IOSR Journal of Computer Science (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727
PP 13-17
www.iosrjournals.org

Review on Enabling Enhanced Privacy in Participatory Sensing

Ms. Sayara Bano Sheikh[1], Mrs. Preeti Deshmukh[2]
[1](Student, M.E. (WCC), PCE Nagpur, India)
[2](Assistant Professor, Computer Technology, PCE Nagpur, India)

ABSTRACT : *The extreme use of mobile phones has increased the amount of digital data produced and processed every day. Participatory Sensing (PS) is an emerging paradigm that focuses on the collection of digital data produced from a large number of connected, always-on, always-carried mobile devices. PS takes the advantage of rapid progress of the sensor-equipped devices and therefore theomnipresence of broadband network infrastructure produces sensing applications whereverreadying of a WSN infrastructure isn't economical or not possible.. It targets to providing high level of privacy and security in participatory sensing to data producers like users who are providing sensed information and consumers like applications that are accessing the gathered information. Hence providing privacy to the users of such a PS today becomes a significant concern. We are here providing a review on enhanced privacy in Participatory Sensing (PS).*

Keywords *-Participatory Sensing (PS), privacy, Mobile Node (MN), Querier, Privacy.*

I. INTRODUCTION

The idea of a wireless sensor network is not novel. A wireless sensor network (WSN) consists of spatially scattered self-directed sensors to observe physical or environmental conditions, like temperature, sound, pressure, etc. and to helpfully pass the sensed information through the network to a main location. We are aware about the sensors that are integrated in low-power devices to collect data which also performs computation along with connectivity with the real world. From the previous decade, researchers have imagine the blast of Wireless sensor Networks (WSNs) and expected the in depth installation of sensors, e.g., in buildings, rivers, forest or probably the atmosphere. This has triggered lots of interest in many different WSN topics.

As sensors abatepriceyand extrawidelyoffered, it'spotential to plant in mobile devicesenhances. Mobile phones have created fundamentally a new stage for data collection, discovery, and social analysis. Mobile phones are usually on and carried devices than any previous personal technology. Mobile devices are progressively more equipped with the ability to sense the physical world (for example, through cameras, microphones, and accelerometers) and therefore network world (with Wi-Fi and Bluetooth interfaces) putting forward several opportunities for cooperative sensing applications.

Participatory sensing (PS) is an upcoming model that targets the seamless collection of data from a large number of user-carried mobile devices which are embedded with sensors. By embedding a sensing element to a mobile phone, PS enables collection of sensed information about environmental trends, such as urban traffic patterns, health-related information, parking availabilities, sharing consumer pricing information in offline market, etc. PS is a new practice which makes use of the sensor equipped tools to collect and analyze data for use in social science, environmental and health discovery. At the same time, they deeply challenge our current understandings of privacy policy and data security.

1. Participatory Sensing (PS)

Participatory sensing (PS)[1] is also known as opportunistic sensing or opportunistic people-centric sensing or urban sensing. PS is revolutionary rising paradigm that focuses on the seamless collection of information from an outsizedrange of connected, always-on, always-carried devices. PS combines the availability and the state of being everywhere of mobile phones with sensing capabilities. PSrefers to a mechanism by which the people collect, share and analyze native data. In PS [2], users with mobile devices (e.g., cell phones) participate in the collection of environmental information around them and submit the collected data to a central server for process, analysis, and storage. PS allows

people to participate as a volunteer and sense their environmentby means of close at hand sensor devices such as smartphones, and share this information with the existing cellularand Internet communication infrastructure.

PS [3] emphasizes the involvement of human being within themethodof sensing. Most significantly, PS begins and ends with public. Several features of mobile phones make them a special and unprecedented tool for engaging participants in sensing their local environment. PS can draw on a range of mobile devices; the very first is their pure ubiquity across the demographic and geographic spectrum. The broad proliferation of mobile phone usage makes it doableto gatherinformation. Through the global wireless network, people who wish to participate in PS scattered across a city or the world willsimply coordinate activities and transferinformation to servers wherever it is processed and integrated with differentinformation. A small computational device which is carried by individuals in their daily activities, sensing information directly or indirectly related to human activity is uploaded to server [3].

Opportunistic people-centric sensing is a sensing modelwhich involves humans as part of the sensing infrastructure. In the opportunistic-sensing model [3], sensor nodes are mobile as they are carried by people which are embedded in their personal cell phone and so are conceptually tied to specific individuals. Most previous sensor-network analysis has centered on aggregation and processing environmental data employing a static topology and an application-aware infrastructure, whereas PS involves collecting, storing, processing and fusing massive volumes of informationassociated witheveryday human activities. This extremely dynamic and mobile setting wherever humans are the central focus presents new challenges for data securityasthe information originates from sensors carried by people and not like WSN in which nodes are fixed.

2. Need To Provide Privacy To PS

The abundance and the heterogeneity of entities in PS is an issue which is presently an increasing challenge [2]. In contrast to WSNs, sensing devices are no longer dull gadgets, owned by the network operator; in PS sensors are nothing but the personal devices that follow users at all time and their reports usually figures their personal information. Thus, not alonetraditional security butin addition privacy issuesought to be taken into account, as there is always a fear of personal information disclosure. PSwill pave because of novel distributed computing and new business models. However, PS is powerfullyrelated tothe numberof users who are willing to devote device resources to sensing applications. Thus, wishing ongiant and omnipresent user participation, PS will become effective provided thatit'llprotectthe privacy of participating entities [3].

Issues like confidentiality or integrity should be rigorously addressed [1]. As an example, all parties must be shielded from external eavesdroppers. The communications between Mobile Nodes and Service Providers or between Service Providers and Queriers must be kept confidential. Then again, the need for privacy protection is high because there is also a probability of the personal information leakage to internal adversaries. Indeed, because theService Provider collects all information (i.e., reports and queries), it would learn an extensive amount of sensitive data regarding each Mobile Nodes and Queriers, and break the privacy of their movements, interests, habits, etc. The continuous collection of information over long periods permits the Service Provider to meticulously profile users. Further, as data collected through PS applications becomes accessible to external entities and organizations (i.e., the Queriers), query interests also become sensitive and need to be hidden. The reports are available only to entitled (e.g., authorized or paying) members. If users feel that their privacy is at risk, they will refuse to share their reports. Particularly, it is required that the Service Provider performs report/query matching but learns no information concerning query interests. Also, data reports should not disclose any sensitive information to the Network Operator, the Service

Provider or unauthorized Queriers about the entities which are involved in PS, any information about their identity and its location.

3. Privacy Enhanced Participatory Sensing Infrastructure (PEPSI)

PEPSI [1] [2] is a designed as a solution to provide privacy in PS application with respect to Mobile Node and Queriers. Fig.1 depicts Participatory Sensing infrastructure which also described following terms

4.1 PEPSI architecture

1. **Mobile Node (MN):** This are the sensor equipped mobile devices which is carried by users who voluntarily participate into PS. the role of MN is to provide the sensed data. The data collected from sensors is also called as report
2. **Querier:** Queriers are the end users who are interested in receiving the sensed report.
3. **Network operator (NO):**The NO is liable for the communication infrastructure. NO provides network to collect and deliver sensor measurements(e.g. GSM or 3G)
4. **Registration Authority (RA):**The RA handles the registration of MN and Querier. RA additionally contributes to privacy protection, and manages Queriers' subscription
5. **Service provider (SP):** The SP acts as an intermediary between the MN and Queriers subscribed to them. As Mobile Nodes and Queriers have no direct communication nor mutual knowledge, Service Providers route reports matching specific subscriptions to their original Queriers

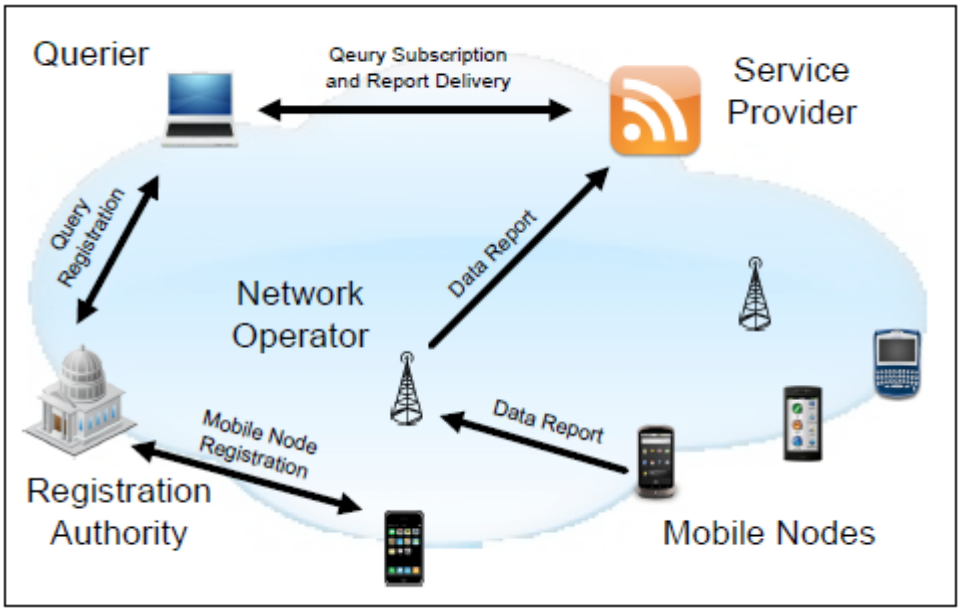

Fig.1 Privacy-Enhanced Participatory Sensing Infrastructure

The main aim of PEPSI is to grant security to both MN and Querier. PS must pay attentionconcerning the privacy of the participants, that is one who provides sensed data and the one who uses that data, their privacy must not be in danger. In order to fulfill this demand, PEPSI introduces an entity called as Registration Authority (RA). Phone manufacturer, as an example nokia, acts as RA and provides inbuilt sensor phone model. RA sets up the system parameters and manages Mobile Node and Querier registration. MN and Querier first register themselves to be authorized participants of PS. Hence only authorized participants can be a part of PS. Service Provider (SP), for example Microsoft or Google, offers PS application and acts as an intermediary between the Mobile Node and Querier.

For example, assume that Querier submits a query "available parking spots on W 16th Street, Canada. One of the Mobile Nodes shares knowledge "3 available parking spots on W 16th Street, Canada", with the Service Providers that makes this information available to Queriers.

PEPSI [1] [2] should also provide secure encryption of reports and queries. The main building block of PEPSI is IBE algorithm; IBE is used as a standard public key cryptography in PS. In IBE there is no need to distribute the public key which is advantageous to PS because there is a need to provide security to numerous mobile devices. As in PS there is no direct communication between MN and Querier, IBE is efficient cryptography tool for PS application. The public key is based on the information submitted by MN. After submitting he query, Querier get encrypted information and public key and Querier can obtain the private key from RA.

II. APPLICATIONS OF PS

PS depicts the state of affairs of "by the public and for the public". Consider a paradigm[1], www.gasbuddy.com is a PS application where gas prices are monitored from the reports and information speak out by participants and hence exposes their locations and movements. Few examples of PS application are explained below.

Iordanis Koutsopoulos [4] classifies the PS applications into three families: environment-centered, infrastructure and facility related, and socially or community centered. The OpenSense[5] PS infrastructure is beneath 1st category performs real-time air quality monitoring and encompasses heterogeneous sensors. Associated example of the 2nd category is GreenGPS[6] that uses a vehicle interface to quantify and hand on fuel consumption and location data which is used to constructs fuel-efficient routes to destinations for querying users. Another example of 2nd class is CrowdPark[7] which facilitates parking slots from obviously, user submitted information and allows this informationto assistalternative users find parking spots. In a system of the third category, LiveCompare[8] participants use their phone cameras to take a picture of the price tag of a product of interest. In exchange for submitting a price data point, the user receives pricing information for the product at nearby grocery stores. One more example is DietSense[9], in which individuals take pictures of what they eat and share it within a community to compare eating habits, e.g. in a community of diabetics.

III. EXISTING SYSTEM AND PROBLEMS

PS is not a new concept. A lot of work is already been done. Currently PS provides more sophisticated and secure architecture. Security is becoming the focus point or say the first priority for the users who are taking part in PS i.e. the participants of PS. But users are demanding if talking about security and privacy. Various security issues are addressed in PS application. PS maintains confidentiality and integrity [1] [2] [3] of the information which is submitted by MN and used by Querier. The information is submitted and available only to the authorized users. Also PS uses some cryptographic tools to ensure security. As PS is getting lot of information continuously there is a need to maintain all the information. Also providing the related information only to Querier is also challenging for PS.PS uses query/report matching for this purpose.

In the existing system PS provides security to users but uses are not satisfied. There is still a requirement to do a lot of work in field of security and privacy of PS. PS must provide a great deal of security that the user won't hesitate to participate and the success of PS greatly depends on the number of participants.

In PS [1] there is a need to provide node privacy SP and RA. Also hiding user's location and identity against NO is an open challenge the identity of participants i.e. identity of MN and Querier. High level of report and query privacy must be taken into account which will be helpful for solving the problem of collision attacks. PS application should adapt more complex syntax of query/report matching.

IV. CONCLUSION

PS is a novel computing paradigm that bears an outstanding potential. If users are encouraged to contribute personal mobile device resources, numerous applications and business models will crop-up. We projected the architecture of a privacy-preserving Participatory Sensing infrastructure and introduced an efficient cryptographic solution that achieves privacy with obvious security. In this paper PS, existing privacy situation in PS and security issues in PS is discussed. We claim without protecting the privacy of both data consumers and data producers, user participation can't be afforded.

REFERENCES

[1] Claudio Soriente andEmiliano De Cristofaro, *Participatory Privacy: Enabling Privacy in Participatory Sensing*, IEEE transactions on networking NO.1 VOL.27 YEAR 2013
[2] E. De Cristofaro and C. Soriente, *Privacy-Preserving Participatory Sensing Infrastructure*, *http://www.emilianodc.com/PEPSI/*.
[3] Kapadia, A.; Kotz, D.; Triandopoulos, N., *"Opportunistic sensing: Security challenges for the new paradigm,"*Communication Systems and Networks and Workshops, 2009. COMSNETS 2009. First International, vol., no., pp.1,10, 5-10 Jan. 2009 doi: 10.1109/COMSNETS.2009.4808850
[4]Koutsopoulos, I., *"Optimal incentive-driven design of participatory sensing systems,"*INFOCOM, 2013 Proceedings IEEE, vol., no., pp.1402,1410, 14-19 April 2013 doi: 10.1109/INFCOM.2013.6566934
[5] *OpenSense Project*: http://www.nano-tera.ch/projects/401.php, 2010
[6] R.K. Ganti, N. Pham, H. Ahmadi, S. Nangia, and T.F. Abdelzaher, *"GreenGPS: A Participatory sensing fuel-efficient maps application"*, inProc. ACM MobiSys, 2010.
[7] T. Yan, B. Hoh, D. Ganesan, K. Tracton, T.Iwuchukwu, J.-S. Lee, *"CrowdPark: A Crowdsourcing-based Parking Reservation System for Mobile Phones"*, University of Massachusetts at Amherst Tech. Report, http://lass.cs.umass.edu/ yan/pubs/yan11CrowdPark.pdf
[8] L. Deng and L.P.Cox, *"LiveCompare: Grocery Bargain Hunting through Participatory Sensing"*, in Proc. ACM HotMobile, 2009.
[9] S. Reddy, A. Parker, J. Hyman, J. Burke, D. Estrin and M. Hansen, *"Image browsing, processing, and clustering for participatory sensing: Lessons from a dietsense prototype"*, in Proc. 4th Workshop on Embedded NetworkSensors (EmNets), 2007.
[10] Chih-Jye Wang; Wei-Shinn Ku, *"Anonymous Sensory Data Collection Approach for Mobile Participatory Sensing,"*Data Engineering Workshops (ICDEW), 2012 IEEE 28th International Conference onpp.220,227, April 2012