ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

Dynamic Smart Grid System for Enhancing User Privacy Location-Based Services

Yasotha R [1], Selvaraj A [2]

PG Student, Dept. of C.S.E, Muthayammal Engineering College, Rasipuram, Tamilnadu, India

Assistant Professor, Dept. of C.S.E, Muthayammal Engineering College, Rasipuram, Tamilnadu, India

ABSTRACT: Suitable to the good looks of mobile devices location-based services have become extra common in recent years. Though, users have to reveal their location information to access location-based services with existing service infrastructures.Location-Based Services (LBS) require users to continuously report their location to service provider to obtain services based on their location. It is possible that adversaries could collect the location information, which in turn invades user's privacy. There are existing solutions for query processing and user defined grid system on mobile networks and mobile user privacy protection. However there is no solution for solving queries on mobile networks with privacy protection. Therefore, we aim to provide network distance mobile query solutions which can preserve user privacy by utilizing mechanisms. We recommend a dynamic smart grid system, our system can be easily complete to maintain other mobile queries, provided the required search area of a mobile query can be abstracted into mobile regions.Smart grid retrieves the location accurately and enables communication.

KEYWORDS: Smart grid system, location privacy, location based services, cryptography

I. INTRODUCTION

In today's world of mobility and ever present internet connectivity, an increasing number of people use Location-Based Services(LBS) to request information relevant to their current locations from a variety of Service Providers(SP).This can be the search for nearby points of interest, location aware advertising by companies, traffic information tailored to the highway and direction a user is traveling and so forth. The use of LBS, however, can reveal much more about a person to potentially untrustworthy service providers than many people would be willing to disclose. By tracking the requests of a person it is possible to build a movement profile which can reveal information about a user's work, medical records, political view, etc. Nevertheless, LBS can be very valuable and as such usersshould be able to make use of them without having to give up their location privacy.

II. RELATED WORK

Location-Based Services(LBS) require users to continuously report their location to a potentially untrusted server to obtain services based on their location, which can expose them to privacy risks and offering limited privacy guarantees and incurring high communication overhead [1].To generate the minimum cloaking region efficiently make use of a grid structure for storing buildings and users as well as a pruning technique for reducing unnecessary computation. Location-Based Service users send location-based queries to servers along with their exact locations, but the location information of the users can be misused by adversaries. A mechanism to deal with the userspsila privacy protection is required [2].Continued advances in mobile networks and positioning technologies have created a strong market push for location-based applications. Examples include location-aware emergency response, location-based advertisement and location-based entertainment. An important challenge in the wide employment of location-based services is the privacy-aware management of location information, providing safeguards for location privacy of mobile clients against vulnerabilities for abuse, the effectiveness of our location cloaking algorithms under various conditions by using realistic location data that is synthetically generated from real road maps and traffic volume data.The concept of K-anonymitywas originally introduced in the context of relational data privacy. It addresses the how a data holder can release its private data with guarantees that the individual subjects of the data cannot be identified whereas the data remain practically useful [3]. The increasing trend of embedding positioning capabilities (for example GPS) in mobile devices facilitates the widespread use of Location-based services. For such applications to succeed privacy and confidentiality are

DOI: 10.15680/IJIRCCE.2016. 0402182

essential the well-established K-anonymity concept to compute exact answers for range and nearest neighbour search, without revealing the query source. A method optimizes the entire process of anonymizing the requests and processing the transformed spatial queries.The LBS maintains the locations of points of interest and answers cloaked queries. The most common spatial queries are ranges and NNs [4].Traffic monitoring using probe vehicles with gps receiver's promises significant improvements in cost, coverage, and accuracy over dedicated infrastructure systems. However, raise privacy concerns because they require participants to reveal their positions to an external traffic monitoring server. Virtual trip lines which are geographic markers that indicate where vehicles should provide speed updates. These markers are placed to avoid specific privacy sensitive locations. It also allows aggregating and cloaking several location updates based on trip line identifiers, without knowing the actual geographic locations of these trip lines. The design of a distributed architecture, in which no single entity has a complete knowledge of probe identities and fine-grained location information.A virtual trip line is a line segment in geographic space that, when crossed, triggers a client's location update to the traffic monitoring server [5].

A population of objects moves continuously in the Euclidean plane. The position of each object, modelled as a linear function from time to points, is assumed known. It may exploit any existing index for the current and near-future positions of moving objects, the Bx-tree is used to extensive empirical study, which elicits the performance properties of the algorithm [6]. Location privacy based on k-anonymity addresses this threat by cloaking the person's location such that there is at least k - 1 other people within the cloaked area and by revealing only the cloaked area to a location-based service. A central server that knows everybody's location determine the cloaked area and the server needs to be trusted by all users and is a single point of failure. It has users jointly determine the cloaked area [7].A framework for supporting anonymous location-based queries in mobile information delivery systems. Quad grid cloaking algorithm is fast but has lower anonymization success rate. The dynamic bottom-up or top-down grid cloaking algorithms provide much higher anonymization success rate and yet are efficient in terms of both time complexity and maintenance cost.The privacy grid approach can provide optimal location anonymity as defined by per user location p3p without introducing significant performance penalties [8]. Advances in sensing and tracking technology enable location-based applications but they also create significant privacy risks. Anonymity can provide a high degree of privacy, save service users from dealing with service providers privacy policies, and reduce the service provider's requirements for safeguarding private information. Location-based requests for urban areas would have the same accuracy currently needed for services, this would provide sufficient resolution for way finding, automated bus routing services and similar location-dependent services [9]. Protecting privacy of mobile users of location-based services is a currently interesting research problem. Most protection techniques can be categorized into either those providing location privacy or those guaranteeing k-anonymity. Anon Twist contains two technical contributions. The first is a user density map in the form of a Quad tree so that we have an estimate of the number of users in each spatial area. The second is a nontrivial counting mechanism, over the density map, to keep track of the number of users in the twisted space [10].

III. PROPOSED ALGORITHM

A dynamic smart-grid system represented in Fig.1 to provide privacy-preserving and continuous LBS. All users need to continuously update their locations with the location analysing, even when they are not subscribed to any LBS. The mobile user can continuously update their location to the service provider. The dynamic smart-grid system which allows users to express their privacy requirements in terms of location find and measures to out of range query distances and analysis the overhead of query processing. It provides more security to user location details and Low communication cost of Dynamic Smart-Grid System (DSGS) for the user does not depend on the user-specified query area size. The grid cells overlapping with a query have required search area.Multiple users can access at a time and security can be provided dynamically to the mobile users.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

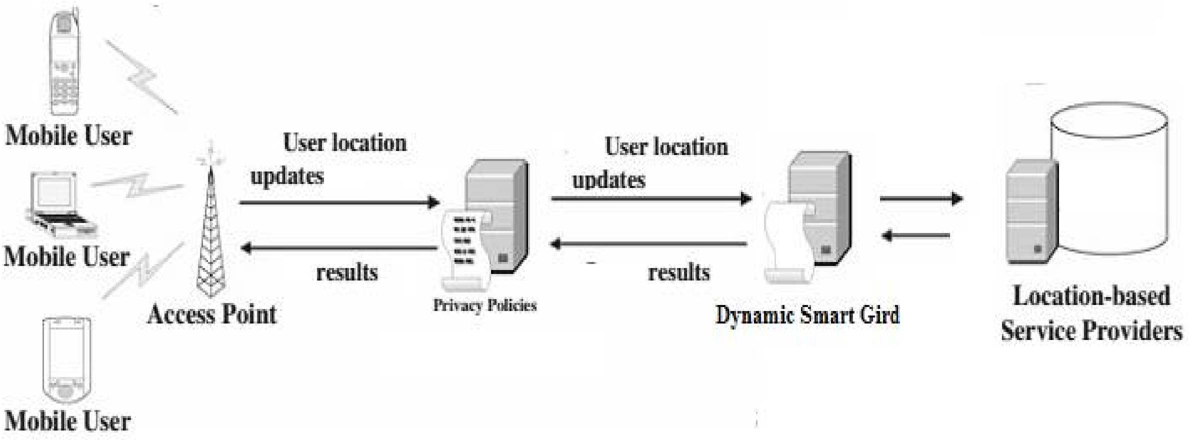


Fig.1 System Architecture

Description of proposed algorithm

Smart gridtechnologies have enabled many utilities to provide that reliable power with an aging transmission and distribution infrastructure, even during periods of peak demand. Powerful communication technology is a key to ensuring effective grid operations. Smart grid communications infrastructure must be not only flexible and reliable, but also capable of intelligent command and control. In addition, it must be able to capture data and leverage intelligence of the network. Utility operators, therefore, should enlist solutions that are cost-effective and minimally invasive, while being sophisticated enough to handle a dynamic distributed power environment.

A smart grid is designed to route electricity from the generation source to the consumer in the most efficient way possible. The distribution network must enable reliable and secure command and control, monitoring of transformers, substations, capacitor banks and moreintelligent control over power grid functions to the distribution level and beyond. In addition, the communication infrastructure should allow the utility to monitor and control load shifting. Wireless IIOT and M2M communications technologies can improve data transmission and process control, as well as help establish intelligent control of processes that were traditionally manual. For example, with advanced communication technology, reclose control can be re-routed across the grid to bypass problem areas and ensure efficient operations.

IV. SYSTEM ORGANIZATION

A. Grid System Allocation

Our modules allocating the processes of grid system, for enhancing the mobile user interact with grid system of the mobile network. The all grid system interconnects with all user locations.

B. Two Grid Allocating System

To make a dynamic smart-grid structure specified by the user. A querying user first specifies a query area, where the user is comfortable to reveal the fact that is located somewhere within that query area. Then processing for defined the two more users locations areas.

C. Distance Calculation

The mobile user requests and check the user request is contain calculate the range Distance value, and then send response to the appropriate values, suppose the request doesn’t contain means send response is Record Not Found‟ that message sent to the particular user.

D. Security Enhancement For Users

The user need privacy based location service, so user privacy has been hacked there. The user not securely maintaining our location information. So we are enhancing new privacy process for each and every user.

DOI: 10.15680/IJIRCCE.2016. 0402182

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

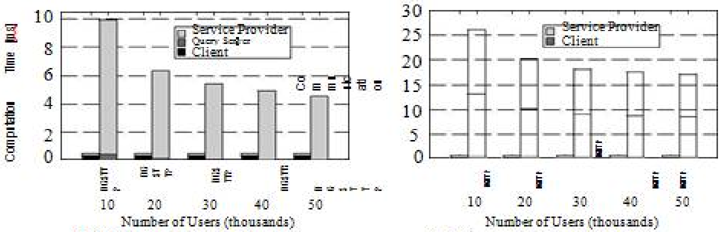
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

V. SIMULATION AND RESULTS

The scalability of DSGS with respect to varying the number of mobile users from 10,000 to 50,000.The results show that DSGS is independent of the number of users and has the desirable privacy feature for privacy preserving location-based services which is free from privacy attacks based on the user distribution.The performance of DGS for continuous NN queries and computation time remains constant. For cloaked area computed by TTP becomes smaller with more users. DSGS is slightly less expensive than TTP in terms of computation cost represented in Fig.2.



(a) Computation Cost (b) Communication Cost

Fig.2. Number of mobile users

VI. CONCLUSION AND FUTURE WORK

Proposed a Dynamic Smart-Grid System (DSGS) for providing privacy-preserving continuous location-based services. Proposed system for private information retrieval that achieves a good compromise between user location privacy and computational efficiency. Allowing the user to have complete flexible control over their privacy and their system, it consider that this trade-off is very reasonable, given that the processing power of today's smartphone's is still less of a concern than the speed and cost of wireless network connectivity.

As a future work, need to study on mobile user security needs to improve that work for future enhancements of service provider and more efficient grid system to improve the mobile network system.

REFERENCES

[1] Schlegel, R., Chi-Yin Chow; Qiong Huang; Wong, D.S.,"user-defined privacy grid system for continuous location- based services,"IEEE Transaction on volume: 14, Issue: 10, 2015
[2] Jungho Um, Hyeongil Kim; Youngho Choi;Jaewoo Chang,"A New Grid-Based Cloaking Algorithm for Privacy Protection in Location-Based Services in IEEE, 2009
[3]B. Gedik and L. Liu, "Protecting location privacy with personalized k anonymity: Architecture and algorithms,"IEEE TMC, vol. 7, no. 1, pp. 1–18, 2008
[4] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, "Preventing location-based identity inference inanonymous spatial queries," IEEE TKDE, vol. 19, no. 12, pp. 1719–1733, 2007
[5] B Hoh, T.Iwuchukwu, Jacobson, D.Work, A.M. Bayen, R. Herring, J.C.Herrera, M.Gruteser, M.Annavaram,J.Ban, "Enhancing Privacy and Accuracy in Probe Vehicle-Based Traffic Monitoring via Virtual Trip Lines," IEEE TMC, vol.11, no.5.pp.849-864, 2012
[6] C.S.Jensen, D.Lin,B.C.Ooi;R.Zhang,"Effective Density Queries on Continuously Moving Objects", IEEE ICDE 2006
[7]G. Zhong and U. Hengartner, "A distributed k-anonymity protocol for location privacy," in IEEE PerCom, 2009
[8] B. Bamba, L. Liu, P. Pesti, and T. Wang, "Supporting anonymous location queries in mobile environments with Privacy Grid," in WWW, 2008
[9] M.Gruteser and D.Grunwald,"Anonymous Usage of Location-Based Services through Spatial and TemporalCloaking," in ACM MobiSys, 2003
[10] S. Wang and X. S. Wang, "AnonTwist: Nearest neighbor querying with both location privacy and k-anonymity for mobile users," in MDM, 2009