International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Survey Paper on User's Location Hiding In Geosocial Recommendation Applications

Mayura Phadnis [1], Kanchan Varpe [2]

[1, 2] Rajarshi Shahu College of Engineering and Research, JSPM Narhe, Technical Campus, Pune-India

Abstract: ***FourSquare is one of the Geosocial application in which lots of communities interrelate with their surrounding environment through their friends and their recommendations. Regarding the security issues Geosocial application can simply misused, for instance to trace the user or target them for home invasions. Therefore providing the privacy to the Geosocial application is the research issue, existing system provides location privacy without adding uncertainty into the query results or relying on strong assumptions about server security. In existing systems the user send message to the another user is of bigger size, therefore the expenses of the server database is increases on existing system. Therefore in the proposed system which provides the security to the user's location as well as uses compression algorithm to compress and decompress the message so that that the message retrieval time will be lesser than the previous system . By using our proposed system cost of the server database will decrease and the time required for transmitting the message is also decreases. The system encrypts the message for the security purpose. The proposed method provides privacy and improves the performance of the Geosocial application. The proposed system also uses keyed tags and random tags which balance the privacy and performance of the system. The keyed tag provides strong privacy and random tags provide privacy and high efficiency to the system.***

Keywords: Location privacy, Security, Location-based services, Geosocial applications, location transformation, efficiency.

1. Introduction

Geo-social networks (GeoSNs) provide a context-aware service that helps to associate location with users and content. The proliferation of GeoSNs indicates that they're rapidly attracting users. GeoSNs currently offer different types of services, including photo sharing, friend tracking, and "check-ins." However, this ability to reveal users locations causes new privacy threats, which in turn call for new privacy-protection methods. The authors study four privacy aspects central to these social networks - location, absence, co-location, and identity privacy - and describe possible means of protecting privacy in these circumstances.

In today's world, Smartphone applications have become popular among the users enhancing computing platform. A type of application is coming into line light that can be put under the category of geosocial application. Examples of this social application are local friend recommendation for dining and shopping, as well as games and collaborative network services. But, it has been noticed that these application prove disadvantages as there is a risk of losing users privacy, at present due to minimal privacy mechanism. User's all know about the "places" feature of facebook which was misused by some thieves. Hence, there is a real need for stronger privacy properties in order to make it more-friendly to the users.

Now a days, Geosocial application have become part and parcel of human lives. But, these may be misused by someone to extract user's personal information. LocX tends to provide with improved privacy and with result quite certain. The primary thing that is done is to use secure coordinate transformation. This transformation would be used only by friends of a particular user. It allows the server to work properly and correctly without accessing the private data of the user. There are users where there is not a need for arbitrary pairs of users to be resolved. Hence, by distinguishing such location data through users social groups and further transformation can be used on location coordination. The coordinate transformations preserve distance metrics, enhancing the task of server to perform queries on transformed data. The transformation is a safe one, since the key is secret which knows only to the users group.

The proposed system uses the compression technique. LZW compression algorithm is used for compression. LZW compression is fast and simple to apply. Since this is a lossless compression technique, none of the contents in the file are lost during or after compression. Sender first sends GPS location.Like the LocX technique use transforms the co-ordinates and save those on to the index sever .The compression method is used the compress the file and then apply the encryption. This technique has advantages of being able to send large files to the mobile devices which has less memory than the naormal computers The system in which the compression technique is used while user send the message to the another ussize so the er initially user encrypt the message by the encryption algorithm and after that compress the message and send to another user. Additionally user adds key hash and random hash tags for improving the privacy and performance of the system. Key hash is significantly more efficient than no tags in terms of processing time on the user's device, while providing the same, strong privacy. The random hash provides both high privacy and high efficiency.

2. Literature Survey

B. Gedik and L. Liu describes [4] a personalized k-anonymity model for protecting location privacy against various privacy threats through location information sharing. Model has two unique features. First, it provides a unified privacy personalization framework to support location k-anonymity for a wide range of users with context sensitive personalized privacy requirements. This framework enables each mobile node to specify the minimum level of

anonymity it desires as well as the maximum temporal and spatial resolutions it is willing to tolerate when requesting for k-anonymity preserving location-based services (LBSs). Second, it devises an efficient message perturbation engine which runs by the location protection broker on a trusted server and performs location anonymization on mobile users' LBS request messages, such as identity removal and spatio-temporal cloaking of location information

P. Kalnis, G .Ghinita, K. Mouratidis, and D. Papadias [7] developed methods for protecting the privacy of users issuing spatial queries against location-based attacks. Specifically, prevent an attacker from inferring the identity of the query source by adapting the well-established K-anonymity technique to the spatial domain. When the user wants to find some information using location based service (LBS) without disclosing his information. The user uses a anonymizer, a trusted server .He establishes the secure connection with anonymizer. Anonymizer removes the ID of the user and transforms his location through a technique called cloaking. Cloaking hides the actual location by a K-anonymizing spatial region (K-ASR or ASR), which is an area that encloses the client that issued the query, and at least K-1 other users. The anonymizer then sends the ASR to the LBS, which returns to the anonymizer a set of candidate results that satisfy the query condition for any possible point in the ASR. Asking the same query from successive locations may disclose the identity of the querying user, who will be included in all ASRs.

T. Jiang, H.J. Wang, and Y.-C.Hu[6] states the three sources of leakage of information in a wireless networks are defined as time, location and sender node identity. System analyzes the achieved location privacy of a mobile node using the metric of privacy entropy. To obfuscate the transmission time, system introduces the opportunistic silent period, which takes place during the idle time between user's communication sessions. To prevent an attacker from using user identity for tracking, users must use frequently changing pseudonyms for communications. To prevent an attacker from using user identity for tracking, users must use frequently changing pseudonyms for communications. In an 802.11 WLAN, MAC and IP addresses are user identities that must be protected by using pseudonyms. This privacy-enabled systems sacrifice service quality. Users in privacy mode will have their communications delayed if they communicate before a silent period ends.

G. Ghinita, P. Kalnis, and S. Skiadopoulo[8] proposes Prive, a distributed architecture for anonymous location-based queries, which addresses the problems of existing systems. (i) Develop a superior K-ASR construction mechanism that guarantees query anonymity even if the attacker knows the locations of all users. (ii) Introduce a distributed protocol used by mobile entities to self-organize into a fault-tolerant overlay network. In Prive, K-ASRs are built in a decentralized fashion, therefore the bottleneck of the centralized server is avoided. Since the state of the system is distributed, Prive is resilient to attacks. This approach hurts the accuracy and timeliness of the responses from the Server.

B.Hoh et al.[9] addresses the challenge of providing strong privacy guarantees while maintaining high data accuracy of time-series location data. Specifically, the key contributions of this work are:
1. Introduction of a novel time-to-confusion metric to evaluate privacy in a set of location traces.
2. Development of an uncertainty-aware privacy algorithm that can guarantee a specified maximum time-to-confusion.

S.Papadopoulos, S.Bakiras, and D.Papadias[15] proposes methods for arbitrary kNN search with strong location privacy. There are two main components in the proposed scheme: (i) the PIR functionality, and (ii) the query plan. The former ensures that the LBS is oblivious of each block retrieved by the algorithms. System employs secure hardware PIR, which is the only practical choice for PIR in databases of non-negligible size. In particular, this mechanism offers private block retrievals with constant communication cost and amortized polylogarithmic computational cost. The query plan ensures that every query retrieves the same number of blocks during its execution. A trivial solution would enforce each query to retrieve a fixed and arbitrarily large number of blocks. Its performance, although improved by using special hardware , but it is still much worse than all the other approaches. Thus it is unclear at present if this approach can be applied in real LBSs.

3. Problem Definition

Due to the advancement in mobile technology, multiple geosocial applications are developed to provide the facilities for the mobile users. Users can share their reviews and recommendation through this new class of applications. But it requires continuous sensing of the users location through GPS which creates new threats for the users sensitive location information. The location information can be used for malicious purposes. This threat creates the need to hide the user's location from the outside world. Location Privacy can be achieved by separating the location information and the data. The query performance of the existing system is depend on varying put message sizes of the system. storing them on different servers. As location puts per client increases, the total data size increases, thus more data needs to be processed and the sizes of query answers increase. The recommendations from users can be saved and accessed in efficient manner irrespective of the message size.

4. Proposed System

In the system the user who wants to share some information about any location retrieves the co ordinates (x,y) of that location from the GPS system. Then by using the secret rotation angle and shift , he will transform those co-ordinates say (x', y'). A random number generator is used to generate the index and is encrypted with the secret key .All the secret information is conveyed to the user's social group by using some secure media like e-mail or telephonic conversation.

Then the transformed co–ordinates along with the encrypted index will be saved on to the index server. The data corresponding to this location is encrypted with the secret key .This data is again compressed with the help of the

compression algorithm for the efficient retrieval of the information from the data sever.

There are multiple reviews present for the same location whether from user's social group or from the unknown users, To distinguish between these two groups we can use the hash code. So the index server contains the one more field for the hash code which can be checked by the user 's friend to retrieve the actual review from his social group.

To resolve the name conflicts i.e same names for the different places the system uses special tags.

To improve the performance of review retrieval from the data server we can use the compression mechanism which compresses the reviews and stores it to the data sever.

When user's friend wants to access the reviews for the specified location again he transforms the co-ordinates and sends the query to the index server. Then he retrieves the index by using secrete key .After retrieving the index a separate query will be fired on to the data server to fetch the review. The review will first decompressed and then decrypted with the same secrete key.

In this way the recommendations can be securely communicated with in the user 's social circle without exposing his location to the outside world.

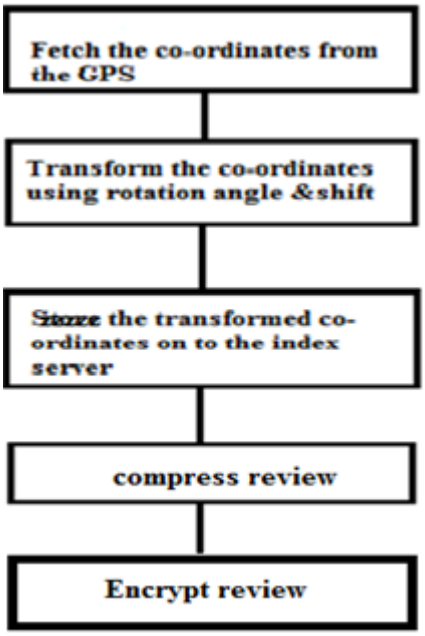

Figure 1: Overview of system operations

System uses following algorithms in our system:

1. Data Compression algorithm
The user data stored in databases might generate bigger sized files. Thus, the Data Compression algorithm is used to compress the generated data. The user will get these compressed files from the database.

2. Data Decompression algorithm
The files that user will get from the database will be in compressed form, as stated above. Therefore, a decompression algorithm is necessary.

3. AES Encryption algorithm
We are using the AES Encryption algorithm, instead of any other, is because of the security that it provides. Here, the user location information will be encrypted before it is sent to the server for storage purpose. Therefore, even if the attacker gets this information somehow, it won't be able to access it.

4. AES Decryption algorithm
The decryption algorithm is used to for decrypting the user location data, when the actual data will be necessary for the processing.

5. Conclusion

In this paper we discussed about providing the security, privacy and increasing the performance of the location-based social network system. Proposed work designed a security and privacy aware protocol for the system and recognized its completeness and correctness. We used the compression technique and search by tag the technique to increase a per-formance of Geosocial application. Existing system takes timefor transmitting the dataor information to the server and also the for getting the correct data. It take more time to transmit the message because the size of the message is large, which degrades the performance of the existing system. The proposed system overcomes the drawback of the LocX system and improves the performance of the system by using
the compression techniques.

References

[1] B. Schilit, J. Hong, and M. Gruteser, Wireless Location Privacy Protection, Computer, vol. 36, no. 12, pp. 135-137, Dec. 2003.
[2] M. Gruteser and D. Grunwald, Anonymous Usage of Location-Based Services through Spatial and Temporal Cloaking, Proc.First Intl Conf. Mobile Systems, Applications Services, 2003
[3] M. Motani, V. Srinivasan, and P.S. Nuggehalli, PeopleNet:Engineering a WirelessVirtual Social Network, Proc. ACM MobiCom, 2005
[4] B. Gedik and L. Liu, Location Privacy in Mobile Systems:A Personalized Anonymization Model, Proc. IEEE 25th Intl Conf.Distributed Computing Systems,2005.
[5] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, Enhancing Security and Privacy in Traffic-Monitoring Systems, IEEE Pervasive Computing Magazine, vol. 5, no. 4,pp. 38-46, Oct. 2006.
[6] T. Jiang, H.J. Wang, and Y.-C. Hu, Preserving Location Privacy in Wireless Lans, Proc. Fifth Intl Conf. Mobile Systems, Applications Services, 2007.
[7] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, Preventing Location-Based Identity Inference in Anonymous Spatial Queries, IEEE Trans. Knowledge Data Eng., vol. 19, no. 12,pp. 1719-1733, Dec. 2007.
[8] G. Ghinita, P. Kalnis, and S. Skiadopoulos, PRIVE: Anonymous Location Based Queries in Distributed

Mobile Systems, Proc. 16th Intl Conf. World Wide Web, 2007
[9] B. Hoh et al., Preserving Privacy in GPS Traces via Uncertainty Aware Path Cloaking, Proc. 14th ACM Conf. Computer Comm.Security, 2007.
[10] G. Ananthanarayanan, V.N. Padmanabhan, L. Ravindranath, and C.A. Thekkath,Combine: Leveraging the Power of Wireless Peers through Collaborative Downloading, Proc. Fifth Intl Conf.Mobile Systems, Applications Services, 2007.
[11] P. Mohan, V.N. Padmanabhan, and R. Ramjee, Nericell: Rich Monitoring of Road and Traffic Conditions Using Mobile Smartphones, Proc. Sixth ACM Conf. Embedded Network Sensor Systems, 2008
[12] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan,Private Queries in Location Based Services: Anonymizers Are Not Necessary, Proc. ACM SIGMOD Intl Conf. Management Data,2008.
[13] J. Manweiler, R. Scudellari, and L.P. Cox, SMILE: Encounter Based Trust for Mobile Social Services, Proc. 16th ACM Conf.Computer Comm. Security (CCS 09), 2009.
[14] K.P.N. Puttaswamy, R. Bhagwan, and V.N. Padmanabhan,Anonygator: Anonymity and Integrity Preserving Data Aggregation, Proc. ACM/IFIP/USENIX 11th Intl Conf. Middleware(Middleware 10), 2010
[15] S. Papadopoulos, S. Bakiras, and D. Papadias, Nearest Neighbor Search with Strong Location Privacy, Proc. VLDB Endowment,vol. 3, nos. 1/2, pp. 619-629, Sept. 2010
[16] T. Isdal, M. Piatek, A. Krishnamurthy, and T. Anderson, Privacy Preserving P2P Data Sharing with Oneswarm, Proc. ACMSIG COMM, 2010.
[17] P. Gill et al., DudeWheres that IP? Circumventing Measurement Based IP Geolocation, Proc. 19th USENIX Conf. Security, p. 16,2010
[18] H. Hu, J. Xu, C. Ren, and B. Choi, Processing Private Queries over Untrusted Data Cloud through Privacy Homomorphism,Proc. IEEE 27th Intl Conf. Data Eng. (ICDE), 2011.
[19] A. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg, and D.Boneh, Location User's Location Hiding In Geosocial Recommendation Applications. Privacy via Private Proximity Testing, Proc.Network Distributed System Security Conf., 2011.