Journal of Information Hiding and Multimedia Signal Processing ©2018 ISSN 2073-4212
Ubiquitous International Volume **9**, Number **6**, November **2018**

An Improved Location Privacy Protection Scheme

Cheng Song, Yadong Zhang*, Lei Wang and Zhizhong Liu

School of Computer Science and Technology
Henan Polytechnic University
Jiaozuo, Henan, 454000, China
*Corresponding author:18339161026@163.com

Received March, 2018; revised August, 2018

Abstract. *To solve the problem of Location privacy protection in mobile Internet, an improved scheme is proposed based on theory of bilinear pairings and K-anonymity. Mobile terminal first generates evenly $2k$ false locations in circular region of Euclidian Distance, and picks out $k-1$ false locations from them according to location entropy, location dispersion and mapping background information, then randomly selects one terminal from the k locations including itself and asks the selected location terminal to request LBS server instead of it by using oblivious transfer protocol. So the scheme can achieve a higher anonymity. Security analyses prove that this scheme not only has such security properties as anonymity and non-forgeability, but also is able to resist query tracing attack. And simulation experiment shows that this scheme has better evenness and efficiency in generating and selecting false locations.*
Keywords: LBS; Bilinear pairings; K-anonymity; Privacy protection

1. **Introduction.** With the rapid development of location technology, mobile communications and intelligent equipment, location-based services has been widely used and benefited more and more users. Location-based services (LBS) [1-4] have been applied into many fields like social networks, medical care, transportation, etc. However, when location-based services provide services to user, user sensitive data information is likely collected so that privacy is leaked. For instance, user's family address and health information, life habits can be detected by checking map information and gathering user's location information [5]. Therefore, user's privacy protection of LBS has been a hot issue[6-8]among domestic and foreign scholars.

K-anonymity is one of important privacy protection technologies. Based on K-anonymity privacy protection scheme was first proposed by KIDO, et al. [9]. The basic idea of the scheme is to generate many false locations for one user, then a false location is selected and sent to LBS server together with user's real location, so that both attacker and server can't identify user's real location. LU et al. [10] proposed two pseudo location generation algorithms: CirDummy and GridDummy. However, the false locations of these two algorithms are based on random movements and virtual circles or grids, which can't guarantee the anonymity if the attacker obtains the background information. WANG et al. [11] introduced a location-aware location privacy protection scheme because they found that users' level of privacy protection may vary due to different locations in continuous location requests. JIA et al. [12] presented two cloaking algorithms which don't exposure accurate location. They are designed for -anonymity, and cloaking is performed based on the identifications (IDs) of the grid areas which were reported by all the users, instead of

directly on their accurate coordinates.

NIU et al. [13] argued that those schemes failed to consider whether attacker discerns background information or not, which may decide the probability of attacker's identification of user's real location. So they put forward a new scheme: create as many false locations (with the same query frequency as user's real location) as possible to strengthen user's privacy protection. However, this scheme doesn't apply to continuous LBS request query, for attacker may identify user's real location based on the connection between neighboring query time and space. Based on the idea of ciphertext matching, SCHLEGE et al. [14] proposed a ciphertext-based location privacy protection scheme that serves to resist query tracing attack when the third-party is guaranteed to be trustworthy. LUO et al. [15] proposed an improved personalized k-anonymous location privacy protection algorithm with fake loaction generation mechanism. By generating fake queries for the source queries that expire, our algorithm guarantees that no source query will be dropped, namely all the source queries can get anonymized. LI et al. [16] claimed that constructing cloaking area based on other users' historical footprints may create an over-sized cloaking area, which in turn reduces service quality. So they proposed a demand-aware location protection scheme for continuous LBS requests, which minimizes the cloaking area by deleting the farthest footprints so as to improve service quality. Nevertheless, this scheme fails to resist query tracing attack when users send requests without the preset/predicted position. FEI et al. [17] proposed a two-tier schema for the privacy preservation based on k-anonymity principle meanwhile reduce the cost for privacy protection.

Aimed at those limitations, this paper devises a security-strengthened location privacy protection scheme based on theory of bilinear pairings and K-anonymity. In this scheme, mobile node is used to generate evenly $2k$ false locations in annular domains of Euclidian Distance, then k-1 optimal false locations are screened out from those false locations based on position entropy, location dispersion and map background information. Finally, the mobile node randomly selects one terminal from the k locations including itself and asks the selected location terminal to request LBS server instead of it by using an optimized oblivious transfer (OT) protocol. In this way, the evenness of false locations can be optimized and K-anonymity can be better improved.

The rest of this paper is organized as follows: In section 2 we introduce preliminaries. The improved scheme is described in detail in section 3. We give the security analyses in section 4. In section 5, we give the simulation experiment about efficiency and evenness. The last section concludes the paper.

2. **Preliminaries.**

2.1. **System Structure of Location Privacy Protection.**

On the basis of k-anonymity theory, this paper devises a confusion server. As is shown in Figure.1, the system is composed of three parts: confusion server, mobile terminal and location information server. The functions of each part are as follows:

Confusion server: confusion server is required to be equipped in anonymity location privacy protection so as to generate pseudonyms for mobile terminal user and send the result to mobile terminal.

Mobile terminal: on the one hand, mobile terminal sends pseudonym-generating request to confusion server and verifies the validity of the pseudonym; on the other hand, it generates and screens out false location nodes, sends location query request to location information server, and receives query result from the server.

Location information server: this is the core of location privacy protection system,

responsible for processing anonymity query from mobile terminal and returning query result to the terminal.

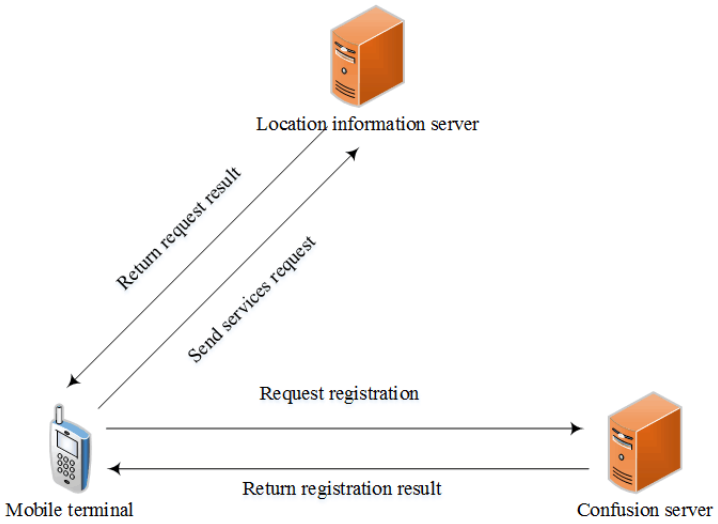

FIGURE 1. System model of location privacy protection

2.2. **Bilinear Pairings.** Let $(G_1, +)$be an addition cyclic group of prime order q, $(G_2, \times)$ be a multiplication cyclic group of order q, P be a generator of G_1. Bilinear map $e : G_1 \times G_1 \to G_2$ satisfies the following properties:

Bilinearity: $\forall a, b \in Z_q^*, P, Q \in G_1, e(aP, bQ) = e(P, Q)^{ab}$;

Non-degeneracy: $\exists P, Q \in G_1$, satisfies $e(P, Q) \neq 1$;

Computability: for each arbitrary $P, Q \in G_1$, there is a valid algorithm to compute $e(P, Q)$.

2.3. **Position Entropy.** When mobile terminal user sends service request to LBS server, privacy level is measured by the privacy measure standard of single user. Assume that the query probability of k candidate false location nodes and k false locations is $Y_i (i = 1, 2, \ldots, k)$, then the probability of each location becoming real location is:

$$Pr(i) = \frac{Y_i}{\sum_{j=1}^{k} Y_i} \tag{1}$$

Specify a cloaking area with k false locations, the probability of user being at any false location i is Y_i, its position entropy is:

$$W(x) = -\sum_{1=1}^{k} Pr(i) \times \log_2 Pr(i) \tag{2}$$

Therefore, position entropy of nodes can be calculated via formula $Pr(i)$ and $W(x)$, which means attacker could guess the information of real location. The bigger the entropy values of candidate location nodes are, the more the privacy protection is strengthened. Apparently, when all $Pr(i)$ are equal, the biggest the entropy values of location nodes are, and the highest the level of privacy protection will be.

2.4. **Location Dispersion.** If the nodes in the set of multiple false location nodes have equal position entropy and maximum entropy values, location dispersion is required to screen them out once again. Because the bigger the location dispersion of false location nodes set is, the bigger the area that they create will be. In this way, it can be avoided that over concentration of the generated false nodes will enable attacker to locate the area where user's real location is and cause location privacy disclosure. Besides, location dispersion is measured by the distance product of false location node pairs.

As is shown in Figure. 2, assume that o is the real position of user, p is the selected false location, then the third false location can be singled out from two candidate locations m and n by elliptic construction. Let o and p be two focuses of ellipse and construct m and n in the ellipse. Since $mo + mp = no + np$, it is difficult to decide which node to select only based on the sum of distance between false node pairs. On other hand, since $mo \times mp > no \times np$, node m is selected as the false location instead of node n , because node m has bigger dispersion.

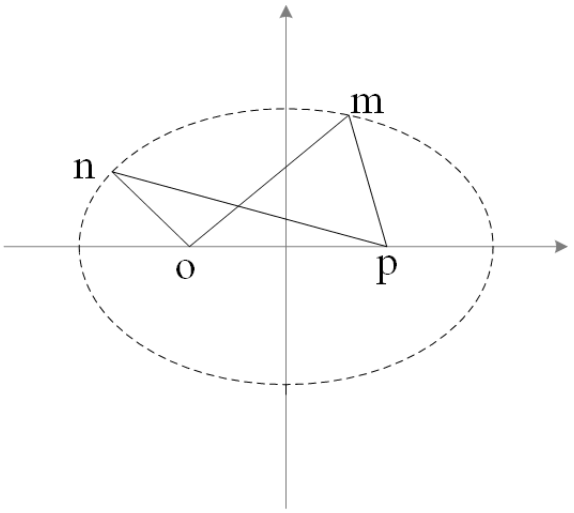

FIGURE 2. Chart of screening candidate nodes

3. **Improved Location privacy Protection Scheme.** This scheme mainly includes four phases: system initialization, user registration, false location generation & selecting, and location service request.

3.1. **System Initialization.** In this phase, system parameters are generated as follows:

Step 1: G_1 and G_2 are two cyclic groups of prime order q, G_1 being addition cyclic group G_2 being multiplication cyclic group, and P being the generator of G_1 . $e : G_1 \times G_1 \to G_2$ stands for a bilinear map. Z_q^* stands for the integer multiplicative group of modular q .

Step 2: Define two secure hash functions: H_1 and H_2, and an encrypted function $enc()$ based on elliptic curve cryptosystem. And $H_1 : \{0,1\}^* \to \{0,1\}^k$, $H_2 : \{0,1\}^* \to G_1$, $\{0,1\}^*$ stands for binary series of any length.

Step 3: Confusion server selects master key $s \in Z_q^*$ for the system, calculate its public key as $P_A = sP$.

Step 4: Confusion server keeps master key s , exposes system parameter: $G_1, G_2, e, k, P, P_A, H_1, H_2, enc()$.

3.2. **User Registration.** Since this scheme is devised on the basis of K-anonymity, so in this phase, confusion server is employed to anonymize users' identities, which is as follows:

Step 1: The user u randomly selects a secret value $r_u \in Z_q^*$, and sends r_u and user's real ID to confusion server to request registration.

Step 2: After receiving registration request, confusion server calculates false identity for user$PID_u = enc(H_1(ID||r_u))$, then calculates $Q_u = H_2(PID_u)$, $X_u = sQ_u$, and returns $\{PID_u, X_u\}$ to u by secure channel.

Step 3: After receiving message $\{PID_u, X_u\}$,u calculates $\bar{Q_u} = H_2(PID_u)$ and judges whether $e(X_u, P) = e(\bar{Q_u}, P_A)$ is valid or not. If the equation is valid, registration succeeds; u calculates $u_{PK} = Q_u$ and $u_{SK} = X_u$, Otherwise, register goes back to Step 1.

3.3. **False Location Generation & Selecting.** In this phase, false locations are generated from mobile terminal users, and $k-1$ optimal locations are selected from $2k$ false locations. As follows:

Step 1: With real location Loc_u of u being a center, mobile terminal user generates a false location Loc_i by employing algorithm of evenly-distributed random points in rectangular region, then specifies the location based on mapping background information. If the location is mountains or rivers, it is discarded and another location is generated; otherwise, calculates Euclidean distance between location Loc_u and Loc_i : $dis(Loc_u, Loc_i)$.

Step 2: Mobile terminal user judges whether equation $R_{min} < dis(Loc_u, Loc_i) < R_{max}$ is valid or not. If valid, let $c_i = Loc_i$, and add it into location set $C = \{c_1, c_2, \cdots, c_{i-1}\}$, then $C = \{c_1, c_2, \cdots, c_{i-1}\} \cup \{c_i\}$; if not, return to Step 1. R_{min} and R_{max} respectively stand for the shortest and longest distance from center to newly-generated false node.

Step 3: if $i < 2k$, $i = i + 1$; return to Step 1; if $i < 2k$, go to next step1.

Step 4: Assume query probability of false location in false location node set C is $w_i(i = 1, 2, \cdots, 2k)$, then it can be speculated that the probability of each false node location becoming real node location is Y_i based on Formula 1. The closer Y_i is to the query probability of real location Loc_u, the higher is the location entropy $W(x)$ and the higher the privacy protection level will be. According to this principle, $k-1$ optimal false locations can be selected from $2k$ false locations $\{Loc_1, Loc_2, \cdots, Loc_{k-1}\}$.

Note: In Step 4, if parallel and in eliminable false nodes exist in critical positions, that is, probability Y_{i-1} of candidate false location Loc_{k-1} and Loc_k becoming real node location is equal to Y_i , then according to location dispersion principle, mobile terminal judges whether or not the inequality $dis(Loc_u, Loc_{k-1}) \times dis(Loc_p, Loc_{k-1}) > dis(Loc_u, Loc_k) \times dis(Loc_p, Loc_k)$ is valid. If valid, select Loc_{k-1} as candidate location; otherwise select Loc_k . Loc_u stands for location u, Loc_p the selected false location. Optimal false location set that is finally selected is $C_{End} = \{c_1, c_2, \cdots, c_{k-1}\}$.

Step 5: Register respectively each location node in optimal false location set C_{End}; generate respectively anonymous user ID: $PID_i(0 < i < k-1)$ for each false location.

3.4. **Request for Location Service.** In this phase, mobile terminal randomly selects one location node as representative to send service request to LBS server. The steps are as follows:

Step 1: User randomly selects one location node $c_j(0 < j \leq k)$ from k location nodes (real location node is included) .

Step 2: Gather false identities PID_i of k nodes, location node Loc_i and query information Q_i to form a query set:$\{Msg\{(PID_1, Loc_1, Q_1), (PID_2, Loc_2, Q_2), \cdots, (PID_k, Loc_k, Q_k)\}\}$, send service request to LBS server with location as representative.

Step 3: After receiving request, the LBS server gets the query result $\{m_1, m_2, \cdots, m_k\}$. Suppose that the user u wants to get the message $m_i, i \in \{1, 2, \cdots, k\}$, The public key

and private key of the LBS server are $A_{PK} = H_2(PID_{LBS})$ and $A_{SK} = sA_{PK}$. LBS server randomly selects $d_\sigma \in Z_q^*$, where $\sigma = 1, 2, \cdots, n$. Calculate $P_1 = d_1 A_{PK}$,$P_2 = d_2 A_{PK}$, $\cdots$,$P_n = d_n A_{PK}$, and publish them as a selection base point.

Step 4: User randomly selects $a_j \in Z_q^*$,and calculates v_i, If $i \neq j$, then $v_i = a_j$. If $i = j$, then $v_j = a_i P_i$. Finally, the user B sends the tuple $\{PID_u, v_1, v_2, \cdots, v_k\}$ to the LBS server.

Step 5: After receiving the tuple $\{PID_u, v_1, v_2, \cdots, v_k\}$, LBS server random selects temporary private key $r \in Z_q^*$,and calculates $Y_0 = rA_{PK}$, $Y_j = rv_j$ and $c_j = m_j \oplus H_1(e(P_j + A_{SK}, u_{PK}))$. Then the LBS server sends $\{Y_0, (Y_1, Y_2, \cdots Y_k), (c_1, c_2, \cdots, c_k)\}$ to the user u.

Step 6: After receiving the $\{Y_0, (Y_1, Y_2, \cdots Y_k), (c_1, c_2, \cdots, c_k)\}$, the user u calculates the multiplication inverse element $a_i^{-1} \in Z_q^*$, then calculates $V_i = a_i^j Y_i$, and finally calculates $m_i = c_i \oplus H_1(e(V_i, u_{PK})e(Y_0, u_{SK}))$ to get the message m_i.

4. **Security Analysis.** This scheme conducts security analysis in terms of three aspects: anonymity, non-forge ability and query service tracing.

4.1. **Anonymity.** In registration phase, encryption algorithm is conducted to encrypt all nodes' real identities ID to generate false identity $PID_u = enc(H_1(ID||r_u))$, so that attacker is unable to guess or obtain the real information of nodes from PID_u, hence anonymity is realized. Meanwhile, in service request, the transport protocol uses an oblivious transport protocol based on bilinear pairs. Since $\{P_1, P_2, \cdots, P_n \in G_1\}$ are not nonzero, $P_1, P_2, \cdots, P_n$ are the generator of G_1. That is $\forall Q \in G_1$,$\exists d_i \in Z_q^*$ to make $Q = d_i P_i$. Because G_1 has elliptic curve discrete logarithm problem (ECDLP): given 2 non zero $P, Q \in G_1$, it is difficult to determine $d_i \in Z_q^*$ to find $P = d_i Q$. In this scheme, because d_i is confidential for an attacker, the attacker can't know which v_j calculated by P_i, thus protecting the privacy of the user. In summary, the scheme achieves user anonymity.

4.2. **Non-forgeability.**

Theorem 4.1. *In Random Oracle Model, if attacker F exists to forge user's registration information by masquerading confusion server in polynomial time, then Diffie-Hellman, the calculative problem, can be solved with non-negligible probability in polynomial time.*

Proof: Assume attacker F is able to solve the calculative problem Diffie-Hellman with non-negligible probability in polynomial time, that is, attacker F finds s in polynomial time with non-negligible probability to make the equation $e(X_u, P) = e(Q_u, P_A)$ tenable.

Initialization: Assume that the challenger C provides system parameters $\{G_1, G_2, e, k, P, P_A, H_1, H_2, enc()\}$ for attacker F, and possesses (P, sP), in which $P_A = sP$, while s is the system key of confusion server , and is unknown to C; the attacker F requests from C a random answer of Random Oracle Model H_1, and maintains consistency to avoid conflict, and C keeps a request-reply list to store the replies from the requests.

Random Oracle Model query phase: C is able to provide Random Oracle Model query for attacker F via Random Oracle Model H_1, and provide corresponding request-reply parameters.

Attacker F conducts query via Random Oracle Model H_1 to obtain harsh values, as follows:

H_1 request: F requests the hash value of identity ID_i from C , and C detects whether there is $ID_i \in L_I$ in request-reply list;

(1) If there is $ID_i \in L_I$, then send the corresponding reply to F.

(2) Otherwise, randomly selects $\tau_i \in Z_q^*$ and calculates $H_1(ID_i)$, sends $(\tau_i, H_1(ID_i))$ to

F, and stores this request-reply in the list L_I , then the corresponding $S_{ID_i} = \tau_i H_1(ID_i)$ can be easily obtained.

Forgeability and problem-solving: attacker F forges user's registration information by masquerading confusion server, but F is unable to obtain the partial system key s of confusion server, and fails to calculate X_u , then the equation $e(X_u, P) = e(Q_u, P_A)$ is invalid. If attacker F manages to obtain the random number $s \in Z_q^*$, then it has to guess random number s via the public key (P, P_A) and $P_A = sP$ in confusion server, which means facing the calculative problem Diffie-Hellman, so attacker F is unable to solve Diffie-Hellman problem with non-negligible probability in polynomial time, which conflicts with the assumption. Therefore, the proposed scheme is able to meet the demand for non-forgeability.

4.3. **Resistance of Query Tracing Attack.** Query tracing attack is also called continuous query attack, which means that attacker obtains users set included in cloaking area based on continuous query sent by a user in different spots, and speculates the user who sends the request by calculating the intersection of users set in different cloaking areas. In this scheme, since the selected false nodes are evenly distributed, and, on the basis of the principles of position entropy, location dispersion and mapping background information, the selected false nodes and real nodes are highly similar, which produces large cloaking area, so that this scheme can be quite effective in resisting query tracing attack. Besides, because one random element is selected as representative from location nodes to send request information whenever LBS service request is sent, attacker will be impossible to obtain the real node only according to the intersection of the nodes of user's continuous query request. Through the above analysis, the comparison results of security analysis between this scheme and other relevant references are shown in TABLE 1.

Table 1. Security analysis

scheme	Ref.[6]	Ref.[7]	Ref.[8]	This paper
anonymity	√	√	√	√
non-forge ability				√
query tracing attack				√

5. **Simulation Experiment.** The environment of simulation experiment in this scheme is as follows: CPU: Intel i5 processor;RAM8G; operation systemWindows7 64 bit; simulation softwareMATLAB. In an ideal network environment, a random node is selected as user's real location, and simulation is conducted in terms of false location generation efficiency and evenness of location distribution that conforms to user's requirements.

The performance index of false location generation algorithm is manifested in efficiency and location evenness. In identical experiment environment, the traditional scheme, CirDummy scheme and GirdDummy scheme are compared. Figure.3 shows the result: there is a linear relation between the time of generating user's false location and anonymity level K , which means that rise of anonymity level K also causes the time required in generating user's ideal location to lengthen. In fact, as anonymity level K rises, more false locations are generated, which also increases the required false locations, and in turn lengthens generation time.

It can be found in simulation experiment that the efficiency of generating required false locations in this scheme is approximate to the efficiency of traditional scheme when $K \leq 5$ the efficiency of this scheme has more advantage over that of traditional scheme when $K > 5$. This is because the false locations generated by the algorithm of traditional

scheme are within the angle θ.in clockwise rotation, that is $\theta = 2\pi/(K-1)$, so with the increase of anonymity level K, angle θ becomes sharper and sharper, while the probability of false locations being generated in angle θ becomes lower and lower. Therefore, as the increase of anonymity level K , the efficiency of traditional algorithm generating the required false locations turns out to be lower and lower than that of the scheme in this paper. Besides, compared with CirDummy scheme and GirdDummy schemealong with the increase of K , the efficiency of this scheme will be higher and higher.

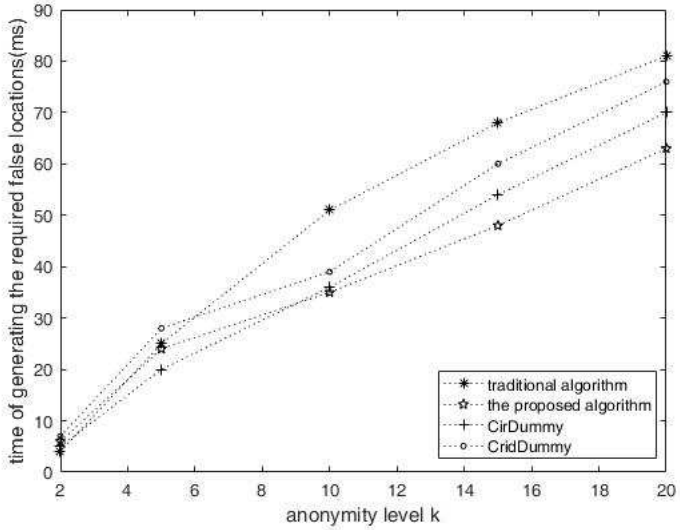

FIGURE 3. Relation between anonymity level k and time of generating the selected locations

As for evenness of location distribution, the more similar the selected locations are to real locations, the higher evenness will be, and the more evenly the false nodes are distributed, which means attacker will be more difficult to find the real location. Evenness of location distribution is shown in $v = f/k$, in which f stands for minimum rectangular region area of real locations and false locations, k stands for anonymity. Obviously, with fixed f , location evenness declines as increases. This simulation experiment selects locations within the range of region radius from minimum 0.1 km to maximum 0.15 km. The simulation comparison of this scheme with traditional scheme and CirDummy scheme in equal environment is shown in Figure.4. Since this scheme adopts position entropy, location dispersion and mapping background information to screen each false location, so the evenness of location distribution is invariably better than tradition algorithm, solving the problem of shrinking cloaking region caused by over-concentration of location nodes and in turn increasing attacker's difficulty of finding user's real location. Due to the fact that in this experiment false nodes are selected in circular area, GirdDummy scheme is not compared and analyzed.

6. **Summary.** To solve the problem of Location privacy protection in mobile Internet, an improved scheme is proposed based on theory of bilinear pairings and K-anonymity. This scheme employs mobile terminals to generate evenly false $2k$ locations in circular region of Euclidian distance, and screens $k-1$ optimal false locations from $2k$ false locations based on position entropy, location dispersion and mapping background information. Security analyses prove that this scheme is able to solve such problems as anonymity, non-forgeability, Man-in-Middle attack and query attack, effectively reinforcing security.

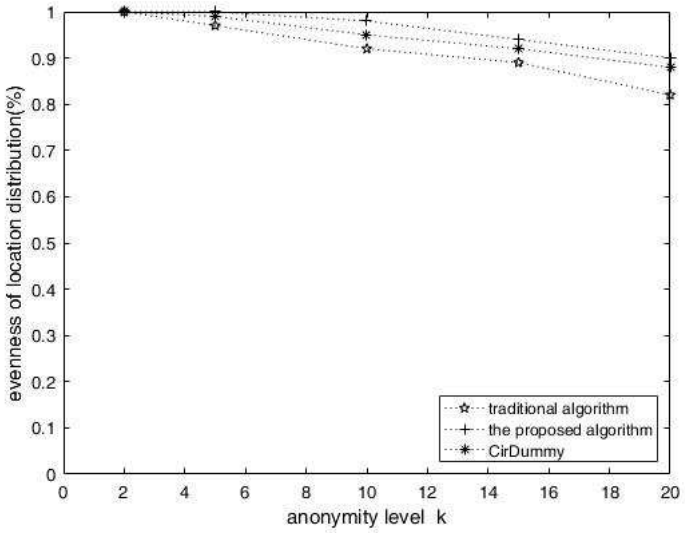

FIGURE 4. Relation between anonymity level k and evenness of location distribution

Simulation experiment shows that the efficiency of generating required false locations in this scheme is approximate to that of traditional scheme when , while the efficiency of this scheme has more advantage over that of traditional scheme when . Meanwhile, this scheme has better evenness of false location, which makes user's privacy more secure. Therefore, this scheme is of important theoretical research and applicable value in the field of LBS location privacy protection in mobile Internet or Internet of Things with limited resources.

Acknowledgment. This work was supported by the National Natural Science Foundation of China (61300216, 61300124, 61772159, 61872126), the Science and Technology Research Program of Henan Province (172102310677).

REFERENCES

[1] M. Xin, M. Lu, W. Li, An adaptive collaboration evaluation model and its algorithm oriented to multi-domain location-based services, *Expert Systems with Applications*, vol.42, no.5, pp.2798-2807, 2015.

[2] Y. M. Sun, M. Chen, L. Hug, Y. F. Qian, and M. M. Huang, ASA: Against statistical attacks for privacy-aware users in Location Based Service, *Future Generation Computer Systems*, vol.70, 2016.

[3] X. H. Li, M. X. Miao, J. F. Ma and K. C. LI, An incentive mechanism for K -anonymity in LBS privacy protection based on credit mechanism, *Soft Computing*, vol.21, no.5, PP.3907-3917, 2017 .

[4] N. Talukder, S. I. Ahamed . Preventing multi-query attack in location-based services, *CM Conference on Wireless Network Security*, ACM, pp.25-36, 2010.

[5] K. Fawaz, G. S. Kang Location Privacy Protection for Smartphone Users, *ACM Sigsac Conference on Computer and Communications Security*, ACM, pp.239-250, 2014.

[6] S. Gao, J. F. Ma, W. S. S, G. X. Zhan, and C. Sun, TrPF: A Trajectory Privacy-Preserving Framework for Participatory Sensing, *IEEE Transactions on Information Forensics & Security*, vol.8, no.6, pp.874-887, 2013.

[7] S. Mascetti, D. Freni, C. Bettini, X. S Wang, and S Jajodia, Privacy in geo-social networks: proximity notification with untrusted service providers and curious buddies, *The international Journal on Very Large Data Bases*, K. Aizawa, Y. Nakamura, and S. Satoh (eds.), vol.20, no.4, pp: 541-566, 2011.

[8] X. X. Liu, K. K. Liu, L. K. Guo, X. L. Li, and Y. G Fang, A game-theoretic approach for achieving k-anonymity in Location Based Services, *INFOCOM, 2013 Proceedings IEEE*, IEEE, pp.2985-2993, 2013.

[9] H. Kido, Y. Yanagisawa, Satoh T. Protection of Location Privacy using Dummies for Location-based Services, *International Conference on Data Engineering Workshops*, IEEE Computer Society, pp.1248, 2005.

[10] L. Hua, C. S Jensen, L. Y Man, PAD:privacy-area aware dummy-based location privacy in mobile services, *ACM International Workshop on Data Engineering for Wireless and Mobile Access Mobide 2008, June 13, 2008*, Vancouver, British Columbia, Canada, Proceedings. DBLP, pp.16-23, 2008.

[11] Y. Wang, D. Xu, X. He, C. Zhang, F. Li, and B. Xu, TrPF: A Trajectory Privacy-Preserving Framework for Participatory Sensing, *INFOCOM, 2012 Proceedings IEEE*, IEEE, pp.1996-2004, 2012.

[12] J. Jia, F. Zhang, Nonexposure accurate location K-anonymity algorithm in LBS, *Scientific World Journal*, vol.2014, no.3, p.619357, 2014.

[13] B. Niu, Q. Li, X. Zhu, G Cao, and H. Li, Achieving k-anonymity in privacy-aware location-based services, *IEEE INFOCOM*, IEEE, pp: 754-762, 2014.

[14] R. Schlegel, C. Y Chow, Q. Huang, and D. S. Wong, User-Defined Privacy Grid System for Continuous Location-Based Services, *IEEE Transactions on Mobile Computing*, vol.14, no.2, pp: 2158-2172, 2015.

[15] Z. Luo, X. Huang, A Personalized k-Anonymity with Fake Position Generation for Location Privacy Protection, *Communications in Computer & Information Science*, vol.502, p.46-55, 2015.

[16] X. Li, E. Wang, W. Yang, and J. Ma, DALP: A demand-aware location privacy protection scheme in continuous location-based services, *Concurrency & Computation Practice & Experience*, vol.28, no.2, pp.1219-1236, 2016.

[17] F. Fei, S. Li, H. Dai, C. Hu, W. Dou, and Q. Ni, A K-Anonymity Based Schema for Location Privacy Preservation, *IEEE Transactions on Sustainable Computing*, vol. 99, pp. 1-9, 2017.