ② to ⑥ until create the point that meet the distance requirement

11: $T_1 = (A_0, A_1)$, track formed by real positions A_0 and A_1, $D_1 = (B_0, B_1)$, track formed by false positions B_0 and B_1.

12: calculate the similarity of T_1 and D_1

13: if ($Total(SH(T_0, T_1)) \leq$ maxadius), return B_1

14: else goto step 09

15: repeat above until create enough amount of positions

16: create false positions at time $t = 1$, ($i = 2, 3, \ldots, m$) in the same way

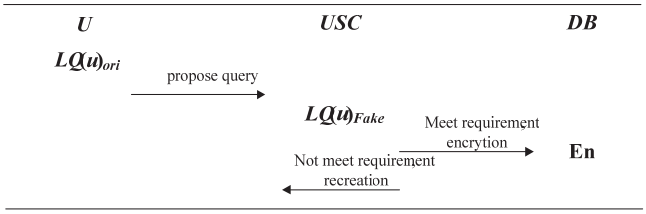


Fig. 3. Fal protocol.

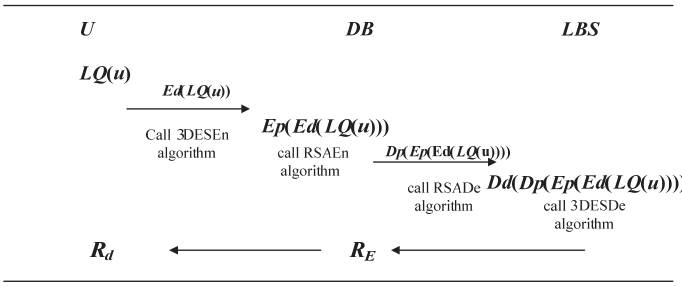


Fig. 4. Per protocol.

(4) Process of digital envelope

Fig. 4 shows the process of digital envelope between user and *LBS*. E_d means encrypt query content, E_p means encrypt key, D_p means decrypt key, D_d means decrypt query content. First, user and *LBS* create its own public key and private key, and store their on key. Uploading *LBS*'s public key to CA and send user's public key to *LBS* together with other encrypted data. Next, user sends location request $LQ(u)$ to LBS, and use 3*DESEn* from set A to encrypt query content, then get the result $E_d(LQ(u))$. User downloads digital certification of *LBS* from CA, and uses *RSAEn* from set A to encrypt key by *LBS*'s public key, then get the result $E_p(E_d(LQ(u)))$. User sends ciphertext together with public key to *LBS*. When *LBS* extract data from *DB*, it uses its private key to de-

crypt text and get the result $D_p(E_p(E_d(LQ(u))))$. Then *LBS* decrypts query content by 3*DESDe* and gets the result $D_d(D_p(E_p(E_d(LQ(u)))))$ to position latitude and longitude. Finally, repeating digital envelope process from *LBS* to user, the encrypt result R_E stor ages in database, and decrypt result is R_d.

3. MODEL ANALYSIS

3.1 Security Analysis

Que protocol, Per protocol and Fal protocol is the key technology of PPM-DED for the security of these three protocol directly affects the privacy of PPM-DED. This section proved the security of Per protocol and Fal protocol in detail.

Definition 11: Perfect Anonymous is used to let attacker cannot find relevance between user and location query, in which, $U = \{u_1, u_2, \ldots, u_n\}$ is set of users, q is user's query $P[q(u_i)] = \frac{1}{n}$ represents the probability of query q requested by user u_i.

Definition 12: Blind Location Query is used to extend point set that user request to the entire LBS database.

Proposition 1: Each query is independent, that is

$$P(q_1, \ldots, q_k) = P(q_1)P(q_2) \ldots P(q_k).$$

Proposition 2: Each query entropy is the largest, that is

$$H(q_1) = H(q_2) = \ldots = H(q_k) = \log n.$$

Theorem 1: Given protocol Que and algorithm set A, execute query $q_1, \ldots, q_k$ through Per protocol, Per has private security if only $q_1, \ldots, q_k$ joint entropy is maximum.

***Proof*:** Using mathematical induction to prove, firstly consider the case of $k = 1$, following by $k = 2$, then assume that the case of $k = K$ proposition is established, to prove the case of $k = K+1$.

When $k = 1$, there is only one query execution protocol and LBS record order is randomly disturbed in order to disturbed the correspondence between encrypt record and original record. $P(q_1 = 1) = \ldots = P(q_1 = n) = \frac{1}{n}$, $H(q_1) = H_{\max}(q_1) = \log n$. Proposition 2 is proved.

When $k = 2$, for LBS reads an encrypted record is irrelevant with $q_1 = q_2$ or $q_1 \neq q_2$, q_1 and q_2 are independent variables for LBS. Therefore, $P(q_1, q_2) = P(q_1)P(q_2)$, $H(q_1) = H(q_2) = \log n$. Proposition 1 is proved.

We assume that $P(q_1, \ldots, q_k) = P(q_1)P(q_2) \ldots P(q_k)$, $H(q_1) = H(q_2) = \ldots = H(q_k) = \log n$. Considering query $K+1$, according to proposition 1 and proposition 2, $H(q_1) = H(q_2) = \ldots = H(q_k) = \log n$, $P(q_1, \ldots, q_k, q_{k+1}) = P(q_1)P(q_2) \ldots P(q_k)P(q_{k+1})$. Proposition is proved.

Theorem 2: Que protocol achieves the perfect anonymity, meet PPM-DED untraceability.

***Proof*:** When Que protocol executes in PPM-DED, location data transmission is encrypted between U and DB due to USC security process. Thus, interaction privacy can be guaranteed between U and DB.

LBS cannot obtain $LQ(u)$, and further, cannot get u's loc. So, Que protocol achieves perfect anonymity, that is to say, user set $U = (u_1, u_2, \ldots, u_m)$ the anonymity of u_i is k, $k = n$. And for the probability of determining the location of u_i is $\frac{1}{n}$ at each LBS query, entropy is log$n$ which up to the maximum entropy.

Therefore, analysis from the view of LBS, users' location is disorderly, and we can come to conclusion that the system is untraceable.

Theorem 3: Que protocol achieves the blind location query, meet PPM-DED irrelevance characteristic.

***Proof*:** For DB_{ori} = {Rec[1], Rec[2], …, Rec[n]}, DB_{Loc} = {Rec″[1], Rec″[2], …, Rec″[n]} are vector set, Rec[i] and Rec″[j] are random vectors of DB_{ori} and DB_{Loc}. Analyzing from the view of information theory, the probability that attacker exactly guesses Rec[i] and Rec″[j] is $\frac{1}{n}$, the information entropy that generated by each query is:

$$H(q) = \sum_{i=0}^{n} p(x_i) \log \frac{1}{p(x_i)} = \sum_{i=0}^{n} \frac{1}{n} \log n = \log n.$$

Therefore, from the above equation, information entropy of each query is up to maximum.

And for each query is independent with each other, attacker cannot capture any information from query, the joint entropy m is

$$H(q_1 \ldots q_m) = \sum_{i=1}^{m} H(q_1) = m \log n.$$

Thus, from above equations, joint entropy of a number of queries is up to maximum. According to Theorem 1, Que protocol has private security, and further proves that Que protocol achieve blind location query, meet irrelevance characteristic.

Theorem 4: System achieves perfect anonymity and blind location query if only PPM-DED is untraceable and irrelevance.

3.2 Performance Analysis

Experiments of performance analysis are under Microsoft Visual C++ 6.0 on Windows platform. The testing machine uses Inter® Core™ i5 CPU, memory 4GB, and database is Microsoft Access Server. The initial data is under transportation network map of Shenyang, China.

Performance testing focuses on the following aspects of the location-based services privacy protection model based on the digital envelope and dummies:

(1) Comparing the location exposure risk between dummies generation algorithm of this model and random generation algorithm.

Firstly, when creating the same number of tracks, we compare the track exposure risk of dummies generation algorithm and random generation algorithm. The user's location and track of this model are protected by the dummies generation algorithm and in random model, the user's locations are created in the range of longitude and latitude that user sets.

In the process of performance testing, we define the following variables.

Definition 13: Exposure risk of a single location

Assuming that m is the total number of points containing in the real-track T, S_i is the location point set of real-track T_r and dummies track T_d at t_i. $|S_i|$ is the cardinality of S_i and probability of exposure of real-location is $\frac{1}{|S_i|}$. We define the average probability that user's real-location can be distinguished by others is the exposure risk of a single location, recorded as LD, $LD = \frac{1}{m}\sum_{i=1}^{m}\frac{1}{|S_i|}$.

Definition 14: Exposure risk of track

Assuming that the total number of real-track and dummies is n, and at least k tracks have cross points with extra track, and $n-k$ tracks have no intersection points with others. N_k is the total number of tracks that created by k intersect tracks. We define the probability that the user's real-track can be inferred from all tracks are exposure risk of track, recorded as TD, $TD = \frac{1}{N_k + (n-k)}$.

Definition 15: Distance Deviation

The average distance among all real-track and dummies at t_i is defined as distance deviation, recorded as DD, $DD = \frac{1}{m}\sum_{i=1}^{m}(\frac{1}{n}\sum_{j=1}^{n} dist(T_r^i, T_d^j))$. Wherein, $dist(T_r^i, T_d^j)$ represents the Euclidean distance between two points.

We select longitude between 121 and 125, latitude between 40 and 44 on the map as an experimental area. Table 1 shows the user's track points. We set t = 1 min as time interval and assume that when the user reach the next position, he will propose a new location query.

Table 1. Longitude and Latitude of user's track.

Longitude	121.685	121.890	121.960	122.075	122.146	122.131	122.4312	122.4407
Latitude	40.9465	40.9078	40.9212	40.9745	41.0282	41.1073	41.2301	41.3334

According to Table 1, we test exposure risk of a single location and track, Figs. 5 and 6, and analyze the relation between distance deviation and running time which shows on Fig. 7.

From Figs. 5 and 6, we conclude that creating the same number of false positions and dummies, exposure risk on our model is less. The more false positions and dummies are generated, the lower value of LD and TD, and privacy exposure of this model is sig-

nificantly lower than the normal random generation algorithm.

From Fig. 7, for the dummies generation algorithm of this model need to judge the distance from original track, so the running time is more than random generation algorithm, but it can be seen that the difference between them is not too large. By contrast, in the case of the user's own privacy requirements are very high, dummies generation algorithm of this model can achieve privacy protection better than the random generation algorithm.

(2) Query privacy protection test

As mentioned in the query privacy metrics framework, attacker attains some prior knowledge, such as age and gender of the user. Thus the posterior probability of user's query q' is $p(u \mid q') = \dfrac{p(u \mid q)}{\sum_{u' \in u(r,t)} p(u' \mid q)}$, wherein, u is one of users in user set, $u(r, t)$ is area at time t.

Fig. 8 shows the measure of dummies generation algorithm when attacker have or does not have prior knowledge. Prior knowledge database is composed of user's gender, address and other data set, Shenyang traffic network and the location query request by users.

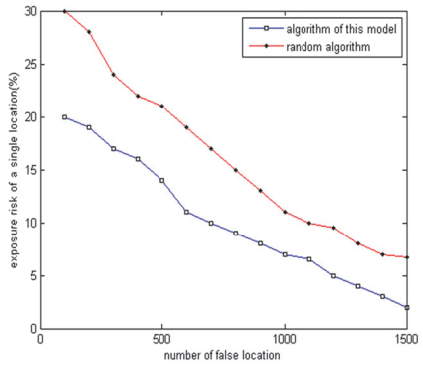


Fig. 5. Exposure risk of locations diagram.

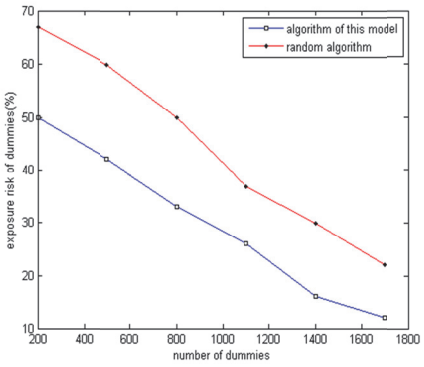


Fig. 6. Exposure risk of dummies diagram.

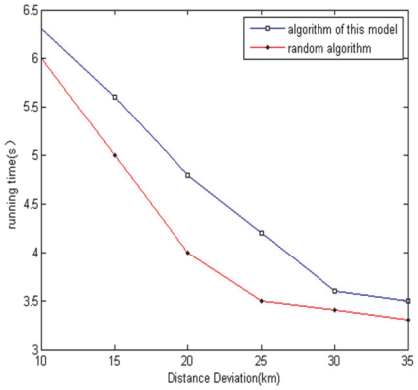


Fig. 7. Contrast diagram of the running time of dummies generation algorithm.

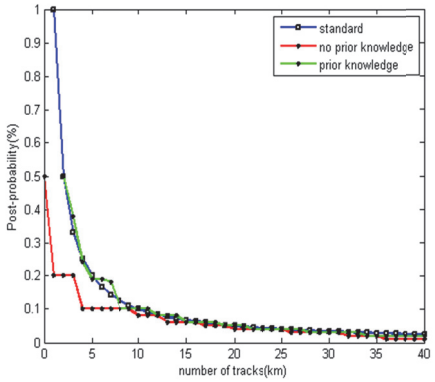


Fig. 8. Distance Deviation and posterior probability relation diagram.

As the number of users and track increasing, the probability that attacker identify a specific user will drop. In view of attacker, each user has the same probability to send a location query within a restricted area and the probability to obtain the exact location of a user shows in red line of Fig. 8. When attacker has prior knowledge, the probability of each query from user is not the same for a user's range of motion is limited. The dummies generation algorithm of our model takes the spatial heterogeneity into consideration which increasing the difficulty of attacking. The result shows in the green line of Fig. 8. The posterior probability is under the baseline which proves the probability of the user's privacy exposure can be accepted.

(3) Performance of encryption and anonymity protection

Encryption method achieves the goal of privacy protection through encrypting the location query. The system uses distributed structure which can strictly protect user's location information and guaranteed service availability. Table 2 shows the comparison of the performance of each privacy protection method.

4. CONCLUSIONS

LBS is an important part of emerging network service and has been integrated into the social networking, electronic commerce, life services and other fields, even become more and more popular around the world. However, it also produces the issue of privacy disclosure. Recently, there are two types of attacks on users' location: (1) Single point attack, that is, the attacker can only get the user's location in a specify time. (2) Track attack, namely, the attacker continuously observes multiple users' location points and according to a certain order, the single point is connected into track, which can be used to predict the personal privacy, such as user's interests, hobbies and so on. In order to solve the problem, efficient location privacy protection scheme which is based on digital envelope and dummies is proposed in this paper. The formal definition and construction method of this model are also given in this paper. The experimental results were based on various parameters (*e.g.* exposure risk of a single location and distance deviation), showing that the scheme is efficient, and that the location privacy can be protected well.

ACKNOWLEDGEMENTS

The authors would like to thank the reviewers for their detailed reviews and constructive comments, which have helped improve the quality of this paper. This work was supported in part by the National Natural Science Foundation of China under Grant No.61440014, the Liaoning Province Doctor Startup Fundunder Grant No. 20141012, the Liaoning Province Science and Technology Projects under Grant No. 2013217004, the Shenyang Province Science and Technology Projects under Grant No. F14-231-1-08, the Fundamental Research Funds for the Central Universities under Grant No. N151704002.

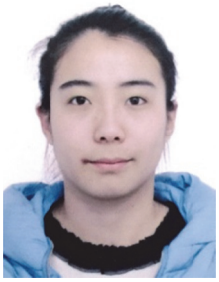
REFERENCES

1. F. H. Zhou, Z. J. Li, S. H. Chen, and G. Xiong, "Parallel transportation management

control system and its applications in building smart cities," *IEEE Transactions on Intelligent Transportation Systems*, Vol. 17, 2016, pp. 1576-1585.
2. F. J. Villanueva, C. Aguirre, A. Rubio, D. Villa, *et al*., "Data stream visualization framework for smart cities," *Soft Computing*, Vol. 20, 2016, pp. 1671-1681.
3. Z. H. Xia, X. H. Wang, X. M. Sun, and Q. Wang, "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data," *IEEE Transactions on Parallel and Distributed Systems*, Vol. 27, 2015, pp. 340-352.
4. Z. J. Fu, X. M. Sun, Q. Liu, L. Zhou, and J. G. Shu, "Achieving efficient cloud search services: Multi-keyword ranked search over encrypted cloud data supporting parallel computing," *IEICE Transactions on Communications*, Vol. E98-B, 2015, pp. 190-200.
5. Y. J. Ren, J. Shen, J. Wang, J. Han, and S. Y. Lee, "Mutual verifiable provable data auditing in public cloud storage," *Journal of Internet Technology*, Vol. 16, 2015, pp. 317-323.
6. Z. Liu, H. Seo, J. Großschädl, and H. Kim, "Efficient implementation of *NIST*-compliant elliptic curve cryptography for 8-bit AVR-based sensor nodes," *IEEE Transactions on Information Forensics and Security*, Vol. 11, 2016, pp. 1385-1397.
7. Z. Liu, X. Y. Huang, Z. Hu, M. K. Khan, H. Seo, and L. Zhou, "On emerging family of elliptic curves to secure internet of things: ECC comes of age," *IEEE Transactions on Dependable and Secure Computing*, Vol. 99, 2016, pp. 237-248.
8. P. Kachroo and S. Sastry, "Traffic assignment using a density-based travel-time function for intelligent transportation systems," *IEEE Transactions on Intelligent Transporation Systems*, Vol. 17, 2016, pp. 1438-1447.
9. M. B. Younes and A. Boukerche, "A performance evaluation of an efficient traffic congestion detection protocol (ECODE) for intelligent transportation systems," *Ad Hoc Networks*, Vol. 24, 2015, pp. 317-336.
10. M. Werner, "Privacy-protected communication for location-based services," *Security and Communicaton Networks*, Vol. 9, 2016, pp. 130-138.
11. X. Lin, J. L. Xu, and H. B. Hu, "Reverse keyword search for spatio-textual top-*k* queries in location-based Services," *IEEE Transactions on Knowledge and Data Engineering*, Vol. 27, 2015, pp. 3056-3069.
12. M. Benisch, P. G. Kelley, N. Sadeh, and L. F. Cranor, "Capturing location-privacy preferences: quantifying accuracy and user-burden tradeoffs," *Personal and Ubiquitious Computing*, Vol. 15, 2011, pp. 679-694.
13. T. H. Ma, J. J. Zhou, M. L. Tang, Y. Tian, A. Al-Dhelaan, M. Al-Rodhaan, and S. Lee, "Social network and tag sources based augmenting collaborative recommender system," *IEICE Transactions on Information and Systems*, Vol. E98-D, 2015, pp. 902-910.
14. N. Jabeur, S. Zeadally, and B. Sayed, "Mobile social networking applications," *Communications of ACM*, Vol. 56, 2013, pp. 71-79.
15. M. Sousa, A. Techmer, and A. Steinhage, "Human tracking and identification using a sensitive floor and wearable accelerometers," in *Proceedings of IEEE International Conference on Pervasive Computing and Communications*, 2013, pp. 166-171.
16. A. R. Beresford and F. Stajano, "Location privacy in pervasive computing," *IEEE Pervasive Computing*, Vol. 2, 2003, pp. 46-55.
17. G. Ghinita, "Private queries and trajectory anonymization: A dual perspective on

location privacy," *Transactions on Data Privacy*, Vol. 2, 2009, pp. 3-19.
18. J. Krumm, "A survey of computational location privacy," *Personal and Ubiquitous Computing*, Vol. 13, 2009, pp. 391-399.
19. Z. Huo and X. F. Meng, "A survey of trajectory privacy preserving techniques," *Chinese Journal of Computers*, Vol. 34, 2011, pp. 1820-1830.
20. K. G. Shin, X. E. Ju, and Z. G. Chen, "Privacy protection for users of location-based services," *IEEE Wireless Communications*, Vol. 19, 2012, pp. 30-39.
21. F. Durr, P. Skvortsov, and K. Rothermel, "Position sharing for location privacy in non-trusted systems," in *Proceedings of IEEE International Conference on Pervasive Computing and Communications*, 2011, pp. 189-196.
22. Y. Huang, Z. Huo, and X. F. Meng, "Coprivacy: A collaborative location privacy-preserving method without cloaking region," *Chinese Journal of Computers*, Vol. 10, 2011, pp. 1976-1985.

Jian Xu (徐劍) received his Ph.D. degree in Computer Application Technology from Northeastern University in 2013. He is currently an Associated Professor at Northeastern University. His research interests include cryptography and network security.



Si-Jia Zhao (趙思佳) received the B.S. degrees in Information Security from Northeastern University and currently study for a MS degree at Trinity College Dublin. Her research interests include network security, distributed system and mobile computing.

Fu-Cai Zhou (周福才) received his Ph.D. degree of Computer Software and Theory at Northeast University. He is currently a Professor and Doctoral Supervisor of Information Science and Engineering College in Northeastern University. His research interests include cryptography, network security, trusted computing, basic theory and critical technology in electronic commerce.