ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 16, April 2017

A Secure and Efficient Data Aggregation Scheme in Mobile Sensing System

[1] K. Raghupathi, [2] Waheeda Khanam

[1]Assistant Professor, Department of CSE, Chaitanya Institute of Technology and Science, Village Kishanpura, Mandal Hanmakonda, District Warangal, Telangana, India.

[2]M. Tech Student, , Department of CSE, Chaitanya Institute of Technology and Science, Village Kishanpura, Mandal Hanmakonda, District Warangal, Telangana, India.

ABSTRACT– ***Several privacy-protection schemes have been proposed to provide anonymity for users, and many incentive schemes have been designed to promote participation by paying credits to users. However, they address privacy and incentive separately. In particular, existing privacy preserving schemes provide anonymity for users. Anonymity may allow a greedy user to anonymously submit unlimited data reports for the same sensing task and earn unlimited credits without being detected. This will increase the cost of data collection. In this paper we propose two privacy-aware incentive schemes for mobile sensing that can support multiple report tasks. We adopt a credit-based approach which allows each user to earn credits by contributing its data without leaking which data it has contributed. At the same time, the approach ensures that malicious users cannot abuse the system to earn unlimited amount of credits.***

1. INTRODUCTION

The Wireless Mobile wireless sensor network can be simply defined as WSN with mobile as sensor nodes. These nodes consist of a radio transreceiver and a microcontroller powered by a battery. The topology used for these networks is not decided. So, routing becomes challenging job. Data Aggregation is nothing but collection of data from different resources or nodes and giving output as a summary. The aggregation statistics are normally computed periodically to analyze its pattern. The source information for data aggregators may originate from public records and databases; the information is packaged into aggregate reports and then may sell to different agencies. These reports can be used in background checks and to make some decisions. Most of the works in this consider that the aggregator is trusted. But this is not the case each time. The challenge is to protect data when the aggregator is untrusted.

All Rights Reserved © 2017 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 16, April 2017

Opportunistic sensing has been gaining reputation, with several structures and programs being proposed to leverage users' mobile devices to collectively measure social or environmental data, occasionally used as context in pervasive computing programs. In those structures, programs can task cell nodes (consisting of a user's sensor-ready mobile telephone or vehicle) in a target location to report context data from their area. In this version, the gadget opportunistically arms the mission to cellular nodes that select to take part, and the nodes record sensor statistics through opportunistic community connections (inclusive of third-party access point to factors they encounter). Examples of such systems encompass CarTel, Mobiscopes, Urbanet, Urban Atmospheres, Urban Sensing, SenseWeb, and Metrosense at Dartmouth College. Applications of opportunistic sensing consist of gathering traffic reports or pollutants readings from a specific avenue or part of a university campus, finding parking spots, finding misplaced Bluetooth-enabled items with the help of different users' cell devices, or even inferring garage area availability.

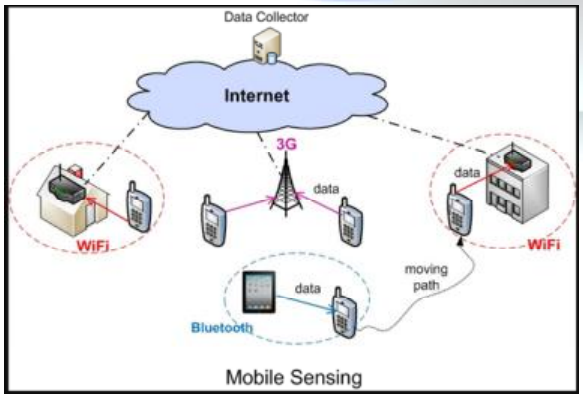

Fig1. Example for Mobile Sensing

Mobile sensing is increasingly more turning into a part of normal lifestyles because of the rapid evolution of the cellular telephone into an effective sensing platform. Popular client Smartphone are now prepared with the essential sensors to monitor a diverse range of human activities and commonly encountered contexts like GPS, digital camera, microphones. The technical challenges of mobile sensing have attracted interest from various research communities, such as experts in machine learning, human computer interaction and mobile systems, who approach this emerging field with their own perspective due to differences in their interests and expertise. Mobile sensing application relies on small number of volunteers hence data is limited. The large scale of deployment of data are affected by lack of participation of mobile users because it leads to high cost of mobile data as well as it consume much power of the device and privacy consent of user. [8] discussed about a method, This scheme investigates a traffic-light-based intelligent routing strategy for the satellite network, which can adjust the pre-calculated route according to the real-time congestion status of the satellite constellation. In a satellite, a traffic light is deployed at each direction to indicate the congestion situation, and is set to a relevant color, by considering both the queue occupancy rate at a direction and the total queue occupancy rate of the next hop. The existing scheme uses TLR based routing mechanism based on two concepts are DVTR Dynamic Virtual Topology Routing (DVTR) and Virtual Node (VN). In DVTR, the system period is divided into a series of time intervals. On-off operations of ISLs are supposed to be performed only

All Rights Reserved © 2017 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 16, April 2017

at the beginning of each interval and the whole topology keeps unchanged during each interval. But it has delay due to waiting stage at buffer. So, this method introduces an effective multi-hop scheduling routing scheme that considers the mobility of nodes which are clustered in one group is confined within a specified area, and multiple groups move uniformly across the network.

2. RELATED WORK

Dejun Yang, Guoliang Xue, Xi Fang designed incentive mechanisms that can be used to motivate smartphone users to participate in mobile phone sensing, which is a new sensing paradigm allowing us to collect and analyze sensed data far beyond the scale of what was previously possible. They considered two different models from different perspectives: the platform-centric model where the platform provides a reward shared by participating users, and the user-centric model where each user can ask for a reserve price for its sensing service.

Yoshitaka Ueyama, Morihiko Tamai, Yutaka Arakawa, Keiichi Yasumoto proposed a novel incentive mechanism based on gamification for participatory sensing. The proposed incentive mechanism uses (1) a status level scheme, (2) a ranking scheme, and (3) a badge scheme based on gamification to attract users for sensing. We formulated the problem of sensing given PoI with minimal reward points and devised a heuristic algorithm for deriving the set of requesting users and reward points for each sensing task. The algorithm requires the participation probability distribution of users and reward points.

Man Hon Cheung, Fen Hou, and Jianwei Huang studied the decisions of both the mobile users and service provider (SP) in a participatory sensing system. We first considered the participation and reporting decisions of users under a deadline reward scheme. For the general case with a time-discounted reward, we proposed an optimal participation and reporting decision (OPRD) algorithm that achieves the maximal expected surplus for each user. For the special case with a fixed reward, they derived the user's participation and reporting decisions in closed-form. Next, given the responses from the users, we considered the reward optimization of the SP, who aims to choose an optimal reward to maximize its expected surplus. Simulation results showed that the proposed OPRD algorithm achieves the highest expected user payoff as compared with the patient and impatient benchmark schemes.

3. PROPOSED SYSTEM

A. Framework of Proposed System

In this paper we propose a credit-based privacy-aware incentive system to provide limited credits to the mobile users from the collector.

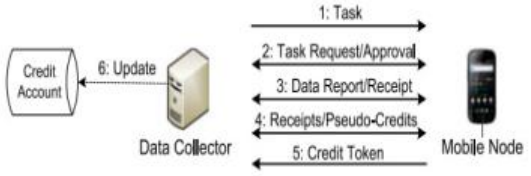

Fig2. System Framework

All Rights Reserved © 2017 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 16, April 2017

We propose two privacy-aware incentive schemes for mobile sensing that can support multiple report tasks. We adopt a credit-based approach which allows each user to earn credits by contributing its data without leaking which data it has contributed. At the same time, the approach ensures that malicious users cannot abuse the system to earn unlimited amount of credits.

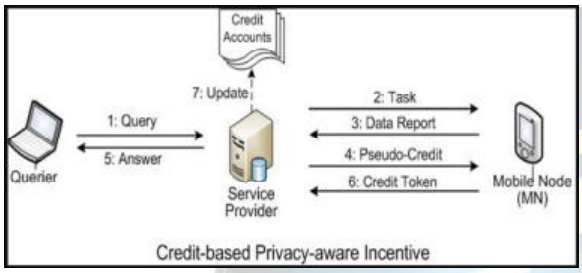

Fig3. Credit-based Privacy-aware Incentive Scheme

In particular, the first scheme is designed for scenarios where an online trusted third party (TTP) is available. It relies on the TTP to protect privacy and prevent abuse attacks, and has very low computation cost at each user. The second scheme does not require any online TTP.

B. Implementation of Credit-based Approach

With respect to privacy, our intention is to ensure that the collector cannot link any document to the reporting node, link multiple reviews submitted with the aid of the same node, recognize if a given node has common a given undertaking, or hyperlink multiple obligations typical via the equal node. With recognize to incentive, our purpose is to ensure that a node can't earn extra credit than allowed by means of our protocol. Specifically, if a node submits reviews for a task, it could earn c and best c credits (i.e., the price at which the assignment is paid) from the undertaking; if a node is not assigned the project or it does no longer submit reviews for the undertaking, it earns nothing.

C. Proposed Scheme Implementation Phases

Setup

This phase happens before any task in the task window is created. In this phase, the tokens and commitments for the task window are pre-computed and appropriately distributed to nodes and the collector.

Task assignment

Suppose a node has retrieved a task from the collector via an anonymous communication session. If the node wants to be assigned this task, it sends a request to the collector which includes its request token.

Report submission

After the node generates a report for task, it submits the report and its report token for task via an anonymous communication session. The collector verifies that the report token has been committed for task, and then issues a receipt to the node.

Receipt submission

After submitting all required reports for a task, a node waits for some random time and then submits

All Rights Reserved © 2017 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 16, April 2017

the receipts to the collector. The collector verifies the receipts, and then issues pseudo-credits to the node. From the pseudo-credits, the node can generate some credit tokens. It cannot obtain any credit token without the pseudo-credits.

Credit deposit

After a node gets a credit token, it waits for some random time and then deposits the token to the collector. The collector verifies that the token.

4. EXPERIMENTAL RESULTS

In this experiment, we are implementing two credit based approaches. While executing TTP-based approach, Trusted Third Party (TTP) and Collector will generate the Request Token, Report Token, Credit Token and Date & Time for every node which are generated by SHA algorithm.

Collector generates or displays the decrypted message and current credit value for the node. In this TTP-based approach, the tokens stored as SHA value in the collector or base station server and it display the credit value.

In TTP-Free scheme, Data collector will generate the Tokens by using SHA algorithm.

In this scheme, after submitting credit token by the node, the tokens may encrypted by the RSA algorithm. And the sensed data also stored in the form of encryption and credit value also generated by the server or collector.

5. CONCLUSION

In mobile sensing system, to provide incentive and privacy in this paper we proposed two credit-based privacy-aware incentive schemes. In this paper, to prevent abuse attacks, each node pre-determines the request token, receipts, and credit tokens that it will use to process each future task, and commits that it will use them for this task. To protect privacy, tokens and commitments are designed and used in a privacy-preserving way. Both the schemes are supported nodes join and leaves in this paper.

REFERENCES

[1] J. Hicks, N. Ramanathan, D. Kim, M. Monibi, J. Selsky, M. Hansen, and D. Estrin, "AndWellness: An open mobile system for activity and experience sampling," in Proc. Wireless Health, 2010, pp. 34–43.

[2] N. D. Lane, M. Mohammod, M. Lin, X. Yang, H. Lu, S. Ali, A. Doryab, E. Berke, T.

All Rights Reserved © 2017 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 16, April 2017

Choudhury, and A. Campbell, "Bewell: A smartphone application to monitor, model and promote wellbeing," presented at the 5th Int. ICST Conf. Pervasive Computing Technologies for Healthcare, Dublin, Ireland, 2011.

[3] M. Mun, S. Reddy, K. Shilton, N. Yau, J. Burke, D. Estrin, M. Hansen, E. Howard, R. West, and P. Boda, "PEIR, the personal environmental impact report, as a platform for participatory sensing systems research," in Proc. 7th Int. Conf. Mobile Syst. Appl. Serv., 2009, pp. 55–68.

[4] C. Cornelius, A. Kapadia, D. Kotz, D. Peebles, M. Shin, and N. Triandopoulos, "Anonysense: Privacy-aware people-centric sensing," in Proc. 6th Int. Conf. Mobile Syst. Appl. Serv., 2008, pp. 211–224.

[5] M. Shin, C. Cornelius, D. Peebles, A. Kapadia, D. Kotz, and N. Triandopoulos, "Anonysense: A system for anonymous opportunistic sensing," J. Pervasive Mobile Comput., vol. 7, no. 1, pp. 16–30, 2011.

[6] T. Das, P. Mohan, V. N. Padmanabhan, R. Ramjee, and A. Sharma, "PRISM: Platform for remote sensing using smartphones," in Proc. 8th Int. Conf. Mobile Syst. Appl. Serv., 2010, pp. 63–76.

[7] E. D. Cristofaro and C. Soriente, "Short paper: PEPSI-privacyenhanced participatory sensing infrastructure," in Proc. 4th ACM Conf. Wireless Netw. Security, 2011, pp. 23–28.

[8] Christo Ananth , P.Ebenezer Benjamin, S.Abishek, "Traffic Light Based Intelligent Routing Strategy for Satellite Network", International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST), Volume 1,Special Issue 2 - November 2015, pp.24-27.

[9] P. Gilbert, L. P. Cox, J. Jung, and D. Wetherall, "Toward trustworthy mobile sensing," in Proc. 11th Workshop Mobile Comput. Syst. Appl., 2010, pp. 31–36.

[10] K. L. Huang, S. S. Kanhere, and W. Hu, "Towards privacy-sensitive participatory sensing," in Proc. 5th Int. Workshop Sensor Netw. Syst. Pervasive Comput., 2009, pp. 1–6.

All Rights Reserved © 2017 IJARTET