SECURE COMMUNICATIONS THROUGH DAPP

[1]Ms.G.Gayathri, [2]V.Muneeswaran
[1]PG Scholar, [2]Associate Professor
Department of Computer Science and Engineering
Sri Krishna College of Engineering and Technology
Coimbatore, India
[1]15epcs007@skcet.ac.in, [2]muneeswaranv@skcet.ac.in

Abstract
A Wireless Sensor Network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental condition such as temperature, sound,pressure etc. The communication delay, security and delivery ratio are the three main design issue in the wireless sensor Network.To overcome these issues a novel delay aware privacy preserving (DAPP) protocol is used. while forwarding the data to server source node may far away from the destination which leads to insecure in the network. The secret key sharing that ensures security of the collected data.This can also preserve security of location while defending against attackers the location privacy has been obtained to the users for various security purpose.Our theoretical analysisand numerical results show that the three design issues can be adjusted to meet various security and practical implementation goals.

Index Terms— Wireless sensor network (WSN), Delay aware privacy preserving ((DAPP), secret sharing,privacy preserving, location privacy.

I INTRODUCTION

Recent technological advances make the urban sensing networks technically and economically feasible to be widely used in civilian applications, such as monitoring of urban environment and patient care and many applications Urban sensing, which is known participatory sensing, relies on sensors embedded in the human-carried mobile devices or electrical devices to collect and report the sensing data. The electrical devices carried by human and vehicles are gradually replacing the traditional static sensor networks for many urban area applications. Participatory sensing networks differ from traditional wireless sensor networks.

First, participatory sensor nodes are embedded in rechargeable mobile devices, such as smart phones,i-Pads, laptops, and auto computers etc[1]. The powerful resources equipped in these devices enhance their capabilities in the sensing, data storage, reliable data communication, and energy lifetime. Hence, energy efficiency is no longer as critical as in the traditional wireless sensor networks as shown in fig 1.

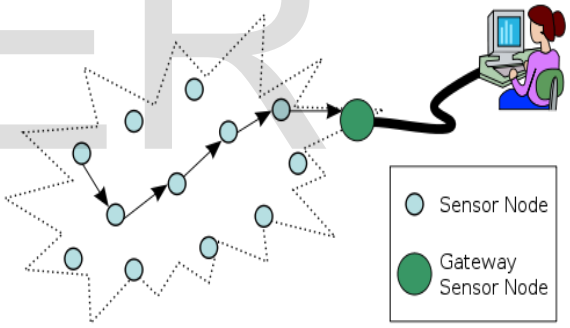

Fig.1. Wireless Communication

Second, In urban sensing networks, sensed data collection and reporting the data on no longer relyonfixed infrastructure[2]. The data can be forwarded by mobile nodes to the sink either directly or indirectly in multiple hops. Due to mobility, the networktopology structure constantly changes, which makes end-to-end communication delay, message delivery ratio, and quality of service.Third, these devices are owned and operated by individuals. Instead of being only data consumers, these devices could also collect the sensed data. It makes data collection more directly related to peoples hence, privacy becomes one of the major concerns for

participating users. In fact, the data collecting and reporting services put users since both the delivery nodes and the wireless access points (APs) are able to identify the data owner through the direct communications.

The uploaded data are collected in spatiotemporal information, which may be used to extract or infer sensitive and private information of the users. As a result, location information and side information may be correlated to recover the trajectory of participating users.

The unique nature of participatory sensing networks creates new security and performance requirements. A centralized data-forwarding scheme to preserve trajectory privacy of participating users based on the secret sharing and dynamic pseudonym. Delay-Aware Privacy Preserving (DAPP) [14] provides a design trade off framework to address security, communication delay, and the delivery ratio based on the selection of an (k, n) secret sharing scheme.

This paper is structured as follows.We provide quantitative analysis on security, communication delay, and delivery ratio based on the parameter settings and also the location privacy of the users. Our contributions in this paper can be presented as follows.

- The DAPP data-forwarding scheme is to protect the trajectory of privacy participant users in the urban sensing networks.
- A devise is to secret-sharing based secure message delivery option and that can providedata integrity verification of the recovered data and it can maximize the message delivery ratio.
- The location privacy that can be obtained by dapp forwarding scheme.
- The scheme is able to achieve a trade off among security, communication delay, and delivery ratio and the privacy of users.

II RELATED WORK

Here we using the participatory sensing [1] network to analyze the behavior of the user. The key idea for participatory sensing is that the network relies on paper carried mobile devices to collect data sensed in urban area. The main issue is the security and the communication delay by these issues we can overcome by delay aware privacy preserving network. The dapp forwarding provides an scheme to ensure the confidentiality of the data [14]. In the future work, we have include the location privacy that will helps the user to find the location [13] securely.

The location privacy that can be obtained from Location Based Service (LBS).They can be analyzed through the social sites or by several communications .It is used like to find their employees and that makes feasible. The fundamental idea is to report dummy locations to conceal the actual location of the reported data. Suppression based technique is proposed to report locations by converting database.

Encryption based algorithms[11] and data exchange schemes to store the sensed data is encrypted and to replica sensors. The replica sensors then store the received data and it upon receiving inquiries. In the Dapp privacy preserving the data can be exchanged multiple times to prevent adversaries from correlating the data and its identity.

DAPP SCHEME

In DAPP, to ensure security of the reporting data we generatedata pieces. Each data piece is then forwarded to a randomly selected delivery node. In this way, the original data can be concealed among trustworthy secret holders. The shared datacan be recovered by anyor more data pieces. Since we assume the delivery nodes may tamper with the reporting data, the application server may receive incorrect data pieces [14]. Therefore, the application data server may not be able to recover theoriginal data.

DAPP includes two phases in data forwarding. In the first phase, the generated data pieces are distributed torandom selected delivery nodes beforebeing relayed to the application server. The data source may choose to add a time interval betweentransmissions of two consecutive data pieces.

A properly selectedcan effectively control theprobability for any single delivery node to receive multiple data pieces, particularly in sparse networks. Since delivery nodes may not be

completely trusted, the integrity of the reconstructed data has to be verified.

The reconstruction algorithm follows the Barycentric Source privacy information[14]can be specified by two equally essential parts: spatiotemporal informationand identity information. Only when both are exposed that the complete privacy information is disclosed. Here, we will provide quantitative analysis that DAPP can provide both identity and spatiotemporal information from being disclosed to adversaries. We first introduce several definitions and metrics.

Query Privacy: Let the target of a query to the urban sensing system. We say that query privacy is guaranteed if any malicious adversaryhas just a negligible advantage over a random guess of the identity of queried sensor

Data Privacy: Let be the target of a query to the urban sensing system, and the owner of the corresponding sensor. We say that data privacy is guaranteed if any malicious adversary has a negligible advantage over a random guess of the reading reported .

Adversaries and Counter Measures

Today's digital society increasingly relies on the interconnection of heterogeneous componentsencompassing assorted actors, entities, systems, and a variety of (often mobile) computing devices[13].Revolutionary computing paradigms, such as people-centric urban sensing, have focused on the seamless collection of meaningful data from a large number of devices. The increasing complexity of deployed urban systems and related infrastructures, along with the growing amount of information collected, prompts a number of challenging security and privacy concerns. In this paper, we explore a number of scenarios where nodes of a urban sensing system are subject to individual queries.

In this setting, multiple users and organizations (e.g., infrastructure operators) co-exist, but they may not trust each other to the full extent[13]. As a result, we address the problems of protecting: 1) secrecy of reported data, and 2) confidentiality of query interestsfrom the prying eyes of malicious entities. We introduce a realistic network model and study different.

III PROPOSED DAPP ARCHITECTURE

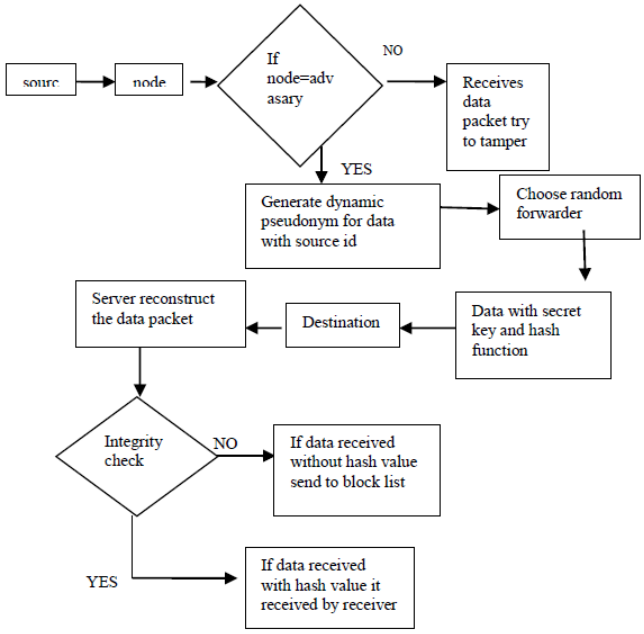

Fig. 2. DAPP architecture

In the dapp architecture diagram, the source of the data get connected to the node and then it check the node is adversary or not if it is adversary means it receives the data packet and try to tamper. if the data is correct valuable pseudonym. The pseudonym means the name or alias name which could get by the server node .if the node can check the adversary the it can generate dynamic pseudonym for the data with source id. The source id that can send with the hash function.

The data should find the random neighbour across on it. The neighbour node that can sense by the sensor and that can send the data safely to the server and it send to the respective destination . The server node reconstruct the data packet and it should verify the integrity of the node .

The verification of the neighbour node that can check by the hash function along with it.Then data can received by receiver if it get with hash value otherwise it will send to the block list. Then the performance metrics has been calculated to the node of the user that can be achieved. The three main design issues have undertaken on that the security, communication delay and the

delivery ratio that has been slightly maintained in the dapp forwarding scheme.

The proposed dapp architecture that provides the data in an secured way. It gives more accuracy in security ,less communication delay. The dapp scheme provides more security while compare to other schemes .Nowadays security is the main concern that has been analyzed by various techniques the dapp that has been sensed the data and that has been verified by many methods analyzed on them .The architecture that has been analysed by using various metric among them .

IV RESULTS

In order to evaluate the proposed dapp algorithm with realistic data flows on a simulation, we have implemented the dapp method on the data flow simulator and the network simulator NS2 Then we have conducted a simulation to confirm if the proposed dapp algorithm can select next registration node more efficiently than our previous work without delay.In the simulation environment the base station ,IOT server, and many sensors were located to sense the data that has been sent to communication for the users. The data has been send through the internet more securely with less communication delay.

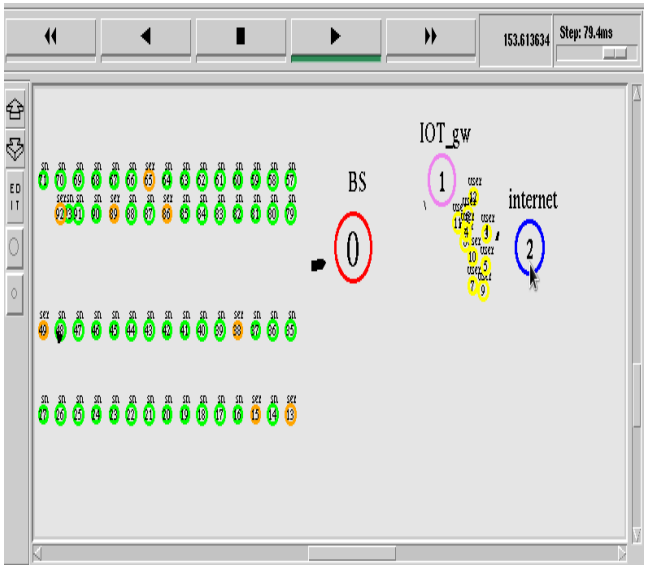

Figure 3: Data Sensing Between Users

i. Throughput (y) Vs interval(x) :

The throughput is calculated by using the AWKprogram. It is an interrupted programming language designed for text processing. The throughputs under various packet sizes are considered as CBR are: 350000, 300000, and 50000. From the graph we can conclude that the throughput and the size of CBR packets are related exponentially. As the no of users increases there is decrease in the throughput, but by using the Dapp algorithm the throughput is maintained.

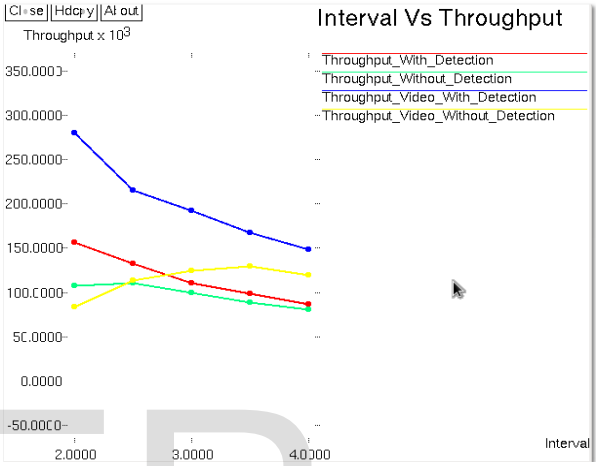

Fig .4. Interval Vs throughput

The throughput is to maximize the data moved successfully from one place to another.The interval has maintained are 20000,30000,and 40000.The throughput video with detection has increases the throughput compare to other values.The throughput with detection has increased to 1,500000 and compare to all detection throughput values the throughput without detection is maintained constant.

i. interval(x) vs jitter(y)

The jitter is calculated by using the AWK program.It is an interrupted programming language designed for text processing.The jitter under various packet sizes are considered as CBR are: 1200000, 900000, and 100000.From the graph we can conclude that the jitter and the size

of CBR packets are related exponential.

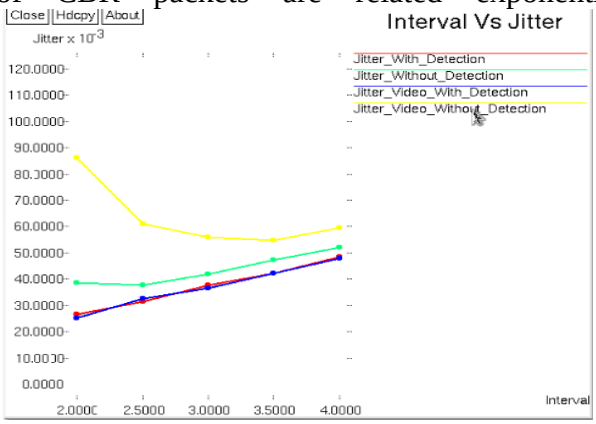

Fig .5. Interval Vs Jitter

In the jitter ,the jitter video without detection has increased the value upto 90,0000and both the jitter with detection methods have constantly maintained and that has been maintained. The jitter has maintain the value about the variation in the received packet.

V CONCLUSION

The DAPPdata-forwarding scheme for people-centric urban sensing networks. It is developed based on Shamir's secret sharing, dynamic pseudonyms, and a two-phase data-forwarding method. The two-phase forwarding method detaches the connection between the source node and the application data server[14]. Shamir's secret sharing prevents delivery nodes from discovering privacy information in the reported data. The proposed dynamic pseudonym scheme can defend against identity-based side information attack. Both theoretical analysis and simulation results demonstrate that the proposed DAPP can provide an excellentdesign trade off among security, communication delay, and delivery ratio. In thefuture work, I have add some features on the network that the message can send securely and the data can be can send in any kind of situation .

REFERENCES

[1] J. Burke et al., "participatory sensing," in proc. 1st workshop world-sensor-web, oct. 2006, pp. 1–5.

[2] A. T. Campbell, s. B. Eisenman, n. D. Lane, e. Miluzzo, and R. A. Peterson, "people-centric urban sensing," in proc. 2nd annu. Int.Workshop wireless internet, 2006, pp. 18–31.

[3] R. Du et al., "effective urban traffic monitoring by vehicular sensor Networks," ieee trans.Veh. Technol., vol. 64, no. 1, pp. 273–286,Jan. 2014.

[4] k. L. Huang, s. Kanhere, and w. Hu, "towards privacy-sensitive participatory Sensing," in proc. Ieee int. Conf. Pervasive comput. Commun., Mar. 2009, pp. 1–6.

[5] S. Gao, J. Ma, W. Shi, G. Zhan, and C. Sun, "TRPF: A trajectory privacy-preserving framework for participatory sensing," IEEE Trans. Inf.Forensics Security, vol. 8, no. 6, pp. 874–887, Jun. 2013.

[6] B. Palanisamy and L. Liu, "Mobimix: Protecting location privacy with mix-zones over road networks," in Proc. IEEE 27th ICDE, Apr. 2011,pp. 494–505.

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

[8] M. Datar, N. Immorlica, P. Indyk, and V. S. Mirrokni, "Locality-sensitivehashing scheme based on p-stable distributions," in Proc. 20th Annu.Symp. Comput. Geometry, 2004, pp. 253–262.

[9] C. Ardagna, M. Cremonini, S. De Capitani di Vimercati, and P. Samarati, "An obfuscation-based approach for protecting location privacy," IEEE Trans. Dependable Secure Comput., vol. 8, no. 1, pp. 13–27, Jan. 2011.

[10]S. Gao, J. Ma, W. Shi, and G. Zhan, "Towards location and trajectory privacy protection in participatory sensing," Mobile Comput., Appl. Services, vol. 95, pp. 381–386, 2011.

[11]H. Kido, Y. Yanagisawa, and T. Satoh, "An anonymous communication technique using dummies for location-based services," in Proc. 9th Int.Symp. PETS, 2005, pp. 88–97.

[12]E. De Cristofaro and R. Di Pietro, "Adversaries and countermeasures in privacy-enhanced urban sensing systems," IEEE Syst. J., vol. 7, no. 2, pp. 311–322, Jun. 2013.

[13]Di Tang and Jian Ren "A Novel Delay-Aware and Privacy-PreservingData-Forwarding Scheme for Urban Sensing

Network" IEEE transactions on vehicular technology, VOL. 65, NO. 4, APRIL 2016

[14]J. Kim and S. Bohacek, "A survey-based mobility model of people for simulation of urban mesh networks," in Proc. MeshNets, 2005, pp. 1– 11.