RESEARCH ARTICLE OPEN ACCESS

Secure Distributed Collection of Data Using Participator Sensing Paradigm

CH.Aravind Kumar[1], SravanKumar.B[2]
[1]*Department of Computer Science, Vaagdevi College of Engineering, Warangal, Telangan,*
[2]*Department of Computer Science, Vaagdevi College of Engineering, Warangal, Telangan,*

ABSTRACT
Distributed collection of data has been made possible with the deployment of sensor devices across many geographical areas. Mobile phone users who employ sensors to acquire local knowledge pertaining to temperature, product pricing, transportation facilities and so on can participate in the network that is distributed in nature. Such network can acquire varied knowledge from diversified geographical locations. This kind of knowledge acquisition from across the globe is known as participatory sensing (PS). Of late it has become ubiquitous and rigorous research is on this field. Cristofaro and Soriente studied the operations of PS recently and came to know the fact that participation of mobile users is at risk when incentives or not considered and the users' privacy is at stake. Their framework could provide privacy besides improving the rate of mobile user participation in PS. However, their solution can be enhanced with respect to query privacy in the operations of PS. Towards this end we propose a framework that incorporates TLS security among the network so as to ensure foolproof security in the distributed collection of data through participatory sensing.
Keywords-Security, distributed collection of data, participatory sensing, and wireless sensor devices

I. INTRODUCTION

Wireless Sensor Networks (WSNs) became popular in the last decade due to their usefulness various fields. The need for sensing data is required in private and public sectors. Therefore there are plenty of real world applications of WSNs which are in use. They include monitoring atmosphere, rivers, woods, buildings, homes, offices, state-of-the-art infrastructures, wild life habitat and so on. Thus WSNs are widely used in the real world. When WSNs are owned by a particular entity and managed by it, privacy concerns do not exist. However, privacy issues came into surface when the WSN is to be made across mobile nodes with sensing capabilities. For instance mobile users can have sensing devices associated with their mobiles for collecting various kinds of information locally. Such users can participate in a distributed sensing network and contribute to the distributed data collection which might be very useful in making well informed decisions. For instance weather information can be collected across the globe in this fashion. Therefore IT professional started developing secure channels for realizing such distributed data collection system. In fact this is a new kind of paradigm in sensing data. This novel approach is known as participatory sensing. As technologies grow in future, it will be ubiquitous to use sensor in moles that can participate in distributed data collection. The data thus collected by local users might be extremely useful to remote users to make expert decisions. The data collected might be related to noise levels, traffic conditions, and weather and so on. This kind of distributed data collection paradigm will revolutionize the way information is shared across the globe in the real world. In fact this paradigm can be realized with well established infrastructure as there is plethora of advantages of it besides having cost benefits. Moreover gadgets like accelerometers, digital cameras, and GPS can boost the usage of such networks for distributed data collection as explored in [1].

II. RELATED WORKS

Participatory sensing has been around for some years and the research underwent on this is presented in this section. With respect to applications of PS, readers can find such information more in [3] where descriptive information is available on plethora of PS applications. Accelerators can be embedded in any Internet-aware device which can be useful to obtain related information in distributed fashion. The power of such information retrieval system is exploited by Kim et al. [4] for monitoring office, home etc. Other researches contributed in the area of PS are related to monitoring water quality [5], noise pollution [6] and air pollution [4]. Sensors can also be used for monitoring health, thanks to technological innovations in health care domain. This is explored in [7] where PS is used to monitor health of patients which will be known to health care providers located remotely. However, there are many privacy issues in PS as explored in [8]. In [9] weak assumptions are made while analyzing participatory sensing. Mixed

networks were used to protect anonymity of mobile users who participated in PS. In order to achieve this, the researcher used anonymizing techniques so as to keep the identity of the mobile users to remain private. However, provable privacy guarantees were not achieved by them due to inherent problems in WiFi infrastructure. The PS applications can be leveraged further in terms of security and speed using 3G/4G networks.

Privacy preserving data aggregation in terms of computing variance, average and sum is studied in [10]. Anonymity technique is used in [11] for providing a solution for community statistics based on time-series data. This is achieved using data perturbation with real world data sets in distributed fashion. Trusted platform modules concept is used in [12] for protecting user – generated content in terms of authenticity and integrity. When multiple un-trusted entities are present in PS network simultaneously, it is very challenging task to provide privacy in PS that includes service providers, data consumers and data producers. In case of public-subscribe networks [16] also similar challenge arises in protecting privacy of users. While PS needs loose coupling in the solution, the solution made in [13] assumes some knowledge priori pertaining to key exchange between subscriber and publisher. Therefore it is not possible to have PS applied to such systems.

Cristofaro and Soriente [2] presented a solution for secure and privacy preserving participating sensing. The solution ensures that the data consumers and data producer do not know each other. Thus their privacy is protected as there was no need for direct interaction between them. However, the solution presented in [2] needs further enhancement for secure query processing in PS. The solution presented in this paper takes care of it.

III. PRELIMINARIES

This section provides the basis information related to participatory sensing before introducing our proposed framework for secure participatory sensing.

Participatory Sensing

Wireless Sensor Networks have been around for sensing data from surroundings. WSN is a collection of sensor nodes that are connected to form a network. Since the inception, the WSN has undergone certain evolution. With the technology innovations, now it is possible to make use of mobile phones as mutes. However, the participatory sensing does not mean mere evolution of WSN. Mobile phones can act as sensing devices with powerful resources when compared to the nodes in normal WSN. As mobiles are used by human users, they can be easily charged and their batteries can be kept alive for long time. This will improve the lifetime of WSN. In traditional WSN the network is owned by an entity. This is not the case with PS as the nodes in PS network can be distributed across the globe and each mobile node with sensing capabilities can participate in sensing local data that will be gathered by service provider. The data thus collected in distributed fashion can be subscribed and queried as shown in Figure 2.

There are four important components in PS network. They are mobile nodes, queriers, network operators and service providers. The mobile nodes are the devices used by humans with mobility. These devices are equipped with sensing capabilities. With such provision, the mobile nodes can report local information. Queriers are the users who subscribe to PS application in order to have required data from various geographical locations. They are interested on the day to day live and interested data from various regions. Network operators ensure that there is network possible among mobile nodes. They provide required infrastructure and support services to see that the nodes are live and perform the intended operations. Service provider is the entity that provides requested data to queriers who subscribe to the PS application.

IV. IPROPOSED FRAMEWORK FOR SECURE PARTICIPATORY SENSING

Inspired by the work of Cristofaro and Soriente [2] we propose a framework which will make use of Transport Layer Security (TLS) [14] in order to protect communications among all parties involved in the PS application. The TLS is a stack of protocols that ensure secure communications among parties. The protocol stack is as shown in Figure 1.

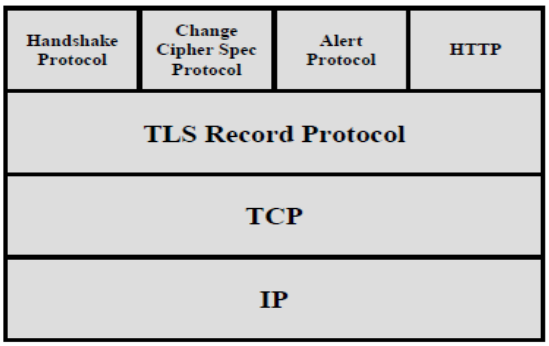

Figure 1 – TLS protocol stack

As can be seen in Figure 1, it is evident that there is a stack of protocols that involve in secure communications among parties in PS application as shown in Figure 2. The TLS protocol stack is made use of in the proposed PS application.

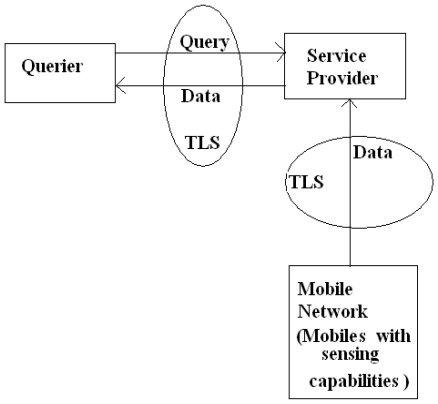

Figure 2 – Various parties involved in PS application

As can be seen in Figure 2, it is evident that four parties are visible. They are network operator (not labeled), mobile nodes, service provider and querier. They play the roles as described in the previous section. Between parties involved in the PS application security aspects such as message authentication, message integrity, message confidentiality and non-repudiation take place.

A. Message Authentication

After identity checking of querier and service provider they need some data exchange which needs to be authenticated. When a genuine querier makes a query to the service provider, the service provider should be able to authenticate the message. Such messages are to be rejected when they come from unknown sources. The TLS is used in order to make this verification. Even when the session is hijacked, the TLS security is able to ensure that it can identify the genuine sender of message and reject all other messages whose source cannot be established.

B. Message Integrity

Message integrity does mean that between two parties the transfer of data is done correctly and the data is not tampered with when it is in transit. MACs are used in order to provide message integrity besides using hash functions such as MD-5 [15]. With hash codes and the procedures required for data integrity, the queries and the replies from the service provider illustrated in Figure 2 are done with fool proof security.

C. Message Confidentiality

It does mean that the messages come from source should reach only the intended destination. It should not go to any other user or hacker. This is known as message confidentiality. In order to achieve this encryption algorithms like RSA are used. Thus the message confidentiality is achieved.

D. Non-Repudiation

It does mean that the sender of message should not be in a position to deny the sending fact later. The disclaim of the sender of message intentionally can happen in many real world networks. PS application is not exception for this. For this reason TLS also ensures non-repudiation besides other security features.

V. CONCLUSIONS AND FUTURE WORK

In this paper we studied the new paradigm for distributed data collection. From the research we came to know that WSNs can be evolved into motes that can help in sensing data from various geographical locations across the globe. Mobile nodes with sensing capabilities can participate in a distributed network and send reports pertaining to local information such as weather, traffic conditions, and pollution level and so on. This kind of network where mobiles nodes can involve is the new paradigm in WSN. We proposed a framework that can incorporate distributed data collection in secure fashion. Here the identity of sender and receiver is not disclosed. Moreover the data is collected and queried in order to make the whole paradigm useful to interesting people. We only focused on securing messages between two parties in the PS application as shown in Figure 1. However, it can be improved further so as to ensure that the mobile devices location can't be traced.

REFERENCES

[1]. D Cuff and M.H. Hansen and J. Kang, Urban sensing: out of the woods, Commun. ACM, vol. 51, no. 3, 2008, pp. 24-33.
[2]. Emiliano De Cristofaro and Claudio Soriente (2013), "Participatory Privacy: Enabling Privacy in Participatory Sensing", p1-10.
[3]. E. De Cristofaro and C. Soriente, Privacy-Preserving Participatory Sensing Infrastructure, http://www. emilianodc.com/PEPSI/.
[4]. D.H. Kim and J. Hightower and R. Govindan and D. Estrin, Discovering semantically meaningful places from pervasive RF-beacons, 11th International Conference on Ubiquitous Computing (Ubi- Comp), 2009, pp. 21-30.
[5]. S. Kuznetsov and E. Paulos, Participatory sensing in public spaces: activating urban surfaces with sensor probes, ACM Conference on Designing Interactive Systems (DIS), 2010, pp. 21-30.
[6]. N. Maisonneuve and M. Stevens and M.E. Niessen and L. Steels, NoiseTube: Measuring and mapping noise pollution

with mobile phones, 4th International ICSC Symposium on Information Technologies in Environmental Engineering (ITEE), 2009, pp. 215-228.

[7]. B. Longstaff and S. Reddy and D. Estrin, Improving activity classification for health applications on mobile devices using active and semi-supervised learning, 4th International Conference on Pervasive Computing Technologies for Healthcare (PervasiveHealth), 2010, pp. 1-7.

[8]. K. Shilton, Four billion little brothers?: Privacy, mobile phones, and ubiquitous data collection, Communications of the ACM, vol. 52, no. 11, 2009, pp 48-53.

[9]. C. Cornelius and A. Kapadia and D. Kotz and D. Peebles and M. Shin and N. Triandopoulos, Anony- Sense: Privacy-aware people-centric sensing, 6th International Conference on Mobile Systems, Applications, and Services (MobiSys), 2008, pp. 211-224.

[10]. J. Shi and R. Zhang and Y. Liu and Y. Zhang, PriSense: Privacy-Preserving Data Aggregation in People-Centric Urban Sensing Systems, 29th IEEE International Conference on Computer Communications (INFOCOM), 2010, pp. 758-766.

[11]. R.K. Ganti and N. Pham and Y.E. Tsai and T.F. Abdelzaher, PoolView: stream privacy for grassroots participatory sensing, 6th International Conference on Embedded Networked Sensor Systems (SenSys) 2008, pp. 281-294.

[12]. P. Gilbert and L.P. Cox and J. Jung and D.Wetherall, Toward trustworthy mobile sensing, 11thWorkshop on Mobile Computing Systems and Applications (HotMobile), 2010, pp. 31-36.

[13]. M. Ion and G. Russello and B. Crispo, Supporting Publication and Subscription Confidentiality in Pub/Sub Networks, 6th Iternational ICST Conference on Security and Privacy in Communication Networks (SecureComm), 2010, pp. 272-289.

[14]. AtharMahboob& Dr. NassarIkram, " Transport Layer Security (TLS) – A Network Security Protocol for E-commerce", p1-13.

[15]. Rivest, R. L.: "The MD5 Message-Digest Algorithm", RFC 1321, 1992

[16]. P.T. Eugster and P.A. Felber and R. Guerraoui and A.M. Kermarrec, The many faces of publish/ subscribe, ACM Computing Surveys, vol. 35, no. 2, 2003, pp. 114-131.