International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 03, March-2015

Survey on Privacy-Preserving by a Trajectory for Participatory Sensing in Wireless Sensor Networks

Mrs. Shreetha
Dept of CS&E
SCEM,Adyar,Mangalore-575007
VTU, Belgaum

Mr. S. Girish
Assistant Professor, Dept of CS&E
SCEM,Adyar,Mangalore-575007
VTU, Belgaum

***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.**

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.

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 participator, t-egress=egress time of participator. 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 [2]. 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 unlink ability 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 [3].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 [4]. 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 anonysense features. To protect privacy, tessellation and clustering mechanisms are used. Anonysense 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, anonysense-anonymous tasking and reporting [5].

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.

Anonysense-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 [6]. 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[7]. 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 daily life, allowing sensors to be remoter tasked on someone else's behalf. In this model sensor nodes are created by people [8]. Method used is opportunistic people centric sensing which collect sensor data in a huge amount without the need to deploy thousands of static sensors. This method is conceptually tied to specific individuals. Integrity of sensed data is achieved here. Limitations are, nodes are not sensing human behavior and data consumer cannot trust sensor nodes.

C. Y. Chow and M. F. Mokbel, proposed location based services(LBS), is due to mobile devices with GPS and internet connectivity, for example e-marketing, social networking, local business search, two types of Location Based services(LBS) are snapshot and continuous LBS[9]. Method used is location trajectory privacy, technique preserves data privacy. Privacy guarantee for a snapshot of the database. Limitation is, this method only support simple aggregate analysis such as range queries and clustering.

L. Liu proposed location privacy threats and various location privacy models. Location privacy defined as the ability to prevent other parties from learning one's current and past location, two level of privacy are personal subscriber level privacy and corporate enterprise level privacy[10]. Methods are location privacy threats, location service quality, and location anonymization.Location privacy threats described as unauthorized access to raw location data by an adversary by hijacking the location transmission channel. Location protection is achieved through user defined policies, through anonymous usage of information, through user identity. Limitations are when more accurate location information is disclosed, risk of location privacy is high. Different users require different levels of privacy.

Location service quality depends on accuracy of the location of users. Location anonymization is system capability to hide the location information.

J.Krumm, proposed computation based privacy mechanisms that treat location data as geometric data. Here it do not include protection schemes based on standard encryption access control, mix routing. We are concentrating here to protect our past location [11].

M. Decker, aim of this survey is to give an overview about the most relevant works [12]. LBS are widely used due to, approximate estimation of a position can be retrieved, after reaching destination navigation services will inform the user about his/her surroundings, location will be subject to many changes.

Methods are pseudonymization and policy approaches. Policy approaches tells under which condition which LBS are allowed to obtain location information. There is a need of technical arrangements to guarantee the policies. Pseudonymization types are role pseudonym, transaction pseudonym, person's pseudonym, public/non public pseudonym. This method is not a LBS specific technique.

R.Shokri,J.Freudiger,and J.P.Hubaux, proposed logical structure for classifying, organizing, identifying the concepts of location privacy. Defining location privacy as individuals to determine themselves when, how and to what extent location information of them is given to others , proposing a framework enables us to design a location privacy protection mechanisms[13]. Methods are anonymization, adding dummy events, obfuscation, hiding events. Hiding events tells hiding trajectories of users. Applied only in distributed architectures. Adding dummy events mislead an observer by adding some dummy events. Generating a trace of events that looks like a 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.Lu,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 [14]. 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 [15]. 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 [16]. 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 [17]. Method used here is message perturbation engine to capture requirements of location privacy, ensure service quality and effectively anonymize message.

M.DuckhamandL.Kulik and C. Ardagna, M. Cremonini, E. Damiani, S. De Capitani DiVimercati, 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 [18][19].

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 communicate, wireless networks require mobile nodes. In this case wireless nodes, over a single hop or multiple hops, communicate directly with each other. In this case to protect location privacy, node uses pseudonym for a while, then discards it and makes use of a new one. Age of pseudonym refers to the time period over which a pseudonym is used [20]. Method used is evolution of the age of pseudonyms. Here privacy is high, it analytically evaluates the age of pseudonyms and captures interaction between nodes and mobility. Limitations are, identity of the node can be leaked. Adversary can track mobile nodes. Location privacy requires effort from neighbouring nodes. Pseudonyms are costly.

J. Freudiger, R. Shokri, and J. P. Hubaux proposed optimal placement of mix zones. Survey propose a novel metric based on the mobility profiles of mobile nodes, paper is working on traceability, also we are considering trusted central authority. Survey will investigate deployment strategies [21].

X. Liu, H. Zhao, M. Pan, H. Yue, X. Li, and Y. Fang proposed traffic-aware multiple mix zone. It investigates a new form of privacy attack to the LBS system and also tell about resilience to such attacks, it will over come with problem of optimal multiple mix zones placement [22]. Method used here is traffic aware multiple mix zone placement, using this mobile networks wireless communication will become easy, also method will investigate optimal multiple mix zone placement problem, method gives protection from inferential attacks. Limitations are restrict privacy enhancing technology and deployment cost is high.

III. 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.

REFERENCES

[1] Sheng Gao,Jianfeng Ma,Weisong Shi, "TrPF:A Trajectory Privacy-Preserving Framework for Participatory Sensing", IEEE Transactions on Information Forensics and Security,vol.8,no.6,June 2013.

[2] A.R.Beresford and F.Stajano, "Location privacy in pervasive computing",IEEE Pervasive Comput.,vol.2,no.1,pp.46-55,2003.

[3] A.R.Beresford and F.Stajano, "Mix zones: User privacy in location aware services", in Proc.2nd IEEE Ann.Conf.Pervasive Computing and Communications Workshops,pp.127-131,2004.

[4] J.Freudiger,M.Raya,M.Flegyhzi,P.Papadimitratos,and J.PHubaux, "Mix-zones for location privacy in vehicular networks", in Proc.1st Int.Workshop on Wireless Networking for Intelligent Transportation Systems,Vancouver,BC,Canada,2007.

[5] A.Kapadia,N.Triandopoulos,C.Cornelius,D.Peebles,and.Kotz, "Anonysense:Opportunistic and privacy-preserving context collection", Pervasive Comput.,vol.5013,pp.280-297,2008.

[6] E.De Cristofaro and C.Soriente, "Pepsi:Privacy-enhanced participatory sensing infrastructure", in Proc.ACM 4th Conf.Wireless Network Security,pp.23-28,2011.

[7] D.Christin,M.Hollick,and M.Manulis, "Security and privacy objectives for sensing applications in wireless community networks", in Proc.IEEE 19th Int.Conf.Computer Communications and Networks,pp.1-6,2010.

[8] A.Kapadia,D.Kotz,and N.Triandopoulos, "Opportunistic sensing: Security challenges for the new paradigm", in Proc.IEEE 1st Int.Communication Systems and Networks and Workshops,pp.1-10,2009.

[9] C.Y.Chow and M.F.Mokbel, "Trajectory privacy in location-based services and data publication", ACM SIGKDD Explorations Newsletter,vol.13,no.1,pp.19-29,2011.

[10] L.Liu, "From data privacy to location privacy: Models and algorithms", in Proc.33rd Int.Conf.Very Large Data Bases,pp.1429-1430,2007.

[11] J.Krumm, "A survey of computational location privacy", Personal and Ubiquitous Comput.,vol.13,no.6,pp.391-399,2009.

[12] M.Decker, "Location privacy-an overview", in Proc.IEEE 7th Int.Conf.Mobile Business,pp.221-230,2008.

[13] R.Shokri,J.Freudiger and J.P.Hubaux, "A unified framework for location privacy", in Proc.9th Int.Symp.Privacy Enhancing Technologies,pp.203-214,2010.

[14] H.Lu,C.S.Jensen,and M.L.Yiu, "Pad: Privacy-area aware, dummy-based location privacy in mobile services", in Proc.7th ACM Int.Work-shop on Data Engineering for Wireless and Mobile Access,pp.16-23,2008.

[15] L.Sweeney, "k-anonymity: A model for protecting privacy", Int.J.Uncertainty Fuzziness and Knowl.Based Syst.,vol.10,no.5,pp.557-570,2002.

[16] M.Gruteser and D.Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking", in Proc.ACM 1st Int.Conf.Mobile Systems, Applications and Services,pp.31-42,2003.

[17] B.Gedik and L.Liu, "Protecting location privacy with personalized k-anonymity: Architecture and algorithms", IEEE Trans.Mobile Comput.,vol.7,no.1,pp.1-18,2008.

[18] M.Duckham and L.Kulik, "A formal model of obfuscation and negotiation for location privacy", in Proc.3rd Int.Conf.Pervasive Computing,pp.152-170,2005.

[19] C.Ardagna,M.Cremonini,E.Damiani,S.De Capitani Di Vimercati,and P.Samarati, "Location privacy protection through obfuscation-based techniques", Data and Applications Security XXI,pp.47-60,2007.

[20] 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,pp.1-9,2010.

[21] J.Freudiger,R.Shokri,and J.P.Hubaux, "On the optimal placement of mix zones", in Privacy Enhancing Technologies. New York,NY,USA:Springer,pp.216-234,2009.

[22] X.Liu,H.Zhao,M.Pan,H.Yue,X.Li,and Y.Fang, "Traffic-aware multiple mix zone placement for protecting location privacy", in Proc.IEEE INFOCOM,pp.972-980,2012.