LBS privacy protection technology based on searchable encryption mechanism

Tao Feng[1,*], *Xudong* Wang[1], and *Xinghua* Li [2]

[1]Lan zhou University of Technology School of Computer and Communication, Lanzhou, China
[2]Xi dian University Network and Information Security College, Xi'an, China

Abstract. Location based Service (the Location - -based Service, LBS) is a System is to transform the existing mobile communication network, wireless sensor networks, and Global Positioning System (Global Positioning System, GPS) with the combination of information Service mode, the general improvement in Positioning technology and the high popularity of mobile intelligent terminals, led to the growing market of LBS. This article from the perspective of LBS service privacy security, mainly studies the LBS location privacy protection scheme based on cipher text search, in LBS service location privacy and search information privacy issues, focus on to design the scheme, based on the cryptography in LBS service privacy protection issues in the process, this paper fully and secret cipher text search characteristics, design a new privacy protection of LBS service model, and expounds the system structure and working principle of model, defines the security properties of the privacy protection model and security model, Under the specific security assumptions, the new location privacy protection scheme based on lbspp-bse (LBS location privacy protection based on searchable encryption) is implemented.

1 Introduction

With the rapid development of the Internet of things, location-based services have become ubiquitous, providing network communication services to any user whenever and wherever they are located. Through GPS devices, everything can be achieved through WIFI, 4G networks, bluetooth and other wireless transmission systems. Therefore, use the portable intelligent device and positioning function, makes the orientation of individual users location become more convenient and accurate, and it can be done by low cost and low power devices, so the location based service (LBS) more and more get the welcome of people [1]. Through to specific LBS server requests personalized location-based services, in order to provide related services, location-aware applications require the user to obtain his or her exact position, the requirements on the user's request and related position information will be provided to the server without reserve [2].

However, in the process of users' enjoyment of services, the issue of user privacy has been paid attention to by many scholars and researchers, because it exposes users' privacy information[3]. According to the literature [4], the user's location information can be

* Corresponding author: fengt@lut.cn

obtained by the relevant server at anytime and anywhere. The more information that is exposed to the user, the more accurate the attacker's analysis of the user is. As individual users become more dependent on smartphones, users are becoming more adept at using smart terminals to obtain relevant location services. Therefore, the location server should reasonably obtain user location privacy information [5] [6] [7]. Therefore, location service providers are not only facing great challenges to protect users' privacy, but also provide relevant location services according to users' requirements [8].

2 Related research

According to the literature [9], the real information of mobile users is usually hidden among other k-1 users. Entropy based measurement is also commonly used to protect the privacy of mobile phone users. The Voronoi diagram scheme is based on the way of road network, and the grid sends the request to realize k-anonymous purpose [10]. This involves the prediction of the user movement to implement the cooperative k-anonymous scheme, so how to effectively build an anonymous area will be a problem that needs to be solved.

Mobile users often protect users' privacy at the expense of communication. In order to solve this problem, a short-distance communication method based on anonymous regional space has been proposed. Based on the existing p-2-p scheme and the short-distance communication defect of regional space anonymity, a method of variance attack is used in the k-anonymous scheme based on spatial concealment [11].

Described in the literature [12] plan, will be based on the contents of the service of privacy protection and location privacy protection is divided into two stages, the system will be through private channels after their own hidden location information to the server. The second communication will upload the information to the server for information retrieval.

In addition to the previously mentioned LBS privacy protection scheme and mechanism, zero knowledge proof (zero - knowledge, ZK) [13] although there are some shortcomings in some ways, but still showed a zero knowledge proof in the advantages of safety, but also got the favour of the researchers and scholars. It should be the focus of the research on how to provide users with efficient and accurate services and the maximum protection of users' privacy issues in all protection schemes.

3 Basic knowledge of cryptography

The protocol is based on cryptography, so we need to make a special statement as follows:
Definition 3.1 Let $\langle G, * \rangle$ is an algebraic system, including $G \not\subset \varnothing$, * is a binary operation on the G, if $\langle G, * \rangle$ comply with the following properties:
(1) Closed: For $\forall x,y \in G$, satisfy $x*y \in G$.
(2)Conjugacy: For $\forall x, y \in G$, satisfy $x*(y*z) = (x*y)*z$.
(3)There is a unique unit: $\exists ! \ \forall \ x \in G$, making $x*e=e*x=x$ true.
(4)There is an inverse element: $\forall x \in G$, there is an inverse element x^{-1} such that $x* x^{-1}=x^{-1} * x = e$ holds. Then we call $\langle G, * \rangle$ a group.

Definition 3.2 Let $\langle G, * \rangle$ be a group. If G is a finite set, then we call this group a finite group. On the contrary, it is called an infinite group. The cardinality p of the group G is called the order of the group G, denoted as $|G|$.

Definition 3.3 If the operation in the group $\langle G, * \rangle$ satisfies the commutativity, in other words, for $\forall x,y \in G$, there is $x*y=y*x$, then we call it the Abelian group, or It is a exchange group.

Definition 3.4 Let's call $\langle G, * \rangle$ a group, and if there is an element x in G that satisfies any element in G that can be expressed as a power, then we call this group a cyclic group, and say that x is the generating element of that group.

Definition 3.5 Let G and G_T represent the p-order cycle group, where p is prime, and is a generator of g. Then there is a bilinear mapping e: $G \times G \rightarrow G_T$ satisfies the following properties:

(1) Bilinear: For all $g, f \in G$ and $a, b \in Z_p$, satisfy $e(g^a, f^b) = e(g, f)^{ab}$.

(2) Non-degenerate: There are $g, f \in G$ such that $e(g, f) \neq 1$.

(3) Computability: For all $g, f \in G$, there is a valid polynomial-time algorithm that can compute the corresponding $e(g, f)$.

Definition 3.6 q - BDHE assumption: Let G and G_T represent the p-order cycle group, where p is prime, and is a generator of g. Then there is a bilinear mapping e: $G \times G \rightarrow G_T$.Let

$$\vec{v}=g,g^{s}, g^{a}, g^{a^{q}}, g^{a^{q+2}}, g^{a^{2q}}, \forall_{1\le j\le q}, g^{s\cdot b_j}, g^{s/b_j}, g^{a^{q}/b_j}, g^{a^{q+2}/b_j},\ldots, g^{a^{2q}/b_j}, \forall_{1\le j,\, k\le q, k\ne j} g^{a.s.b_k/b_j},\ldots, g^{(a^{q}\cdot s.b_k/b_j)} \quad (1)$$

where a,s, b_1, …, $b_q \in Z_p$. The vector $\vec{v}$ sent to an attacker, there is no probability polynomial time algorithm to solve H, by non-ignorable $Q=e(g,g)^{a^{q+1}s} \in G_T$ with random elements $Q \in G_T$ to distinguish, H time algorithm advantage is defined as:

$$\Delta = \left| Pr\left[H\left(\vec{v},\ Q = e(g,g)^{a^{q+1}s}\right) = 0 \right] - Pr\left[H\left(\vec{v},\ Q \in G_T\right) = 0 \right] \right| \quad (2)$$

4 Scheme construction

4.1 LBSPP-BSE scheme model

This article proposed LBS location privacy protection scheme based on ciphertext search (LBSPP - BSE) general model as shown in fig.1. The model contains the following objects: LBS Server (LBS Server), user (Users) and trusted authority (TrustAuthority, TA).

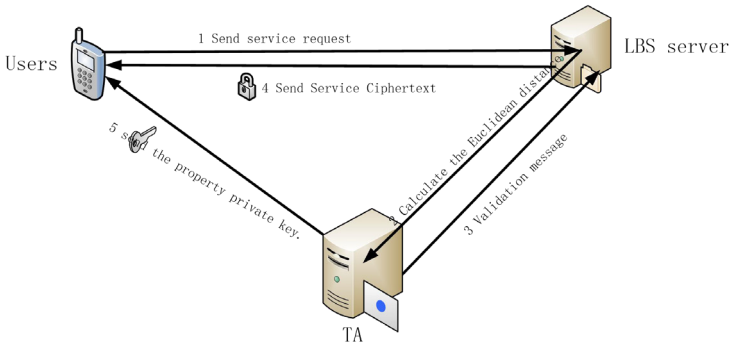

Fig. 1. LBSPP-BSE scheme model.

4.1.1 LBS server

The LBS server in this scheme is a comprehensive server that contains the location server and the data owner module. The server not only provides data storage capabilities to the data owner, but also performs encryption of the stored data. At the same time, the LBS

server also needs to match the requested ciphertext information of the user, and then feedback the ciphertext information required by the user to the user.

4.1.2 Users

After being authorized, the authorized user can access the ciphertext data in the LBS server and at the same time, upload the location information to the trusted third party. When the trusted third party generates the private key based on the user's location information, it is sent to the user. A user saves the private key, and decrypts the ciphertext through the key, so as to obtain the required ciphertext.

4.1.3 TA

In the scenario of this article, we are based on this part is completely trusted. The trusted authority performs the system initialization program, then generates the global parameters and the master key of the system, and then generates a user private key according to the geographical location information provided by the user, and sends it to the user for self-storage. After the search is successful, the ciphertext information is decrypted.

4.2 LBSPP-BSE solution detailed description

This scheme mainly consists of six algorithms: initialization, generation of private key, encryption ciphertext, generation threshold, search matching, decryption ciphertext, and detailed description below.

4.2.1 Setup (1^{μ}*, U)→（PK, MSK）*

The trusted third party executes the Setup algorithm, input the security random parameter μ, and the global attribute set U, |U|=*n*. First, select two cyclic groups with prime number *p*, G, G_T, randomly select two generated elements $g, g_1 \in G$, and then select three random Numbers *a,b,c*, and then choose random values u_1， u_2， ……,$u_n \in G$, hash function H_1：$\{0,1\}^* \to Z_p$, H_2： $\{0,1\}^* \to Z_p$, *PK* public parameters. Trusted third party storage system master key *MSK*={a,b,c}.

4.2.2 KeyGen (PK, MSK ,Ua) →SK

Input system public key *PK* and master key *MSK*, and user's attribute set Ua, trusted third party executes KeyGen algorithm. Output user private key *SK*.

4.2.3 Encryption (PK, As, Loc, w) →CPH

The LBS server executes a keyword encryption algorithm. Enter the keyword location information *Loc*, the access structure As = (M, φ, Λ) and the keyword *w* that needs to be encrypted. Where *M* is the current matrix of $l \times n$ and φ is a single mapping function that maps each row of the matrix to the attributes of the user, $\Lambda=(t_{\varphi(1)},\cdots, t_{\varphi(t)}) \in Z_p^t$, from the first row to the *l* th row, calculate $\lambda_{\varphi(i)} \leftarrow \vec{v} \bullet M_i$, where M_i is the vector corresponding to the *i* th row of the matrix *M*.
Output ciphertext *CPH*

$$CPH=\{A,\ B,\ x\in [1,l]\{C_x,D_x\}, W_1, W_2\} \tag{3}$$

4.2.4 TokenGen (PK, SK , W, Loc_U, d) →TK

Enter the user's private key *SK* and the keyword *W* to be checked, and the server executes the threshold generation algorithm. Loc_U is the location ciphertext message of the user, and Loc_U= Encrypt（Gps，PK）, the search radius is *d*, and the output threshold *TK*:

$$TK =\{T_1,\ T_2,\ T_3,\ T_4,\ T_x\}_{s_x\in Ua} \tag{4}$$

4.2.5 Search (PK , CPH, TK) →CPH'or F

Input system public key *PK*, ciphertext *CPH* and threshold *TK*, cloud server performs ciphertext search algorithm. Assume that the user attribute set Ua meet access structure(M, φ, Λ), then there must be a set of values $\{\omega_i \in Z_p\}_{i\in I}$ makes the $\sum_{i\in I}\omega_i\lambda_i=q_2$, including $I=\{i,\varphi(i)\in Ua\}$. The system output *CPH'* indicates that the retrieval is successful, otherwise the output F fails.

4.2.6 Decrypt (PK , SK, CPH') → m / ⊥

Enter the system public key *PK*, the user private key *SK*, and the encrypted ciphertext *CPH'*. The user performs the algorithm to decrypt. For the original ciphertext, if *m* is output, the key search succeeds, and the relevant cipher text exists, and the user's private key is included. The attribute has already met the access structure in the ciphertext, and then the ciphertext can be successfully decrypted. Otherwise, the search fails.

5 Safety analysis

This scheme can resist attacks by unauthorized users based on background knowledge.

Proof: We introduced the public and private key system to achieve the user's location information and request information in the complete ciphertext status. We use the ciphertext algorithm for the user's request information (L_{oc} ,*Q*). Select random value $\sigma \leftarrow Z_p$, $T_1=\left(g^b g^{aH_1(w)}\right)^{\sigma}$, $T_2=(g)^{\sigma c}T_3=K^{\sigma}=g^{(bc+at)\sigma}$, $T_4=L^{\sigma}=g^{t\sigma}$, $x\in$Ua, $T_x=(K_x)^{\sigma}=\left(u_x^{s_x}\right)^{t\sigma}$, Loc_U is the user's location information, and *d* is the query radius set by the user. Output threshold *TK* .

User's ciphertext *CHP*, user private key *SK* as input. And then we calculate

$$\frac{e(B,K)}{\prod_{i\in I}(e(C_i,L)e(D_i,K_i))^{\omega_i}}=e(g,g)^{\alpha s} \tag{5}$$

This scheme can resist the unauthorised user to carry out the anti-camouflage attack.

Proof: Due to this scenario to the user's location information and the request information is encrypted, so, even if the attacker position ciphertext information, also hard to disguise, trusted third party to perform the KeyGen algorithm. Please select random value $t\leftarrow Z_p$, calculate $K=g^{bc+at}$,$L=g^t$, for random $s_i$please$s_i \leftarrow Z_p$, $s_i\in Ua$, $K_i=\left(u_i^{s_i}\right)^t$. The output user's private key *SK*={K, L,$\{K_i\}_{s_i\in Ua}$ }, it is difficult for the adversary to obtain the user's private key, so it can resist the camouflage attack.

6 Conclusion

For LBS location privacy protection scheme in the practical application feasibility and efficiency, and three problems of privacy protection, this paper made the following three points: (1) improved in scheme based on cipher text search, proposed a more safe and effective LBS location privacy protection system in the practical application feasibility and efficiency; (2) the protection of LBS location privacy, including the trusted third party key mechanism, effectively protects the location privacy and query privacy of the LBS users; (3) the problem of disclosing users' privacy in LBS service, using ciphertext access structure, thus protecting users' privacy information.

References

1. C.Chow,M.Mokbel,X.Liu. A peer-to-peer spatial loaking algorithm for anonymous location-based service[C]. ACM on Advances in geographic information systems, 171-178,(2006)
2. R. Cramer, I. Damgard, and J. B. Nielsen, “Secure multipartycomputation and secret sharing: Aninformation theoretic approach”, Book Draft, (2012).
3. Blumberg, Andrew J, Eckersley, et al. On Locational Privacy, and How to Avoid Losing it Forever[J]. Electronic Frontier Foundation, (2009).
4. L. Calderonia, P. Palmierib, and D. Maioa, “Location privacy without mutual trust: The spatial bloom filter”, Computer Communications, vol. **68**, pp. 4–16, (2015).
5. L. Kulik, “Privacy for real-time location based services,” SIG SPATIAL Special vol. **1**, no. 2, pp. 9–14.
6. X Shu, D Yao. Data Leak Detection as a Service[M]// Security and Privacy in Communication Networks. Springer Berlin Heidelberg, 222–240, (2012).
7. S. V. Watzdorf, and F. Michahelles, “Accuracy of positioning data on smartphones. In: Loc Web, ACM(2010).
8. X. Pan, and X. Meng, “Preserving location privacy without exact locations mobile services”, Front. Comput. Sci. vol. **7**, no.3, pp. 317-340,(2013).
9. L.Sweeney, “k-anonymity: a model for protecting privacy,” Int.J.Uncertain. Fuzziness Knowl-Based Syst., vol. **10**, no. 5, pp.557–570,Oct. (2002).
10. C. Ma, C. Zhou, and S. Yang, “A voronoi-based location privacypreserving method for continuous query in LBS,” Int. J. Distrib. Sens.Networks, vol. **2015**,(2015).
11. B. Niu, X. Zhu, Q. Li, J. Chen, and H. Li, “A novel attack to spatial cloaking schemes in location-based services,” Futur. Gener. Comput. Syst., vol. **49**, pp. 125–132, (2015)
12. R. Paulet, M. G. Kaosar, X. Yi, and E. Bertino, “Privacy-preserving and content-protecting location based queries,” IEEE Trans. Knowl. Data Eng., vol. **26**, pp. 1200–1210,(2014).
13. E. Brickell, J. Camenisch, and L. Chen: Direct anonymous attestation. In Proc. 11th ACM Conference on Computerand and Communications Security, pp. 132 -145, ACM Press, (2004).