International Journal of Combined Research & Development (IJCRD)
eISSN: 2321-225X;pISSN:2321-2241 Volume: 4; Issue: 7; July -2015

Enhancing location privacy and security in Geo-social Networking

Surabhi Lachuriye
Student, M-tech Dept. CSE
GNDEC, Bidar, India.

Rajshekhar Gaithond
Assoc. Professor, Dept. CSE
GNDEC, Bidar, India.

Abstract : Geo-Social Networking is networking dealing with geographic locations. It allows users to interact relative to their current locations. Location is private information and can be used by malicious individuals for blackmail, stalking, and other privacy violations. In this paper, we analyze the problem of location privacy and present a protocol for improving it. We proposed Location to index mapping (LocX) approach that provides strong location privacy while maintaining full accuracy. We propose the idea of coordinate transformation in which secret angle and shift are used by the users to transform all the location coordinates they share with the servers. These secrets are known only to the friends, and therefore only the friends can retrieve and decrypt the data. A secret key cryptographic is used for secured transformation of location data and an Encryption technique AES, is further applied to enhance the security of server. Lastly we compare the performance of LocX with recent k-Anonymity based system. Simulation result shows the effectiveness of our approach with the consideration of several performance metrics.

Keywords: ***Geo SNs*, location privacy, security, location Transformation, efficiency.**

1. INTRODUCTION

ONLINE social networks (OSNs) such as Face book, and Twitter allow people to share personal information and make social connections with friends, co-workers, colleagues, family, and even with strangers. In recent years, we have seen unprecedented growth in the application of OSNs. For example, Face book, one of representative social network sites, claims that it has more than 800 million active users and over 30 billion pieces of content (web links, news stories, blog posts, notes, photo albums, and so on.) shared each month. Within this, Geo-Social Networking is networking dealing with geographic locations. Geosocial networks (GSNs) collect fine grained location information, through check-ins performed by users at visited venues. A variety of services exists and can be envisioned that exploit GeoSN resources. In GeoSN It is possible for exact locations of users to be exposed to untrusted entities that may in turn utilize these to infer sensitive information about the users. For example, the presence of a user in certain locations, e.g., a hospital or a night club, may reveal sensitive information about the user. Location privacy is an important and growing concern in the real world today. Existing systems have taken many approaches to improve user privacy in geo-social systems 1)introducing uncertainity or error in location data, 2) relying on trusted servers or intermediaries to apply anonymization to user identities and private data , and 3) relying on heavy-weight cryptographic or private information retrieval (PIR) techniques. All these techniques fall short to provide strong location privacy as they hurt the accuracy and

timeliness of the responses from the server. Less accuracy makes it unsatisfactory to the users & the application providers are not able to read the data properly and trusted one are easily attacked by others and are costlier to be used on mobiles.

The challenge, then, is to design a method that efficiently protect user privacy while maintaining the accuracy of the system, or making strong assumptions about the security or trustworthiness of the application servers. We focus mainly on Geo-social applications, and assume that servers can be attacked and, therefore, are untrusted. We focus on two main queries necessary to support the functionality of these geo-social applications: point queries and nearest-neighbour (kNN) queries. Points queries query for location data *at* a particular point, whereas kNN queries query for k nearest data *around* a given location coordinate.

2. PROPOSED WORK

In this paper, we propose LocX (location to index mapping), a novel approach that provides an effective solution to a wide range of applications. First in Loc-x the location and data is split into two pairs: a mapping from transformed location to an encrypted index (L2I) and a mapping from index to encrypted location data (I2D). Second untrusted proxies are used to store and retrieve the L2I. This redirection of data via proxies, together with splitting, significantly improves privacy in Loc-x.

2.1 Architecture diagram

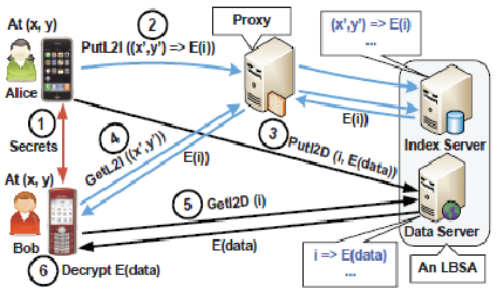

Figure 1: Design of LocX

2.2 privacy in LocX:

To achieve this, Firstly we propose the idea of coordinate transformation. In most of the systems, the real location coordinate and data are stored directly on the server which can be compromised or attacked by malicious users. But in LocX we first transform the real world location(x, y) into transformed location(X, Y) using secret rotation angle (theta) and secret shift (b) as:

$$(X, Y) = (\cos(\text{theta}) \times - \sin(\text{theta}) y + b, \sin(\text{theta}) x + \cos(\text{theta}) y + b)$$

Where, (x, y) are real coordinate of a location and (X, Y) are transformed coordinate of that location.

Secondly, the user generates a random index I using random no. generator and encrypts it with symmetric key and stores on index server via proxy. Then it stores the encrypted location data on data server. In this way privacy is maintained with correctly and securely in LocX.

3. IMPLEMENTATION AND PERFORMANCE EVALUATION

3.1 Protocol Implementation

We implement LocX using Network Simulator tool (NS-2).we used AES with 128 bits key for encryption and decryption and RSA algorithm for key generation. To implement it we placed all the nodes in 800x800 areas. In our experiment we are taking 25 nodes of which 3 nodes proxy server node, index server and data server nodes represent security infrastructure. When source wants to communicate with destination these nodes are responsible for handling security of data and location privacy.

3.2 Simulation Environment

In order to evaluate the performance of the proposed protocol LocX, we compare it with recent k-anonymity based system using the NS-2 simulator. K-anonymity based system is a trusted third-party anonymizer that stands between the clients and servers to anonymize queries and to filter query responses. The anonymizer knows the user Id and the user's friends' information in order to filter responses. Simulation parameters are as follows: The Distributed Coordination Function (DCF) of the IEEE 802.11 protocol is used as the

MAC layer protocol. The radio channel model follows a Lucent's Wave LAN with a bit rate of 2 Mbps, and the transmission range is 250 meters. We consider constant bit rate (CBR) data traffic and randomly choose different source destination connections. Every source sends four CBR packets whose size is 512 bytes per second. In order to reflect the network mobility, we set the max-speed to 5 m/s and set the pause time to 0. The Max Delay used to determine the rebroadcast delay is set to 0.01 s and the simulation time for each simulation scenario is set to 300 seconds. The detailed simulation parameters are shown in Table 1.

TABLE 1
Simulation parameters

Simulation Parameter	Value
Simulator	NS-2
Topology size	800m*800m
Number of Nodes	25
Transmission Range	250m
Bandwidth	2Mbps
Interface queue length	50
Traffic Type	CBR
Packet Size	512 bytes
Packet Rate	4 Packet/sec
Pause Time	0s
Min Speed	1 m/s
Max Speed	5 m/d

3.3 Performance Evaluation

To show the performance of LocX we compare it with a recent k-anonymity based system. We plotted a graph of Average delay with varied no. of nodes. Figure shows that the Average delay for our proposed Locx is much lesser than k-anonymity based system.

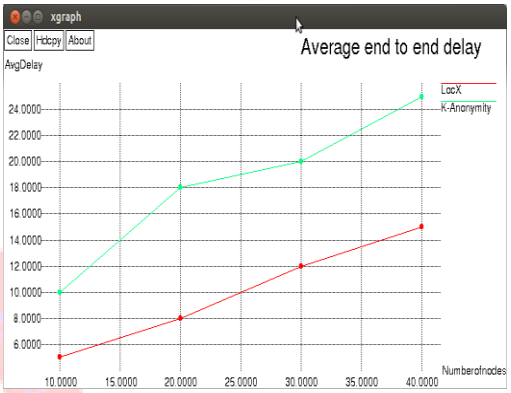

Fig 2: Average delay vs. varied no. of nodes

Next, we plotted a graph of packet delivery ratio with varied no. of nodes. The graph in fig 3 shows that packet delivery ratio of Locx is more than k-anonymity based system.

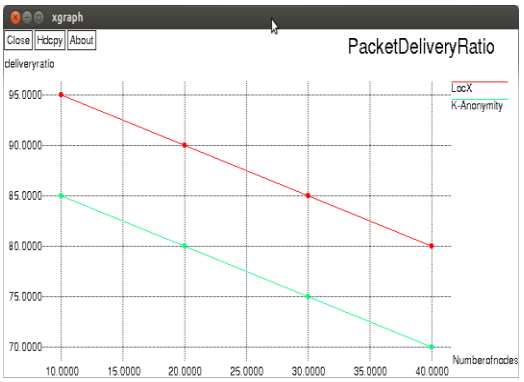

Fig 3: packet delivery ratio vs. varied no. of nodes

4 CONCLUSION

Location privacy is of utmost concern for location-based services. It is the property that a person's location is revealed to other entities, such as a service provider or the person's friends, only if this release is strictly necessary and authorized by the person. We introduce LocX that provide strong location privacy for such a service. In LocX, users efficiently *transform* all their locations shared with the server and encrypt all location data stored on the server using inexpensive symmetric keys. The transformation is *secure*, in that transformed values cannot be easily associated with real world locations without a *secret*. The Implementation of LocX using Cryptographic and the encryption technique contribute to the concrete implementation for providing strong location Privacy. Finally we use prototype measurements to show that it provides privacy with very little performance overhead, making it suitable for today's mobile devices.

5. ACKNOWLEDGMENTS

I would like to express my deep gratitude to my Project coordinator Mr. Dhananjay. M, Head, CSE for enthusiastic encouragement and continuous support. I extend my thanks to my Project Guide Mr. Rajshekhar Gaithond, Assoc.Professor, CSE for his patient guidance and unending support right from the stage the idea was conceived. My grateful thanks are also extended to the Management, Guru Nanak Dev Engineering College for their continuous encouragement. Finally I wish to thank my family and my friends for their support throughout my study.

6. REFERENCES

[1] B. Schilit, J. Hong, and M. Gruteser, "Wireless location privacy protection," *Computer*, vol. 36, no. 12, pp. 135–137, 2003.

[2] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in *Proc. of Mobisys*, 2003.

[3] M. Hendrickson, "The state of location-based social networking," 2008.

[4] B. Gedik and L. Liu, "Location privacy in mobile systems: A personalized anonymization model," in *Proc. of ICDCS*, 2005.

[5] T. Jiang, H. J. Wang, and Y.-C. Hu, "Preserving location privacy in wireless lans," in *Proc. of MobiSys*, 2007.

[6] A. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg, and D. Boneh, "Location privacy via private proximity testing," in *Proc. of NDSS*, 2011.

[7] G. Zhong, I. Goldberg, and U. Hengartner, "Louis, lester and pierre: Three protocols for location privacy," in *Proc. of PET*, 2007.

[8] S. Mascetti, C. Bettini, D. Freni, X. S. Wang, and S. Jajodia, "Privacyaware proximity based services," in *Proc. of MDM*, 2009.

[9] A. Khoshgozaran and C. Shahabi, "Blind evaluation of nearest neighbor queries using space transformation to preserve location privacy," in *Proc. of SSTD*, 2007.

[10] G. Ghinita, P. Kalnis, and S. Skiadopoulos, "Prive: anonymous location based queries in distributed mobile systems," in *Proc. of WWW*, 2007.

[11] P. Golle and K. Partridge, "On the anonymity of home/work location pairs," in *Proc. of Pervasive Computing*, 2009.

[12] B. Hoh *et al.*, "Preserving privacy in gps traces via uncertainty-aware path cloaking," in *Proc. of CCS*, 2007.

[13] J. Krumm, "Inference attacks on location tracks," in *Proc. of Pervasive Computing*, 2007.

[14] A. Beresford and F. Stajano, "Mix zones: User privacy in location-aware services," in *Proc. of Pervasive Computing*, 2004.

[15] D. Lin, E. Bertino, R. Cheng, and S. Prabhakar, "Position transformation: a location privacy protection method for moving objects," in *Proc. Of Security and Privacy in GIS and LBS*, 2008.