Location Based Secure Communication in Mobile Sensor Network

Madhuri Bhandalkar
Department of Computer Engineering
Trinity College of Engineering & Research
Pune, India
madhuri.bhandalkar89@gmail.com

Prof. Avinash Palve
Department of Computer Engineering
Trinity College of Engineering & Research
Pune, India
avi.palve@gmail.com

Abstract**—** Now a day's Mobile crowd sensing is an new paradigm which is based on power of the crowd jointly with sensing capabilities of various mobile devices such as Smartphone's or wearable devices.MCS helps users to acquire local information from the surrounding environment through the sensing property of mobile device which is used in many areas like healthcare, transportation, environmental which helps in improving peoples quality of life. But MCS has two major problems like user privacy and data trustworthiness. In this first we discuss the MCS architecture with its characteristics and advantages over wireless sensor network. And at last we will discuss future recent trends as well as our efforts to MCS.

Keywords*-Mobile Crowd Sensing.User privacy,data trustworthiness,smartphones*

*****

I. INTRODUCTION

Many emerging technologies have been evolved into smart phones which consists more processing power and storage capacity. In today's world the evolution of mobile phones is increasing rapidly which makes them so powerful that many novel applications can be run on them. Recently mobile wearable devices like Google Glass and Galaxy Gear are equipped with similar capabilities. These devices consists of powerful embedded sensors like gyroscope, camera, microphone etc. using these sensors many sensing applications can run on wearable devices among them MCS is an example.

MCS depends on the user to collect information from the surrounding environments using the sensors, and then upload the data to application server using the network. Then the application server will process the data and extract the useful information and forward that information to the user.

Mobile crowd sensing has different categories of applications like healthcare, business, environment, social networking and transportation. for example of environment when the user wants to find the current environment status of the particular location at that time using his mobile application he will get logged in and then the current position all these data is sent to the server and then server will process those data and extract useful information like temperature, time, date, location, climate condition and then these information is sent back to the user.

Usually MCS focuses on upcoming new applications and solution of data collection. But MCS faces mainly two problems that are user privacy and data trustworthiness. The first issue is the user privacy as we know that MCS application contains large amount of data collection from different areas. As the participants upload their own personal information on the web which may get hacked by the another person on the internet. Or sometimes the hackers may disclose their location, or sometimes they may hack there important information. The different type of attacks on user privacy may be like user identification attack in which ID and time/date may get hacked. Second one may be the Sensitive location tracking in which the IP address and location may get disclosed. The third one may be the sequential tracking attack in which all of the above information may get loosed. As the result the people may get afraid of taking part into the MCS or get afraid of using MCS. So this issue needs to be addressed immediately. The second security issue is the Data trustworthiness that can be called as the reliability of the uploaded data. Whenever the user sends data to the application server there the data owner saves the data to the database but he is not confirmed whether the data faulty or true data. So this issue also be resolved.

II. LITERATURE SURVEY

In this paper the author S.Gaonkar has presented design and implementation of MicroBlog, which allows smart phones equipped users to use geotagged data which is called microblogs. This data can be extract or queried through either internet map service for example Google Maps or physical space when a user moves through a location. Hence the Microblog allows the internet user to directly end queries to a set of phones located in a region of interest. Then the phone in the appropriate region which receives these request can reply at their decision.[1]

In this motivation of the author P.Narula is the message security using trust-based muti-path routing in MANETs.He proposed method of message security using trust-based multi-path routing. Less trusted nodes are given lower number of self-encrypted parts of a message, making it difficult for malicious nodes to gain access to the minimum information required to break through the encryption strategy. Using trust levels, we make multi-path routing flexible enough to be usable in networks with 'vital' nodes and absence of necessary redundancy. In addition, using trust levels, we avoid non-trusted routes that may use brute force attacks and may decrypt messages if enough parts of the message are available to them paths.[2]

In a participatory sensing system mobile users sense and collect data from sensing devices in wich the data can be either saved on the device or uploaded to a centralized server so the data can be shared among other users. Here the challenge is that privacy preservation for participatory sensing data for example user trajectories.In this paper the author develops the participatory sensing system app for Android smartphones and proposes an efficient method for privacy preservation.[3]

In this the author K.L Huang and S.S Kanhare has made the case for evaluating device trustworthiness in partipatory sensing applications and motivated the need for a reputation system. And also proposed reputation system that employs the Gompertz function for calculating reputation scores. And also experimentally evaluated there system by incorporating it within a real-world noise monitoring application using Apple phone. And the results shows that there scheme scores three-fold improvement as compared to state of the art Beta reputation scheme.[4]

As we know that the two main challenges in partipatory sensing are user privacy and data trustworthiness. It this paper the author A.Dua presented a way to transfer reputation values(which may be a proxy for getting trustworthiness) between anonymous contributions. Also proposed a reputation scheme that prevents the leakage of privacy due to the inherent relationship between reputation information. Thus the result shows the scheme reduces the probabilities of users being tracked via successive contributions by as much as 80%.[5]

In this paper argue that openness of privacy preserving system makes it vulnerable to be miss used by malicious users who may misuse the information ,damage the information or launch Sybils to destroy the information. So the author proposed and implemented a trusted platform module(TPM),i.e angel based system that points the problem of providing sensor data integrity.The main idea is to provide a trusted platform within each sensor device to attest the integrity of sensor readings. TPM prevents users from launching Sybils. They also make the case for content protection and access control mechanisms that enable users to publish sensor data streams to selected groups of people and address it using broadcast encryption techniques.[6]

In this paper the author D.Christin address the privacy threat by introducing a framework called Incognisense. In which thesystemutilizes periodic pseudonyms generated using blind signature and depends on reputation transfer between these pseudonyms.Theauthor investigate by means of extensive simulations several reputation cloaking schemes that address this tradeoff in differentways. And the system is robust against reputation corruption and a prototype implementation demonstrates that the associatedoverheads are minimal.[7]

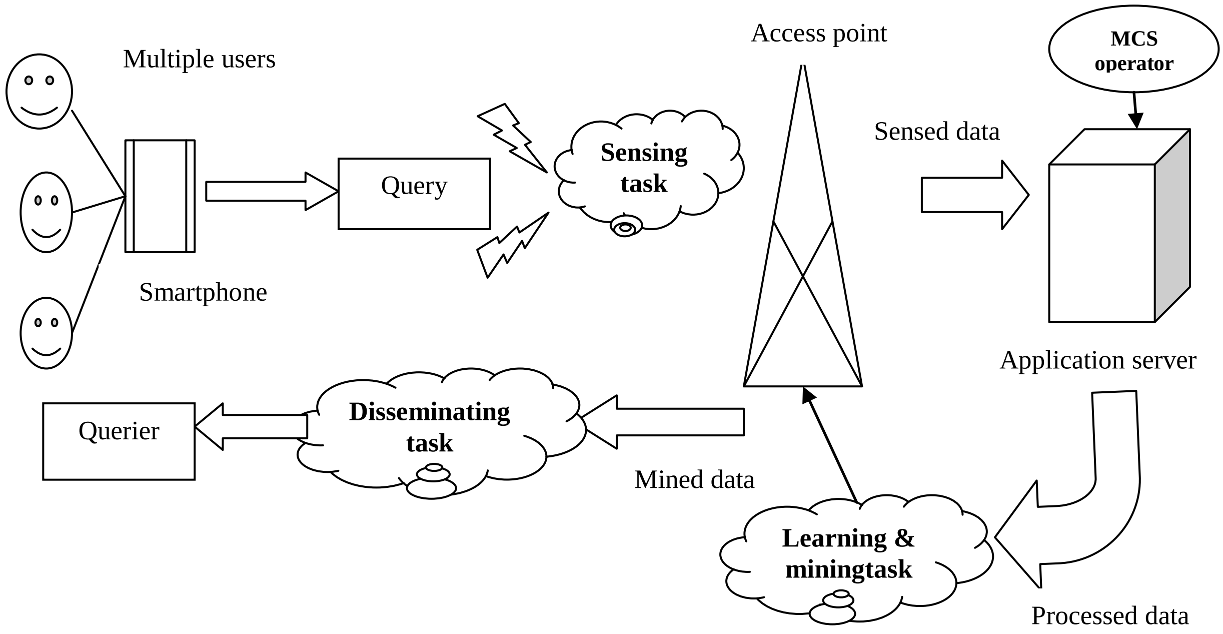
This paper studies how an untrusted aggregator in mobile sensing can periodically obtain desired statistics over the data contributed by multiple mobile users, without compromising the privacy of each user. Also, they do not consider the Min aggregate, which is quite useful in mobile sensing. To address these problems, Q.Li.G.Cao and T.La Porta propose an efficient protocol to obtain the Sum aggregate, which employs an additive homomorphic encryption and a novel key management technique to support large plaintext space. They also extend the sum aggregation protocol to obtain the Min aggregate of time-series data. To deal with dynamic joins and leaves of mobile users, we propose a scheme that utilizes the redundancy in security to reduce the communication cost for each join and leave. [8]

The authors C.Counelius tried to achieve anonymity of users by using Mix Networks. A mix network is statistical-based anonymizing infrastructure achieving the k-anonymity property,which ensures that the operator cannot identify the originator of each sensing record from a group of k or more participants. It aims to prevent an adversary from linking all reports of a mobile node, identifying which mobile node sent the report were generate.[9]

In this paper the author S.Gao proposed trajectory privacy preserving framework, named TrPF, for participatory sensing. Based on this framework, improve the theoretical mix-zones model with considering the time factor from the perspective of graph theory. It analyze the threat models with different background knowledge and evaluate the effectiveness of proposal on the basis of information entropy, and then compare the performance of proposal with previous trajectory privacy protections.[10]

In this paper , the author have proposed using Virtual Individual Servers as privacy-preserving proxies for mobile devices. He discussed advantages and disadvantages of this approach and argued that the advantages outweigh the disadvantages. He also described a number of applications that can benefit from this approach, and presented our initial implementation and evaluation of a decentralized framework for mobile social services based on VIS proxies. Our experience so far suggests that building such applications on top of the VIS concept is feasible and desirable.[11]

III. PROPOSED SYSTEM ARCHITECTURE



1.Participant or Mobile Node: Participants or mobile nodes register properly with the application servers managed by MCS operator. Once the registration is confirmed by authority, he/she can upload reports with the help of mobile sensors in their smart phones.

2.Service providers: The service providers on the other hand handle the mobile phone sensing information to the system. After getting all the user registration of participant and querier the confirmation for the mobile nodes are given, only when they have given valid details. Then the collected reports from mobile nodes are verified. When the querier queries, the reports for their query is transmitted to the querier with the encrypted details of participant.

3.Querier: Querier are mobile users, who queries for their needs. They too have a valid registration with the registration authority. They get the reports according to their queries with encrypted details of participants. Also the location is shown in Google maps.

4.Phases of Mobile crowd sensing:-

4.1 Sensing phase:

In the sensing task ,before the user of a mobile wearable device would use the MCS application the user first of all needs to download the corresponding app then only the user can becomes the participant of the MCS application. Whenever the user gives a query, the application server informs all participants about their sensing tasks. Then only the app starts collecting data using the relevant sensors.

4.2 Learning and mining phase :

In the learning and mining phase there are two data collection models, in the first model the participants important role who decides when to report data. In the second model ,reporting occurs then only when the state of the mobile wearable device satisfies the task requirements. So the sensed data are uploaded to the application server with the help of the Wi-Fi or different networks. Then the application server processes the sensed data to extract the appropriate information using different methods like machine learning, data mining.

4.3 Disseminating phase:

The results whichever have been generated are formatted into suitable forms and then they are made available to the queriers**.**

IV. CONCLUSION

In this way, in this paper we have identified two important challenges user privacy and data trust- worthiness on mobile crowd sensing application and methods two provides these issues.

REFERENCES

[1] S.Gaonkar et al.,” Micro-blog:Sharing & Querying Contents through mobile phones and social participants,,” Proc.ACM MobiSys,2008,pp.174-86.

[2] P.Narula,” Security in Mobile Ad-hoc networks using soft encryption trust-based multi-path routing”, Comp.Commun,vol.31,no.4,Mar.2008,pp.760-69.

[3] I.Boutis and V.Kalogeraki,”Privacy Preservation for participatory Sensing Data”,IEEE PerComm,Mar.2013,pp.103-13.

[4] K.L.Huang.S.S.Knahere,”Are you contributing trustworthy data? The case for reputation system in participatory sensing”, Proc.ACM MSWiM,2010,pp.14-22.

[5] L.K.Huang,S.K.Salil,"A privacy preserving reputation system for participatory sensing,” ,IEEE LCN,2012, pp.10-18.

[6] A.Dua, ”Towards trustworthy participatory sensing,”, USENIX HotSec.,2009.pp.1-6.

[7] D.Christin,”IncogniSense: An anonymity-preserving reputation framework for participatory sensing applications,” Persasive and Mobile Computing,vol.9,no.3,2012,pp.353-71.

[8] Q.Li,G.Cao and T.La Porta,”Efficient and privay aware data aggregation in mobilesensing,”IEEE Trans.Dependable Sec.Comp.,vol.11,no.2,Mar.-Apr.2014,pp.115-29.

[9] C.Cornelius,”Anonysense:Privacy-aware people-centric sensing,”ACM Mobisys ,2008,pp.211-24.

[10] S.Gao,”TrPF:A trajectory privay preserving framework for participatory sensing’,IEEE trans.Info.Forensics Security,vol.8,no.6,June 2013,pp.874-87

[11] R. Caceres, “Virtual Individual Servers as Privacy- Preserving Proxies for Mobile Devices,” Proc MobiHeld Wksp.,2009,pp.32-36

[12] E. De Cristofaro and C. Soriente, “Participatory Privacy:Enabling Privacy in Participatory Sensing,”IEEE Network,vol.27,no.1,Jan.Feb.2013,pp.32-36.