Advanced Science and Technology Letters
Vol.31 (ACN 2013), pp.98-103
http://dx.doi.org/10.14257/astl.2013.31.23

CSPC: A Context-Sensitive Personalized Collaborative Location Privacy Preserving Method

Nianhua Yang[1,2], Yuru Cao[2], Qing Liu[2], and Jiming Zheng[2]

[1] Department of Computer Science and Engineering
Shanghai Jiaotong University, Shanghai 200240, China
[2] School of Business Information Management
Shanghai University of International Business and Economics, Shanghai 201620, China
yangnh@sjtu.edu.cn, caoyuru2003@suibe.edu.cn, liuq@suibe.edu.cn, zhengjiming@suibe.edu.cn

Abstract. This paper proposes a decentralized cloaking region creation approach to protecting location privacy. The cloaking region is formed through collaboration to hide the precise position of the location based service requestor. A mobile user can set personalized anticipated and minimum privacy requirements respectively according to different contexts. The anticipated parameters will be satisfied if the time is allowed. Otherwise, the system will pursue the minimum standards for privacy requirements. This approach can satisfy k-anonymity, l-diversity and cloaking granularity simultaneously for privacy preserving.

Keywords: location privacy, personalize, decentralize

1 Introduction

In order to protect location privacy in LBSs (Location-Based Services, LBSs), different researches have been conducted based on k-anonymity [7], l-diversity [4] or cloaking granularity [5] approaches. For location privacy preserving, the exact geographic position value is extended to a cloaking region. The anonymization server, which delegates the user, sends the LBS requests to the service provider based on the cloaking region substituting for the exact geographic position. For computing a cloaking region, methods based on k-anonymity, l-diversity or cloaking granularity hold different privacy metrics. K-anonymity based methods extend a cloaking region until k-1 other users are included. L-diversity based methods extend the cloaking region until l-1 different locations are included. Cloaking granularity requires the cloaking region to be larger than a user-specified threshold.

Although these methods guarantee location privacy in some degree, each of them has a critical limitation. In a k-anonymity based cloaking region, some requestors may hold the same location value. And in an l-diversity based one,

ISSN: 2287-1233 ASTL

requestors may be in a very small populated area. So they can't be able to prevent the location disclosure. A granularity based cloaking region can not defend against attacks for requestor identifies in the case where the locations are publicly known and there is only one requestor in the cloaking region [6].

On the other hand, most of previous location privacy preserving methods [3], [8] rely on a centralized trusted third party (TTP). A mobile user (requestor) sends its geographic location and query requirement to the centralized trusted anonymizing proxy. The location cloaker in the trusted anonymizing proxy extends the geographic location into a cloaking region according to the cloaking algorithm. Then, the cloaking region and corresponding query requirement are sent to the LBS provider by the trusted anonymizing proxy. After getting the qurey results for the cloaking region from the LBS provider, the trusted anonymizing proxy will select the exact results according to the exact geographic location from the results of the cloaking region. At the end, the exact results will be returned to the mobile user. However, the trusted anonymizing proxy knows every exact geographic location of the requestor, and it may pose serious privacy threats. Furthermore, the trusted anonymizing proxy could be a system bottleneck in the TTP-based architecture.

In order to overcome these inherent drawbacks in the TTP-based system architecture, more and more researches have paid attentions to decentralized location privacy preserving approaches [1]. Though these decentralized approaches can avoid performance bottleneck and hostile attacks on the anonymizing proxy, most of them just consider part of privacy metrics among k-anonymity, l-diversity and cloaking granularity.

The ability for forming a cloaking region in a system may be different under different contexts. In a populated area, a k-anonymity based cloaking region can be easily formed even if k is very large. But it is hard to form the cloaking region in a sparsely populated region even if k is very small. So the privacy requirement parameters in a location anonymization model should be personalized and context-sensitive.

This paper proposes a context-sensitive personalized collaborative location privacy preserving method (CSPC). It corporates privacy metrics of k-anonymity, l-diversity and cloaking granularity.The privacy requirement can be personalized. It is realized in a decentralized architecture.

2 The CSPC Architecture

CSPC is decentralized and the location anonymization is realized through collaboration among neighbors. In addition, each user can assign a personalized minimum level as well as an anticipated level parameters for k-anonymity requirement. Similarly, it can assign a personalized minimum level as well as an anticipated level parameters for l-diversity requirement. Furthermore, the mobile user can assign a personalized minimum level and anticipated level of s for the side length of the cloaking region. Each user can also assign a maximum temporal value it is willing to tolerate when waiting for forming an anonymizing

area. In a general area, the cloaking region should satisfy the requirements of the anticipated levels for k-anonymity, l-diversity and the side length of the cloaking region. If these anticipated requirements can't be satisfied within the assigned temporal limitation, the requirements can be relaxed to the minimum levels.

Each mobile client holds a privacy profile that specifies its desired privacy requirements. A privacy profile includes seven parameters, $k_{\min}$, k_{nor}, $l_{\min}$, l_{nor}, $s_{\min}$, s_{nor} and T. $k_{\min}$ and k_{nor} represent the minimum level and anticipated level for k-anonymity requirement respectively. $l_{\min}$ and l_{nor} represent the minimum level and anticipated level for l-diversity requirement respectively. $s_{\min}$ and s_{nor} represent the minimum level and anticipated level for the side length of the cloaking region respectively. T represents the temporal limitation the user can tolerate for computing the cloaking region.

3 The CSPC Algorithm

3.1 Data Structure

The mobile user and its neighbors communicate with each other to discover at least other k-1 neighbors until the cloaking region satisfies k-anonymity, l-diversity and cloaking granularity metrics within T units of time.

Messages are divided into two types, i.e. type={FG, ACK}. FG is used to find nearest neighbors for forming an anonymity group. Likewise, ACK is used to reply the FG message.

Structures of a message broadcasted by the LBS requestor for searching nearest neighbors and the corresponding reply message are described in Def. 1 and Def. 2. The structure of a cloaking region is described in Def. 3.

Definition 1 *(Message for searching nearest neighbors) A query message for searching the nearest neighbors is defined as* $Q_n = (M_{id}, h, type, S_{id})$*, where* M_{id} *is the message sequence ID,* h *represents the hop distance propagated in the network,* $type = FG$ *and* S_{id} *is the pseudonym of the message sender.*

Definition 2 *(Reply message for group forming) A reply message for group forming is defined as* $R = (M_{id}, A, type)$ *where* M_{id} *represents the message sequence given by the requestor,* $type = ACK$*,* $A = \{(LCA_{id}, R_{id})\}$ *is the set of the tuples, each of which consists of locally cloaked areas (LCA) [2] and corresponding* R_{id} *which represents the pseudonym of the replier. An LCA is used to obfuscate the precise location of the mobile user.* $LCA = ((x_1, y_1), (x_2, y_2))$*, where* x_1 *and* y_1 *are the longitude and latitude of the left button corner of the LCA respectively, while* x_2 *and* y_2 *are the longitude and latitude of the top right corner of the LCA respectively.*

Definition 3 *(Cloaking region) A cloaking region is defined as* $CR = ((x_1, y_1), (x_2, y_2))$*, where* x_1 *and* y_1 *are the longitude and latitude of the left button corner of the cloaking region respectively, while* x_2 *and* y_2 *are the longitude and latitude of the top right corner of the cloaking region.*

3.2 Cloaking Algorithm

Firstly, a mobile requestor broadcasts searching messages to find nearest neighbors. After finding enough neighbors to form a cloaking region which satisfies k-anonymity, l-diversity and cloaking granularity requirements, the mobile requestor computing the cloaking region and sends it to the members among the cloaking region.

In order to prevent a neighbor to get the exact location information, each neighbor response its LCA substituting the actual location to the message forwarder. Then, the original requestor computes a globally cloaked area (GCA) and broadcasts it to the neighbors in the cloaking group. The idea to use LCA for protecting location privacy from neighbors is firstly proposed by Hashem [2].

Algorithm 1 Spatial Cloaking.

Require: R_{id}: LBS requestor
Personalized request parameters $k_{\min}$, k_{nor}, $l_{\min}$, l_{nor}, $s_{\min}$, s_{nor} and T
(x, y): x and y represent longitude and latitude of the current position
Ensure: A cloaking region for anonymity requesting
1: Let the hop distance h=0
2: Let the discovered neighbors set $P = \phi$ and the number of discovered neighbors $n = |P| = 0$
3: Let the diversity of locations $d = 0$
4: Computing the LCA of the requestor L_r using the Alg. 2
5: Let the discovered LCAs set $L = L_r$
6: **while** (n $< k_{nor} - 1$ or $d < l_{nor} - 1$ or one of the side length of the cloaking region is less then s_{nor}) and the expended time not exceeds T **do**
7: $h = h + 1$
8: Broadcast a message $(M_{id}, h, type, S_{id})$ with type=FG
9: $A = \{(LCA_i, R_i)\}$ is the set of neighbors that response back to the requestor by executing Alg. 3
10: $L = L \cup \{LCA_i\}$
11: $P = P \cup \{R_i\}$
12: $n = |P|$
13: Set d with the number of different geographic locations of the discovered neighbors
14: Set x_1 with the minimum longitude of the LCAs in L
15: Set y_1 with the minimum latitude of the LCAs in L
16: Set x_2 with the maximum longitude of the LCAs in L
17: Set y_2 with the maximum latitude of the LCAs in L
18: $CR = ((x_1, y_1), (x_2, y_2))$
19: **end while**
20: **if** n $\geq k_{\min} - 1$ and $d \geq l_{\min} - 1$ and any side length of the cloaking region is not less than $s_{\min}$ **then**
21: Propagating CR to the neighbors within the cloaking region with h hops.
22: **else**
23: cloaking failed
24: **end if**

3.2.1 Searching neighbors

Alg. 1 is the pseudo code for searching nearest neighbors. The original requestor r_o wants to get an LBS from the server. It firstly sets the broadcasting hop number $h = 0$, the set of discovered neighbors P to be null, diversity of d to be zero. The original LCA set L is set to be the LCA of r_o, which is computed using Alg. 2. Then, r_o generates a union message sequence number and broadcasts a message for group forming with broadcast hops $h = 1$.

Algorithm 2 LCA Generating.

Require: The position (x,y) of the user
Personalized side length of the LCA
Ensure: A rectangle defined by $((x_{leftButton}, y_{liftButton}), (x_{topRight}, y_{topRight}))$
1: Generate two random numbers, m and n, where $0 \leq m, n \leq c$
2: $x_{leftButton} = x - m$
3: $y_{leftButton} = y - n$
4: $x_{topRight} = x + c - m$
5: $y_{topRight} = y + c - n$

After sending the group forming message, r_o waits for replies from neighbors. Sec. 3.2.3 details the response done by the message receiver. After receiving the response message $R = (M_{id}, A, ACK)$, new discovered neighbors and their LCAs are added into corresponding sets. Meanwhile, cloaking region (CR) is computed based on the received LCAs. The most left button coordinate among LCAs is regarded as the left button coordinate of CR, and the most top right coordinate among LCAs is regarded as the top right coordinate of CR.

While the number of response neighbors is less then $k_{nor} - 1$, or the number of different locations is less then $l_{nor} - 1$, or the CR is not large enough, r_o will broadcast the neighbor searching message again with $h = h + 1$ before timeout. If the loop is terminated for timeout, and the current CR satisfies $k_{\min}$, $l_{\min}$ and $s_{\min}$, CR will be accepted. Otherwise, it means the requestor can't find appropriate CR for LBS requesting. It may try to requiring an appropriate CR after a time.

3.2.2 LCA generating

LCA is firstly used by Hashem et al. [2] to protect location privacy among neighbors. The idea of Alg. 2 is modified from the Alg.1 in [2]. A mobile user assign a number c which represents the side length of LCA. m and n are generated randomly with $0 \leq m \leq c$ and $0 \leq n \leq c$. And the coordinates of left button and top right are computed from the line 2 to 5 in Alg. 2.

3.2.3 Receiver response

Alg. 3 describes the response of a neighbor when it receives a group forming requiring message. If the message ID is duplicate, it just reply with an ACK message. Otherwise, it will act according to the value of h. If h=1, it will just reply an ACK message with its LCA. If h>1, then h is set to be h-1, and the message is rebroadcasted. The sender's pseudonym of the message is replaced with the pseudonym of the forwarder itself. After receiving the responses from its neighbors, the forwarder replies the prior forwarder with its collected LCAs and its own LCA.

4 Conclusion

This paper proposes a decentralized cloaking region creation approach to protecting mobile location privacy. The cloaking region is formed through collaboration

Algorithm 3 Receiver Response.

Require: an FG message $Q_n = (M_{id}, h, FG, S_{id})$
Ensure: $A : \{(LCA_{id}, R_{id})\}$
1: let r be the responser
2: **if** the M_{id} is duplicate **then**
3: Reply the request forwarder with an ACK message
4: Return
5: **end if**
6: Computing the LCA of the requestor L_r using the Alg. 2, and the result is represented by $((x_{leftButton}, y_{liftButton}), (x_{topRight}, y_{topRight}))$
7: **if** h=1 **then**
8: Send the tuple $(M_{id}, (((x_{leftButton}, y_{liftButton}), (x_{topRight}, y_{topRight})), r), ACK)$ back to the S_{id}
9: **else**
10: h=h-1
11: Broadcast a message $(M_{id}, h, type, r)$ with type=FG
12: $A = \{(LCA_i, R_i)\}$ is union of the response set to r
13: $A = A \cup \{(L_r, r)\}$
14: Return (M_{id}, A, ACK)
15: **end if**

among neighbors to hide the precise position. A mobile user can set personalized privacy requirements at different contexts. The system will pursue the privacy requirement on an anticipated level before time out. Otherwise, the system will pursue to satisfy the minimum level of privacy requirement. The approach can satisfy k-anonymity, l-diversity and cloaking granularity simultaneously for privacy protecting.

References

1. Ahamed, S.I., Haque, M.M., Hasan, C.S.: A novel location privacy framework without trusted third party based on location anonymity prediction. SIGAPP Appl. Comput. Rev. 12(1), 24–34 (Apr 2012)
2. Hashem, T., Kulik, L.: "don't trust anyone": Privacy protection for location-based services. Pervasive Mob. Comput. 7(1), 44–59 (Feb 2011)
3. Kim, Y.K., Hossain, A., Hossain, A.A., Chang, J.W.: Hilbert-order based spatial cloaking algorithm in road network. Concurr. Comput. : Pract. Exper. 25(1), 143–158 (Jan 2013)
4. Machanavajjhala, A., Kifer, D., Gehrke, J., Venkitasubramaniam, M.: L-diversity: Privacy beyond k-anonymity. ACM Trans. Knowl. Discov. Data 1(1) (Mar 2007)
5. Mokbel, M.F., Chow, C.Y., Aref, W.G.: The new casper: query processing for location services without compromising privacy. In: Proceedings of the 32nd international conference on Very large data bases. pp. 763–774. VLDB '06, VLDB Endowment (2006)
6. Pan, X., Xu, J., Meng, X.: Protecting location privacy against location-dependent attacks in mobile services. IEEE Trans. on Knowl. and Data Eng. 24(8), 1506–1519 (Aug 2012)
7. Sweeney, L.: k-anonymity: a model for protecting privacy. Int. J. Uncertain. Fuzziness Knowl.-Based Syst. 10(5), 557–570 (Oct 2002)
8. Xu, T., Cai, Y.: Exploring historical location data for anonymity preservation in location-based services. In: The 27th IEEE Conference on Computer Communications (INFOCOM 2008). pp. 1220–1228 (2008)

