INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

A SURVEY ON LOCATION BASED PRIVACY PRESERVING FRAMEWORK FOR PARTICIPATORY SENSING

C Chandrasekhar Reddy[1], Mr. K Suresh Babu[2]

[1]M Tech- Computer networks information security, cchandumtech@gmail.com
[2] Assistant professor in cse, kare_suresh@yahoo.co.in
School of information technology, JNTU Hyderabad, India

Abstract

There is wide range of use cheap embedded sensors on mobile devices like cameras, microphones, Wi-Fi adapters, accelerometers, Bluetooth and so on. In the participatory sensing with these embedded sensors we have a threat in communication while participatory sensing can be used by the individual and communities greatly. When we are collecting and analysing the locations of participators, we have various threats in aspects of privacy. And the existing proposals are mainly focused on providing privacy for participators locations. But there is no chance in protecting the trajectory data. And very few are done in the aspect of protecting trajectory data. I am proposing the effective analysis on trajectories that having special temporal history information can reveal the participators locations and the relevant personal privacy.

Keywords*:* Trajectory, Privacy, Framework, Sensors, Participators and information.

1. Introduction

In now a day, there is an emerging computing paradigm that is called participatory sensing which enables the collection of data by selected participants, selected by themselves. The participatory sensing mainly used by number of mobile users to share their local information to other system. This can allows the users to identify , measure using mobile systems with basic sensors like global positioning system(GPS), cameras, text messaging . The participatory sensing uses the development of wireless technologies like WiMAX, 3G/LTE, Zig bee, Wi-Fi networks, WLAN, Bluetooth's and so on. These sensors are equipped with a variety of powerful embedded sensors. Storage and processing capabilities which enables participatory sensing to emerge as a new powerful technology. While research initiatives and prototypes , participatory sensing's real-world impact is often bounded to comprehensive user participation. If users have nothing incentive, or feel that their privacy might be in danger, it is likely that they will not participate.

1.1 Location privacy

It is a particular type of information privacy. This can be defined as the ability to avoid or prevent other unauthorised parties knowing ones present or past location information. There are many technologies that can find the location of individual persons. And GPS is the earliest technology used for tracking the location. This technology can uses the satellite services to help the devices to determine their location. Mostly cars can use this service. This Global positioning system is widely deployed across the world especially in map applications. GPS is mostly integrated into PDAs and other devices which will do. If a attack is successfully done on a victim then somebody will get unauthorised information. Individuals intend that some information about themselves should be available to others, and that the rest remain private. The means by which the individual's preferences were circumvented is the attack vector. The main privacy concern with regards to ubiquitous

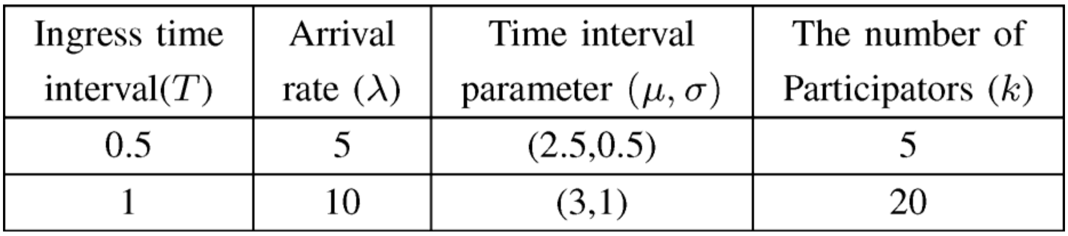
computing is that many new automated attack vectors become possible. Negligibly organized, automated digital devices will get information either through communication, observation, or inference.

1.2 Trajectory privacy:

Trajectory is the path in which the object or information flows to the destination from source in the function of time. The participatory sensing mainly depends on the group of data from different areas. The data collected from sensors will be tagged with special temporal information of participators when the readings were recorded the trajectories which are published for decision making criteria. For example merchants can decide where the supermarket can be placed by following the trajectories of customers. And the inspector of vehicles can know where to check the vehicles by observing the trajectories of vehicles. But it may tends to serious threats to participators privacy. It may possibly analyze the trajectories which contain good spatial-temporal history information to link multiple reports from the same participators and determine certain private information such as the locations where the data reports are collected. So it is necessary to cut the link between participators' identities from sensitive data collection locations. One of the methods to ensure trajectory privacy is the Mix Zones.

2. Related work:

There are some existing systems that used to protect participators locations. Some are used to hide some unwanted information like personal information, identity data. In some cases we cant stop sending data to different destinations as it is much important. So it causes some problems. Unexpected personal problems may be the result. To avoid this the participators may ask to treat their information confidentially. In this automated database world, researchers developed some schemes. These may enable privacy protection.



Ingress time interval(T)	Arrival rate (λ)	Time interval parameter (μ, σ)	The number of Participators (k)
0.5	5	(2.5,0.5)	5
1	10	(3,1)	20

a. ANODR:

It's a routing protocol that points about the anonymity in routing and location privacy. The main focus is that the pocket cannot be traced in the network by observing adversary. And their routing schemes benefits to cut the link. Before sending some packets, the route must be established between sender and receiver through route discovery. This can be achieved by broadcasting packets. Here the sender is anonymous because we can't judge it is sending or just forwarding a packet.

b. Obfuscation:

Obfuscation is a class of very important approaches in the location privacy. And it can protect participators location privacy by degrading the accuracy of special temporal information.

c. Mix networks

It uses the anonymizing channels to unlink process of reports submitted by the sensors before they reach the applications. Mix networks acts as the proxy servers between the sender and receiver. It follow some system defined criteria. It waits for some anonymity to send the packet further. In k-anonymity it will wait for k reports from system to met. It depends on no of reports received and mixed by mix networks.

And do not guarantee provably-secure privacy. Moreover, there may be scenarios when a long time can pass before the desired level of anonymity reached (when enough reports have collected). So it wil wait for some reports from system to met. And it decreases system throughput and it is not widely used.

d. k- Anotimy:

It provides guarantee that in a set of k objects the target object is hidden from other k – 1 objects. Thus, the probability of identify the targeted user is 1/k. The idea behind the k-anonymity is that a user reports an obfuscation area to a client containing his position and the positions of k – 1 other users instead of his precise position that is protected by a pseudonym. As an example consider that ram is currently located at home and queries a location based service for the nearest clinic. Without using anonymization, this query could reveal to the client implementing the service that ram has health problems. By using k-anonymity, ram would be indistinguishable from at least k – 1 other users, so the client cant link the request to ram. Therefore, it is required that all k users of the calculated anonymization set sent to the client share the same obfuscation area such that the client cannot link the issued position to the home location of ram.

e. Mix Zones:

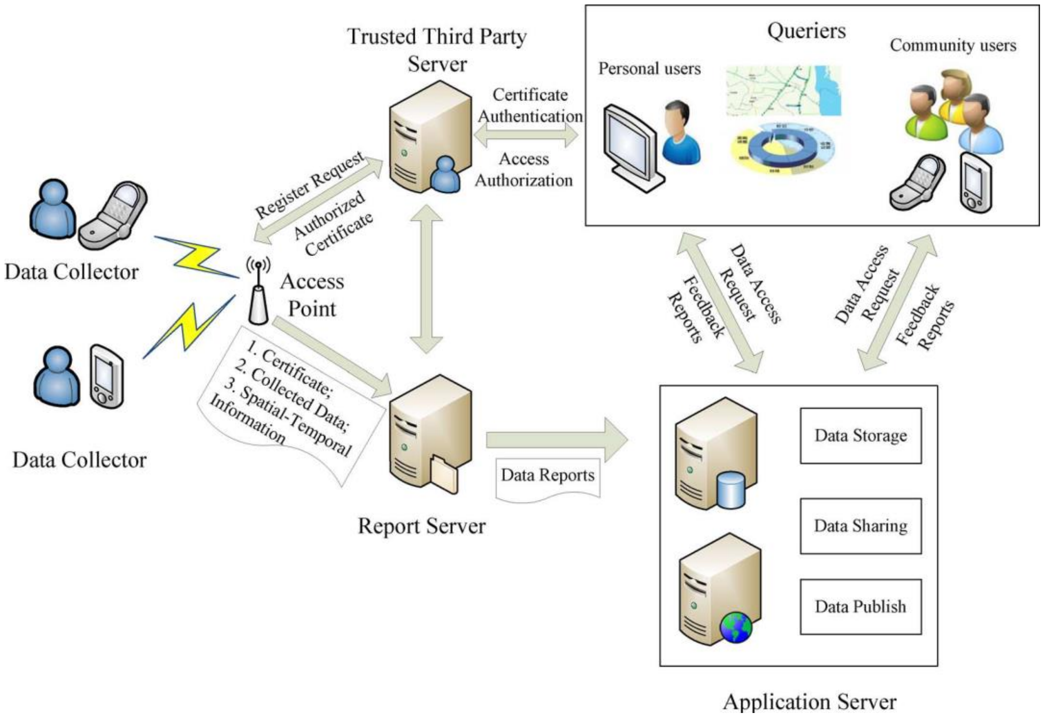
Pseudonym is used to unlink user’s identity to his/her events. The process of its change is usually performed in some pre-determined areas called the mix-zones. In these mix zones networks, the infrastructure provides anonymity service. The infrastructure delays and reorders messages from subscribers within a mix zone to confuse the third party. There is a problem with this system is that there must be enough subscribers in the mix zone to provide an acceptable level of anonymity.

f. Dummy locations:

This is a method mainly employs the idea of dummy locations to protect participators location privacy. The location-dependent query is written as Q = (pos; P), where parameter pos is the location of mobile user and parameter P is user defined predicates. And query Q is the original query. With the location dummy approach, the original query is converted into Q 0 = (pos1; pos2; : : : ; posk; P), where the posi include the location of real participators and k - 1 dummy locations, and P is the original query predicate that applies to all k-locations. We call query Q 0 a location privacy query, because it hides the user location.

2.1 Trajectory privacy protection:

Whenever the user’s trajectory path is known to others then their personal data is exposed to the public. Then It causes a threat to their personnel. So to get their information to be in private mode, then simplest way is dummy trajectories and suppression method. To produce a user’s dummy trajectories by using random pattern and band rotation pattern. More specifically the former generated dummy trajectory randomly from the source towards the destination and the later did it by rotating the user’s trajectory.



a. Dummy trajectory confusion:

Protecting the trajectory privacy in a data publication perspective done with a simple dummy trajectories confusion technique, So it suggest the technique of confusing the third party or hacker by adding dummy trajectories and to confuse the path in which the packets are travelling. It can be used to hide and protect the original path. Dummy trajectories are generated under two main principles: first, the movement patterns of dummies should be same as the real users; second one is the intersections of trajectories should be as more as possible. Based on these rules, The dummy trajectories can be generated by rotating the real trajectories of participators,.

b. Suppression based method:

It is based on assumption the different adversaries may have the different and disjoint sets of users' trajectories. Suppression-based method can reduces the probability of being disclosing the whole number of trajectories. Trajectory pieces should be suppressed and, publication of these sets of pieces may increase the trajectory's breach probability to be above a certain threshold.

c. Trajectory k-anonymity:

In this technical method first, the trajectories can be clustered based on log cost metric system, then each sample locations on the trajectories is generalized to a region which containing at least k number of moving objects. Then trajectories can be reconstructed through the randomly selecting the sample points from anonymized region.

3. Proposed work:

A trajectory privacy-preserving framework, for participatory sensing the proposed system helps to prevent linking of participators' identities with their uploaded data reports .The proposed method protects participators' identities and trajectories privacy from the perspective of graph theory based on mix-zones model and pseudonym technique. The locations on or nearby participators' trajectories may not all be sensitive, and with this thought, proposed system only deals with the sensitive trajectory segments. Here the theoretical mix-zones model is improved to construct trajectory mix-zones model for protecting sensitive trajectory segments from the perspective of graph theory. Compared with existing trajectory privacy-preserving proposals, the proposed method has advantages of lower costs and lower information loss while the privacy level would not decrease.

3.1 Trajectory privacy preserving framework:

TRPF anonymizes the sensitive trajectory segment from the perspective of graph theory. To reduce information loss and costs at a certain privacy-preserving level, the whole area should be divided into several parts. According to the sensitive locations on or nearby the trajectories, the whole trajectories need to be divided into sensitive trajectory segments and no sensitive trajectory segments. TRF identifies and protects sensitive trajectory segments based on mix-zones model and pseudonym technique.

Any data collector who enters the Sensitive Area should select a pseudonym provided by TTPs to anonymize the link ability between his identity and his collected data reports. Meanwhile, they record their ingress and egress time. A participator's information we describe as a tuple which consists of the participator's pseudonym provided by TTPs, mapping from participator's identity to his pseudonym, sensitive area the participator passes by, participators' enter time and participator's egress time interval. Trajectory Mixzones is modeled as Directed Weighted Graph (DWG), which is formalized as the set of vertexes which are constructed by the pseudonyms provided by TTPs. It can be depicted as the set of edges that represent the participators' Trajectory mapping from the ingress to the egress in the sensitive area. DWG is a complete bipartite graph with Different weights on each edge. As a result of pseudonym technique, there may be some difficulties for adversary to link the ingress and egress participator with the same identity.

In mix zones the participators may vary in time, if the residence time was constant, it may encounter First in First out (FIFO) attacks that is the first participator exited related to first person entering mixzones. To prevent this FIFO attack TRPF allows the time of participator's stay in mix zones to be random. Since the time interval of data collection in sensitive area is random, even though adversary obtains the related information such as ingress and egress order and time, it cannot link the ingress pseudonym to egress pseudonym. A participator vi enters the mix-zones at time tingress (vi) and exits the mix-zones in a time interval from tj to tj+1. Let P (vi,t) present the probability of participator vi exits the mix-zones in time
Interval [tj, tj+1].

4. Conclusion

The openness of data collector's trajectories causes very serious threats to participators' personnel privacy. It may be in a way of preventing participators from data to be sharing. This project, proposes a trajectory privacy-preserving framework called TrPF for participatory sensing and a trajectory mix-zones graph model to protect participators' trajectories from the perspective of graph theory. . It may be good in realistic in practice. In the future, the paper can be extended to work on the semantic trajectory privacy problems of multiple mixzones in detail.

Here the simulation results are likely to be proving that our mix zone trajectory privacy preserving graph model will acts very smartly against attacks on privacy threats from the hackers. It can reduce the information or data loss with respect of participators in the network. And it's to be very cheap and cost effective and easy to deploy in any type of the network in any architecture.

References

[1] http://en.wikipedia.org/wiki/Wireless_sensor_network.

[2] J. Freudiger, M. H. Manshaei, J. Y. Le Boudec, and J. P.Hubaux, "On the age of pseudonyms in mobile ad hoc networks," in Proc. IEEE INFOCOM, 2010, pp. 1–9.

[3] Juels, R. L. Rivest, and M. Szydlo. The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. In V. Atluri, ed. 8th ACM Conference on Computer and Communications Security, pages 103{111. ACM Press, 2003.

[4] C. Bettini, S. Mascetti, X. S. Wang, and S. Jajodia, "Anonymity in location-based services: Towards a general framework," in *Proc. IEEE Int. Conf. Mobile Data Management*, 2007, pp. 69–76.

[5] M. Saini, P. K. Atrey, S. Mehrotra, and M. Kankanhalli, " -privacy: Understanding what, when, and where inference channels in multicamera surveillance video," *Multimedia Tools and Applicat.*, pp. 1–24, 2012.

A Brief Author Biography

C Chandrasekhar reddy – Received B.Tech degree in the stream of computer science from JNTU Anantapur. And presently working toward M.Tech degree in the stream of Computer science information security from School of information technology, JNTUH, Hyderabad.

Mr. K Suresh babu – Completed M.Tech from Hyderabad Central University (HCU) , Hyderabad. Presently pursuing Ph.D. from JNTU Hyderabad in the field of network security in MANETs. Currently Assistant Professor of CSE in School of information technology, JNTUH, Hyderabad.