PRIVACY-PRESERVING BY A TRAJECTORY FOR PARTICIPATORY SENSING IN WIRELESS SENSOR NETWORKS

Mrs. Shreetha, Mr. S. Girish
Dept of CS&E
SCM,Adyar,Mangalore-575007
VTU,Belgaum
shreetha.shashidhar@gmail.com, giriait@gmail.com

Abstract— Emerging of embedded sensors like cameras, microphone, accelerometers etc, made the emergence of participatory sensing applications. The participator sensors are applied where there is use of users and group of users. The adversary is used to collect and analyses participators location and trajectory data, from which privacy of the system is harmed. By focusing on trajectory privacy, trajectory privacy preserving framework TrPF is proposed. Based on this a theoretical mix zone model with time as a factor from the graph theory is proposed, from which loss of information is less and hence it is cost effective, privacy is protected[1].

Keywords—component; Trajectory mix zone model using graph theory,TrPF:Trusted third party,Data collector.

I. INTRODUCTION

When comparing with WSN, participatory sensing offers advantages on deployment costs, availability, spatial-temporal coverage, energy consumption etc. Once participators come to know that their sensitive information is disclosing then they will not participate in the campaign. Since the success of campaign depend on the unselfishness process of data collection, if the participators are not ready to contribute their data, then it will weaken the popularity and impact of the campaign[1].

Harmful agent can analyze participators trajectory information which contains rich sensitive information. If harmful agent already has knowledge about participator trajectory, it destroys the record of the participatory. To overcome this drawback k-anonymity and trajectory mix zone graph models are proposed. When sending information from one node to another node the data holder can protect the other sensitive data through these two methods. In which participators information taken as tuple I=(IDp,Ri, Si,t-ingress, t-egress).

Where ID=participators pseudonym provided by Trusted Third-party (TTP), Ri= mapping from participators identity to his pseudonym, Si=sensitive area, t-ingress=entering time of participant, t-egress=egress time of participant. Trajectory mix zone is represented as Directed Weighted Graph (DWG), G=(V,E), where V is vertexes, constructed by the pseudonyms provided by TTPs. E is edges represents number of participators.

In the participator sensing system each participators report will be collected and it is tagged. When participator visited particular location, adversaries may trace this trajectory and can steal some sensitive data. To prevent linking of participator identity to their uploaded data report we propose a method to protect participator identity and trajectory privacy from the perspective of graph theory based on mix zone model and pseudonym technique, for that, a simulation tool is designed to define WSN and framework for participating in transaction.

II. RELATED WORK

Beresford and F. Stajano proposed pervasive computing, concentrates on location privacy, a particular type of information privacy that is able to prevent others from learning one’s current or past location. Privacy of location information here is actually controlled access to information [3]. The methods proposed here is anonymity set and mix networks. Anonymity set method tells, during the same time group of people will visit the mix zone. To measure the level of location privacy we take size of anonymity set. Until the mix zone offers a minimum level of anonymity we will not get any location updates. Limitations are, cannot trust these applications, these may reveal information that we aim to hide. Anonymity set is only an upper bound estimate.

Mix networks method tells about Store and forward networks (Network with normal message). Mix node collects n equal length packets as input before forwarding them it reorders the packet to provide unlikeliness between incoming and outgoing messages. Limitations are, to develop technique that lets users benefit from location based application with also preserving their location privacy.

Beresford and F. Stajano proposed mix zone model, at first privacy of personal location information has not a critical issue. But when location tracking system has the capacity to capture user movements, then location privacy becomes important. First strategy used here is geographic location privacy, rule based policies used here. Second strategy using digital certificates combined with rule based policies [4].This model assumes the presence of a trusted third party. Aim is to prevent tracking of long term user movements, but it allows the operation of short term location aware applications. Limitation is, analysis is expensive and requires partial evaluation of the problem.

J. Freudiger, M. Raya, M. Flegyhzi, P. Papadimitratos, and J. P. Hubaux proposed Vehicular Networks(VN). Vehicular network consists of Road Side Units equipped with radios and vehicles. Using vehicle-vehicle and vehicle-infrastructure communication, vehicles share information and location based services. Vehicular networks are more efficient traffic management which should satisfy requirements like sender, data, real time delivery, liability. VNs are applications of Ad-hoc networks. Public key infrastructure is available, so that messages are signed to achieve liability of their sender [5]. Limitations are, vehicles transceivers cannot be switched off, so 24*7 we can monitor vehicles whereabouts. Adversary installs radio receivers close to the road network so that we can eavesdrop the safety messages.
Kapadia, N. Triandopoulos, C. Cornelius, D. Peebles, and D. Kotz proposed anonymsense features. To protect privacy, tessellation and clustering mechanisms are used. Anonymsense focus on evaluating tessellation and clustering. In opportunistic sensing systems, applications can task mobile nodes. With opportunistic system, applications need not rely on a static sensor deployment. Opportunistic sensing systems examples are Cartel, Urban Sensing, and Mobiscopes. Methods proposed here is k-anonymity, local location blurring to improve k-anonymity, anonymsense-anonymous tasking and reporting [6].

K-anonymity tells that K reports are combined together before being revealed. To improve privacy against the system suggests the use of peer-peer mechanisms. Limitations are, here user must reveal their personal information to a trusted party. Method is expensive.

Local location blurring to improve k-anonymity tells that granularity of the user’s location is altered by adding uncertainty to the user location. Limitation is level of blurring all the time it is not sufficient to prevent deanonymization by the system.

Anonymsense-anonymous tasking and reporting tells that without any user intervention location privacy can be achieved. Tasks can be delivered to anonymous nodes and collects reports from anonymous nodes. Limitation is this method will mainly rely on mobile nodes carried by humans thus putting privacy of users at risk.

E. De Cristofaro and C. Soriente proposed participatory sensing infrastructure that involves sensors, carriers, network operators, queriers. With very low computational cost and no communication overhead, can achieve the privacy. Sensors are high end mobile devices, which offer greater resources. Here we have entities, operations and privacy requirement [7].

Entities are devices with sensing capabilities, responsible for communication infrastructure, handling application set up. Limitation here is to prove our proposal we must concentrate on authentication, data integrity, DOS prevention. Operations generate all public parameters and secret key. This method cannot extend our work for cellular network operator. Privacy requirement goal is to protect the privacy of producers and consumers data.

D. Christin, M. Hollick, and M. Manulis proposed Wireless Community Network (WCN). Wireless community networks are formed by the combination of wireless sensor network that are internetworked by wireless mesh networks. WCN offers valuable community and human centric services. WCN infrastructure offers high degree of heterogeneity, WCN will share information and digital resources [8]. Methods are community sensing, security and privacy model, mechanisms for privacy preserving personal and designated sensing. Security and privacy models, purpose is to protecting privacy in WCN sensing. Here it is difficult to provide controlled access to the sensed data. Mechanism for privacy preserving personal and designated sensing is based on privacy preserving access control mechanisms. Access is limited here. Challenge here is to deal with multiple authorities. Only to owner or community member are permitted to access. Community sensing has controlled access to the sensed data.

A. Kapadia, D. Kotz, and N. Triandopoulos proposed opportunistic sensing, describes small computational devices which are carried for daily activities, if we take interest in people centric sensing application then we can handle new security and privacy challenges. In opportunistic sensing model people own the mobile devices to collect sensor data of their
normal user’s trajectory. Obfuscation results in inaccuracy of the location. Time taken by this method is more. Anonymization is difficult to understand. Break the link between user and its event.

H.Liu,C.S.Jensen,andM.L.Yiu proposed privacy in mobile services. In mobile service location privacy become very important. This survey helps in large privacy region at reasonable costs. This survey is efficient in terms of computation communication costs and can come to know with what probability service provider able to infer the exact location. Limitation that we require a trusted third party that maintains all user location [15]. Methods is circle based dummy generation, grid based dummy generation. Circle based dummy generation is aware of the privacy area requirement. Grid based dummy generation is easy to implement, simple and effective, these have technique that reduces both upstream and downstream communication between client and server. Limitations are there is no trusted third party. Server side cost is high and considers only snapshot queries.

L.Sweeney proposed k-anonymity model. Data holder wants to share a data with researchers, data holder release a data, a release provides k-anonymity protection that is the information for each person in the release cannot be distinguished. Released information limits what can be revealed about information of the entities that are to be protected [16]. Methods are person specific information, disclosure control. Person specific information is specific to one person and no two tuples belong to same person. Data holder cannot always be up to date. Disclosure control limit disclosure in released data. There is a possibility that released data mapped to incorrect entities.

M. Gruteser and D. Grunwald, proposed spatial and temporal cloaking. Anonymity can provide a high degree of privacy. Here we are concentrating on the principle of minimal collection. From this approach, both parties will get benefit and there is less overhead. Service provider can get access to anonymous location information [17]. Methods are road hazard detection and road map. Road hazard detection is low time accuracy, helpful for deciding on accident prevention measures. Road map, from this automatically current location can be obtained. Response time must be accurate.

B. Gedik and L. Liu proposed personalized k-anonymity. Survey describes a scalable architecture for protecting the location privacy from different privacy threats. This propose flexible privacy personalization framework, also this survey describes personalized k-anonymity model in other words location privacy is personalized requirement and is context sensitive [18]. Method used here is message perturbation engine to capture requirements of location privacy, ensure service quality and effectively anonymization message.

M.DuckhamandL.Kulik and C. Ardagna, M. Cremonini, E. Damiani, S. De Capitani DiVemercati, and P. Samarati proposed obfuscation and negotiation. Obfuscation is important technique for protecting one’s location privacy. Negotiation is used to ensure that a location based service provider receives only the information it needs to know in order to provide quality of service. Obfuscation provides a high quality location based service based on low quality location information [19][20].

J.Freudiger,M.H.Manshaei,J.Y.LeBoudec,andJ.P.Hubaux proposed age of pseudonyms in mobile ad hoc networks. It provides detailed analytical evaluation of the age of pseudonyms and detailed quantitative framework. To

III. EXISTING SYSTEM

Trajectory privacy preserving framework (TrPF) system is based on mix zone graph model and k-anonymity.

- In mix zone graph model we have sensitive trajectory segments and non sensitive trajectory segments, only sensitive trajectory segments are protected.
- In k-anonymity k reports are combined together before being revealed [6].

Based on these points showed above many network applications have been developed, the major drawback of these are user must reveal their personal information to a trusted party ,also these are expensive.

IV.PROPOSED SYSTEM

When sender wants to send a data to a receiver, sender knows receiver address but it does not know the path to reach there. So it will ask with trusted third party in turn trusted third party will ask with owner or data collector .Data collector is a owner which has all information about ingress and egress time of participants, only data collector has that information. Data collector(owner) and participants are not directly connected. Trusted third party is a part of data collector(owner) by which participants are connected to data collector. Example for network application is, if for your email id unwanted mails are coming and you want to prevent it so by this system we trace the path of email id and give it to firewall system so we can stop it. Another example is when you enter into a organization as a participant first you will register yourself so while registering you can see other participants report that should be hidden by this system.
V. PERFORMANCE DISCUSSION
Performance of proposed system is more in terms of time and cost. This method is easy to implement in a short time and low cost. We can trace the path of participators and also there is no loss of information.

VI. CONCLUSION
In the proposed system at first TrPF is proposed for participatory sensing. Then trajectory mix zone model is proposed to protect participators trajectory. Then to prove the mix zone model time factor is taken into consideration. The proposed methodology can protect the participators trajectory privacy and reduce the cost and loss of information compared to existing systems [1].

REFERENCES