

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

Implementing Improved Credit-based Approaches to Prevent Data Leakage in Mobile Sensing Systems

N.Naveen Kumar¹, Zufishan Mahveen²

Assistant Professor, Department of CSE, School of Information technology (JNTUH), Village KPHB, Mandal
Kukatpally, Dist Medchal, Telangana, India. ¹

M.Tech Student, Department of Computer Networks & Information Security, School of Information technology
(JNTUH), Village KPHB, Mandal Kukatpally, Dist Medchal, Telangana, India. ²

ABSTRACT: In Mobile sensing systems we have several problems such as; there is a lack of incentives for mobile device users to participate in mobile sensing. To participate, a user has to trigger her sensors to measure data which may consume much power of her smart phone. Traditionally, we have several credit based approaches are developed to provide data security to the mobile sensing system users. But the traditional approaches are providing unlimited credits to the user. By this reason we are getting above mentioned obstacles. To overcome these problems in this paper we propose two credit-based approaches named as TTP-based Scheme and TTP-free Scheme. These two schemes can improve the security to the mobile user and provide limited credits to the users to prevent the data leakage.

I. INTRODUCTION

Most mobile devices like sensible phones are equipped with an expensive set of embedded sensors like camera, microphone, GPS, measuring system, close light-weight sensing element, gyroscope, then on have created a large chance of sensing. This allows numerous mobile sensing applications like environmental observation, traffic observation, healthcare, then on by collection information through mobile devices and utilizing information to get made information regarding people and their surroundings. In several eventualities, aggregation statistics ought to be sporadically computed from a stream of data contributed by mobile users, to spot some phenomena or track some necessary patterns. As an example, to monitor the propagation of a replacement contagious disease and count the amount of users infected by this contagious disease ("1" if infected and "0" otherwise); However, this aggregation of statistics is hindered by obstacles. An untrusted mortal will sporadically get desired statistics over the info contributed by multiple mobile users, while not compromising the privacy of every user. To handle this drawback they style coding schemes in which the mortal will solely rewrite add of all users' information however nothing else. To rewrite add, their theme desires an additional spherical of interaction between the mortal and every one users in every aggregation amount, which implies high communication price and long delay. Also, it needs all users to be on-line until cryptography is completed, which cannot be sensible in several mobile sensing eventualities thanks to user quality and the heterogeneousness of user property. To address this drawback we tend to propose a construction that doesn't need two-way communications between the aggregator and also the users, however it's high computation and storage price to subsume collusions in an exceedingly giant system. We propose a replacement protocol for mobile sensing to get the add combination of your time series information within the presence of an untrusted mortal. Our protocol employs an additive homomorphic coding and a completely unique key management theme based on economical HMAC to confirm that the mortal will only get the ad of all users' information, while not knowing individual user' information or intermediate result. In our protocol, every user (the aggregator) only has to reckon a really small variety of HMACs to code her information (decrypt the sum). Hence, the computation price is extremely low. Another nice property of our protocol is that it solely needs one spherical of user-to-aggregator communication. Our protocols for Sum may be simply custom-made to derive several alternative combination statistics like Count and Average.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

II. RELATED WORK

2.1 Routing in Socially selfish Delay Tolerant Networks during this paper to propose a Social Selfishness Aware Routing (SSAR) algorithm to allow user selfishness and supply higher routing performance in an economical means. To select a forwarding node, SSAR considers each user's willingness to forward and their contact opportunity, resulting in a higher forwarding strategy than strictly contact-based approaches. Moreover, SSAR formulates the info forwarding process as a multiple haversack drawback with Assignment Restrictions (MKPAR) to satisfy user demands for selfishness and performance. Trace driven simulations show that SSAR allows users to maintain selfishness and achieves higher routing performance with low transmission value.

2.2 Mitigating Routing misbehavior in Disruption Tolerant Networks in this paper we propose a distributed scheme to find packet dropping in DTNs. In our scheme, a node is required to stay some signed contact records of its previous contacts, supported that following contacted node will discover if the node has born any packet. Since misbehaving nodes could misreport their contact records to avoid being detected, atiny low a part of every contact record is disseminated to a particular variety of witness nodes, which may collect applicable contact records and discover the misbehaving nodes. We also propose a theme to mitigate routing misbehavior by limiting the quantity of packets forwarded to the misbehaving nodes. Trace-driven simulations show that our solutions are economical and can effectively mitigate routing misbehavior.

2.3 Privacy-Preserving Stream Aggregation with Fault Tolerance during this paper we have a tendency to think about applications wherever associate untrusted human would like to collect privacy sensitive knowledge from users, and figure mixture statistics sporadically. For example, imagine a wise grid operator who wishes to mixture the entire power consumption of a part each 10 minutes; or a market researcher who needs to trace the fraction of population look ESPN on an hourly basis. We style novel mechanisms that enable an aggregator to accurately estimate such statistics, while providing provable guarantees of user privacy against the untrusted human; our constructions are resilient to user failure and compromise, and may with efficiency support dynamic joins and leaves. Our constructions also exemplify the clear advantage of combining applied cryptography and differential privacy techniques.

2.4 Providing Privacy-Aware Incentives for Mobile Sensing during this paper propose 2 privacy-aware incentive schemes for mobile sensing to promote user participation. These schemes enable every mobile user to earn credits by contributing knowledge while not leaking that information it has contributed, and at an equivalent time make sure that dishonest users cannot abuse the system to earn unlimited quantity of credits. The primary theme considers situations wherever a sure third party (TTP) is out there. It depends on the TTP to guard user privacy, and therefore has terribly low computation and storage value at every mobile user. The second scheme removes the idea of TTP and applies blind signature and commitment techniques to guard user privacy

III. FRAME WORK

To achieve the motivation goal that every MN will earn at most c credits from every task, our approach satisfies 3 conditions: (i) every MN will settle for a task at the most once, (ii) the MN will submit at the most one report for every accepted task, and (iii) the MN will earn c credits from a report. To satisfy the first condition, the fundamental plan is to issue one request token for each task to every MN. The MN consumes the token once it accepts the task. Since it doesn't have additional tokens for the task, it cannot settle for the task once more. Similarly, to satisfy the second condition, every MN are given one report token for each task. It consumes the token once it submits a report for the task and therefore cannot submit additional reports. To satisfy the last condition, once the SP receives a report, it issues pseudo-credits to the coverage MN which may be reworked to c credit tokens. The MN can deposit these tokens to its credit account. To achieve the privacy goals, all tokens are made in a privacy-preserving method, such asking (report) token cannot be connected to a MN and a credit token can't be connected to the task and report from that the token is attained. Thus, our approach pre computes privacy-preserving tokens for MNs that are wont to method future tasks. To confirm that MNs can use the tokens fitly (i.e., they're going to not abuse the tokens), commitments to the tokens are pre computed such that every request (report) token is committed to a selected task and every credit token is committed to a selected MN.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

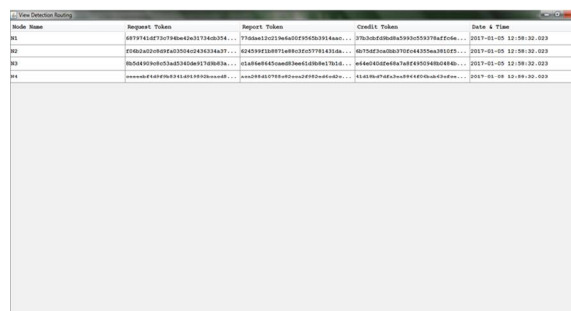
Vol. 6, Issue 7, July 2017

3.1 Scheme Overview

Following the same approach, we have a tendency to propose 2 schemes. The primary theme assumes a trustworthy third party (TTP), and uses the TTP to get tokens for every MN and their commitments. This theme depends on the TTP to guard every MN's privacy, and therefore has terribly low computation and storage cost at every MN. The second theme doesn't assume any TTP. Every MN generates its tokens and commitments in cooperation with the SP victimization blind signature and partly blind signature techniques. The utilization of blind and partly blind signatures protects the MN's privacy against attacks by any third party. Certainly, such unconditional privacy isn't free: each MN has higher computation and storage overhead. Setup during this part, the tokens and their commitments that each MN and therefore the SP can use to method ensuing M (which is a system parameter) tasks are pre computed, and distributed to each MN and therefore the SP. The distribution method ensures that each MN cannot get the report token for a task unless it is approved by the SP to accept the task, and it cannot get the credit tokens for a task unless it submits a report for the task. Task assignment suppose a MN has retrieved a task i from the SP via an anonymous communication session; If the MN decides to accept this task, it sends a request to the SP. The request includes the MN's request token. The SP verifies that the token has been committed for task i in the setup phase. If the SP allows the MN to accept this task, it returns an approval message to the MN. From the approval message, the MN can compute a report token for task i. However, the MN cannot derive a valid report token without the approval message. Report submission after the MN generates a report for task, it submits the report via another anonymous communication session. The MN's report token for task i is also submitted. The SP verifies that the report token has been committed for task i, and then sends pseudo-credits to the MN. From the pseudo-credits, the MN computes c credit tokens, where c is the number of credits paid for each report of task i. It cannot obtain any credit token without the pseudo-credits. Credit deposit After the MN gets a credit token, it deposits the token to the SP after a random period of time to mitigate timing attacks. The SP verifies that the token has been committed for the MN, and then increases the MN's credit account by one. Token and commitment renewal when the previous M tasks have been processed, the tokens and their commitments for the next M tasks should be pre computed and distributed similar to the setup part. Note that within the setup, credit deposit and token renewal phases, every MN communicates with the SP exploitation its real identity. However, within the task assignment and report submission phases, every MN uses a random name generated by it to speak with the SP. The name cannot be connected to the important identity of the MN.

IV. EXPERIMENTAL RESULTS

In our experiment, we have Trusted Third Party (TTP) and Collector and both will generate the Request Token, Report Token, Credit Token and Date & Time for every node. TTP and Collector, display the Request Token, Report Token, Credit Token and Date & Time. These are generated by the collector by using SHA algorithm. We can say these are all in the form blind signatures for all nodes. Because these are not revealed to the any node in the simulation until node gets reports from collector.



| Node Name | Request Token | Report Token | Credit Token | Date & Time |
|-----------|--------------------------------|--------------------------------|--------------------------------|-------------------------|
| n1 | 8079f1e073c79d0e2a3774d024... | 7f0bae23c51bda0f550b03914aa... | 7f0bae23c51bda0f550b03914aa... | 2017-01-01 12:30:30.003 |
| n2 | 7f0bae23c51bda0f550b03914aa... | 8079f1e073c79d0e2a3774d024... | 8079f1e073c79d0e2a3774d024... | 2017-01-01 12:30:30.003 |
| n3 | 8079f1e073c79d0e2a3774d024... | 7f0bae23c51bda0f550b03914aa... | 7f0bae23c51bda0f550b03914aa... | 2017-01-01 12:30:30.003 |
| n4 | 7f0bae23c51bda0f550b03914aa... | 8079f1e073c79d0e2a3774d024... | 8079f1e073c79d0e2a3774d024... | 2017-01-01 12:30:30.003 |

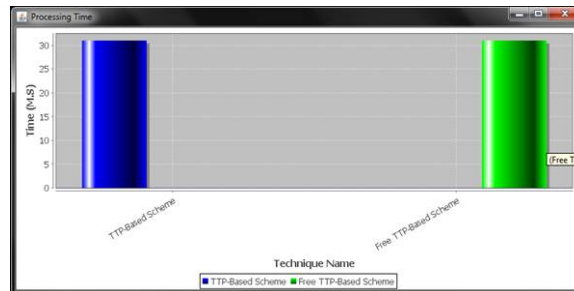
If any node sent a request task to the collector then the collector verifies his all token then Collector generates or displays the decrypted message and current credit value for the node.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017



Similarly, in TTP-Free scheme, the collector provide tokens to the nodes and those tokens will be encrypted by the collector.

V. CONCLUSION

In this paper, we proposed two credit-based approaches named as TTP-Based scheme and TTP-Free Scheme. These two schemes are achieved two goals such as privacy to the mobile device users and improving incentives in mobile sensing systems. From the experimental results we can prove that our proposed schemes are secured.

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. Mohammad, M. Lin, X. Yang, H. Lu, S. Ali, A. Doryab, E. Berke, T. 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] A. Thiagarajan, L. Ravindranath, K. LaCurts, S. Madden, H. Balakrishnan, S. Toledo, and J. Eriksson, "VTrack: Accurate, Energy-aware road traffic delay estimation using mobile phones," in Proc. 7th ACM Conf. Embedded Netw. Sens. Syst., 2009, pp. 85–98.
- [4] 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.
- [5] C. Cornelius, A. Kapadia, D. Kotz, D. Peebles, M. Shin, and N. Triandopoulos, "Anonymsense: Privacy-aware people-centric sensing," in Proc. 6th Int. Conf. Mobile Syst. Appl. Serv., 2008, pp. 211–224.
- [6] M. Shin, C. Cornelius, D. Peebles, A. Kapadia, D. Kotz, and N. Triandopoulos, "Anonymsense: A system for anonymous opportunistic sensing," J. Pervasive Mobile Comput., vol. 7, no. 1, pp. 16–30, 2011.
- [7] 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.
- [8] 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.
- [9] D. Christin, C. Rosskopf, M. Hollick, L. A. Martucci, and S. S. Kanhere, "Incognisense: An Anonymity-preserving reputation framework for participatory sensing applications," in Proc. IEEE Int. Conf. Pervasive Comput. Commun., 2012, pp. 135–143.
- [10] 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.