Incentivizing mobile crowdsensing using Bitcoin micropayments

ABSTRACT

Contribution

- Incentive mechanism for participating in mobile crowdsensing based on Bitcoin micropayments

- Discussion of the advantages of using Bitcoin in comparison to previous monetary incentive mechanisms such as Mturk (20% fees, complex process to become a worker) or credits (trust, costs, No personal sign up anywhere,..)

- Presenting an Implementation

- Evaluation and discussion of performance, security, privacy and cost (?) aspects

- Presenting opportunities and challenges for future work

1. INTRODUCTION

Crowdsensing - Participatory sensing - Opportunistic sensing - Need for incentives - Monetary Incentives - Payment infrastructure (MTURK / Pay Pal) - Bitcoin

2. RELATED WORK

2.1 Mobile crowdsensing in general

In the vast galaxy of crowdsourcing activities, crowdsensing consists in using usersâĂŹ cellphones for collecting large sets of data. In this chapter, we present the APISENSE distributed crowd-sensing platform. In particular, APISENSE provides a participative environment to easily deploy sensing experiments in the wild. Beyond the scientific contributions of this platform, the technical originality of APISENSE lies in its Cloud orientation, which is built on top of the soCloud distributed multicloud platform, and the remote deployment of scripts within the mobile devices of the participants. We validate this solution by reporting on various crowd-sensing experiments we deployed using Android smartphones and comparing our solution to existing crowd-sensing platforms. [3]

With the surging of smartphone sensing, wireless networking, and mobile social networking techniques, Mobile Crowd Sensing and Computing (MCSC) has become a promising paradigm for cross-space and large-scale sensing. MCSC extends the vision of participatory sensing by leveraging both participatory sensory data from mobile devices (offline) and user-contributed data from mobile social networking services (online). Further, it explores the complementary roles and presents the fusion/collaboration of machine and human intelligence in the crowd sensing and computing processes. This article characterizes the unique features and novel application areas of MCSC and proposes a reference framework for building human-in-the-loop MCSC systems. We further clarify the complementary nature of human and machine intelligence and envision the potential of deep-fused human–machine systems. We conclude by discussing the limitations, open issues, and research opportunities of MCSC. [2]

The ubiquity of smartphones and their on-board sensing capabilities motivates crowd-sensing, a capability which harnesses the power of crowds to collect sensor data from a large number of mobile phone users. Unlike previous work on wireless sensing, crowd-sensing poses several novel requirements: support for humans-in-the-loop to trigger sensing actions or review results, the need for incentives, as well as privacy and security. In this paper, we design and implement Medusa, a novel programming framework for crowd sensing that satisfies these requirements. Medusa provides high-level abstractions for specifying the steps required to complete a crowd-sensing task, and employs a distributed runtime system that coordinates the execution of these tasks between smartphones and a cluster on the cloud. We have implemented ten crowd-sensing tasks on a prototype of Medusa. We find that Medusa task descriptions are two orders of magnitude smaller than standalone systems required to implement those crowd-sensing tasks, and the runtime has low overhead and is robust to dynamics and resource attacks. [6] – uses Mturk for incentives/payments

2.2 Incentive mechanisms

Mobile sensing exploits data contributed by mobile users (e.g., via their smart phones) to make sophisticated infer- ences about people and their surrounding

and thus can be applied to environmental monitoring, traffic monitoring and healthcare. However, the large-scale deployment of mobile sensing applica- tions is hindered by the lack of incentives for users to participate and the concerns on possible privacy leakage. Although incentive and privacy have been addressed separately in mobile sensing, it is still an open problem to address them simultaneously. In this paper, we propose two privacy-aware incentive schemes for mobile sensing to promote user participation. These schemes allow each mobile user to earn credits by contributing data without leaking which data it has contributed, and at the same time ensure that dishonest users cannot abuse the system to earn unlimited amount of credits. The first scheme considers scenarios where a trusted third party (TTP) is available. It relies on the TTP to protect user privacy, and thus has very low computation and storage cost at each mobile user. The second scheme removes the assumption of TTP and applies blind signature and commitment techniques to protect user privacy. [4]

With the prosperity of smart devices, crowdsourcing has emerged as a new computing/networking paradigm. Through the crowdsourcing platform, service requesters can buy service from service providers. An important component of crowdsourcing is its incentive mechanism. We study three models of crowdsourcing, which involve cooperation and competition among the service providers. Our simplest model generalizes the well-known user-centric model studied in a recent Mobicom paper. We design an incentive mechanism for each of the three models, and prove that these incentive mechanisms are individually rational, budget-balanced, computationally efficient, and truthful. [7]

Recent years have witnessed the fast proliferation of mobile devices (e.g., smartphones and wearable devices) in peopleâĂŹs lives. In addition, these devices possess powerful computation and communication capabilities, and are equipped with various built-in functional sensors. The large quantity and advanced functionalities of mobile devices have created a new interface between human beings and environments. Many mobile crowd sensing applications have thus been designed, which recruit normal users to contribute their resources for sensing tasks. To guarantee good performance of such applications, itâĂŹs essential to recruit sufficient participants. Thus, how to effectively and efficiently motivate normal users draws growing attention in the research community. This paper surveys diverse strategies that are proposed in the literature to provide incentives for stimulating users to participate in mobile crowd sensing applications. The incentives are divided into three categories: entertainment, service, and money. Entertainment means that sensing tasks are turned into playable games in order to attract participants. Incentives of service exchanging are inspired by the principle

of mutual benefits. Monetary incentives give participants payments for their contributions. We describe literature works of each type comprehensively and summarize them in a compact form. Further challenges and promising future directions concerning incentive mechanism design are also discussed. [8]

2.3   Privacy

Mobile participatory sensing has opened the doors to numerous sensing scenarios that were unimaginable few years ago. In absence of protection mechanisms, most of these applications may however endanger the privacy of the participants and end users. In this manuscript, we highlight both sources and targets of these threats to privacy and analyze how they are addressed in recent privacy-preserving mechanisms tailored to the characteristics of participatory sensing. We further provide an overview of current trends and future research challenges in this area. [1]

2.4   Reputation

Participatory sensing is an emerging paradigm in which citizens everywhere voluntarily use their computational devices to capture and share sensed data from their surrounding environments in order to monitor and analyze some phenomenon (e.g., weather, road traffic, pollution, etc.). Interest in participatory sensing systems has risen since a large mobile sensor network can now be opportunistically constructed with much less cost and effort than it was the case a decade ago. However, relying on citizens who share their contributions raises many challenges. Participants can disrupt the system by contributing corrupted, fabricated, or erroneous data. Consequently, monitoring the participantsâĂŹ behavior in order to estimate their honesty is an essential requirement. This enables to evaluate the veracity and accuracy of participantsâĂŹ contributions and therefore, to build robust and reliable participatory sensing systems. Recently, several trust and reputation systems have been proposed to trace participantsâĂŹ behavior in these systems. This survey presents a study and analysis of existing trust systems in participatory sensing applications. First, we study the nature of participatory sensing applications by surveying existing systems and outlining their common features. We then analyze the main vulnerabilities and attacks that can be launched in these systems. Furthermore, we discuss the concept of trust and we introduce a classification of existing trust systems. The two main classes of trust assessment methods for participatory sensing (i.e. Trusted Platform Module and reputation) are discussed. In addition, we analyze the merits as well as the limitations of each of them. We then derive a comparative study of several existing trust systems for participatory sensing. From this study, we identify many trust problems

that have not been solved and many attacks have not been addressed yet in the literature. Finally, we list future research directions regarding trust management in participatory sensing systems. [5]

3. BITCOIN

3.1 Technical introduction

- Peer-to-peer network
- Cryptographic signing of transactions
- Blockchain, a distributed ledger based consensus by proof of work
- Structure of transactions (challenge and claiming scripts)
- But: Transaction costs, consensus process -> payments aren't instant

3.2 Important characteristics

- Ad-hoc generation of accounts by anyone and anything
- Pseudonymous
- Global: frictionless payments across boarders
- Irreversibility of payments
- But: Transaction costs, consensus process -> payments aren't instant

3.3 Instant Bitcoin micropayments

3.3.1 One-to-one payment channels

3.3.2 N-to-N mediated payment channels

4. SYSTEM DESIGN

4.1 Requirements or Features ?

- Low barrier for participation
- Focus on data provider / data provider centric
- Limit power of platform provider

4.2 Architecture

5. IMPLEMENTATION

5.1 HTLC payment client

5.2 HTLC payment server

5.3 Mobile sensing application

- Physical sensors
  - Motion
  - Acceleration
  - Magnetic Field
  - Network strength
  - Barometric pressure
  - Temperature
  - Relative humidity
  - Light
  - Cellular network strength
  - Location
- Virtual sensors
  - Wifi networks
  - Bluetooth Beacons
  - Data rate
  - Transportation mode
  - Installed apps
  - Running apps
  - Number of contacts

5.4 Querying and buying application

5.5 Hub

6. EVALUATION

6.1 Performance

- Performance of each task (query, buy, initialize payment channel..)
- Would be interesting to disintegrate cryptographic operations and network (round trip) times
- Contrast on-chain payment with off-chain payment

6.2 Security

- Security analysis of HTLC

6.3 Privacy

6.3.1 Data providers

- IP address / device id
- location
- Inference based on bought data

6.3.2 Buyers

- IP address / device id

7. DISCUSSION

7.1 Privacy

- TOR

7.2 Quality of data and fraud

- Fake phone

- Fake data

7.3 Locking of funds / Capital investment

- Hub operator needs to lock funds with every sensor

7.4 Bitcoin transaction malleability

8. FUTURE WORK

8.1 Internet of Things

- Implementation on constrained devices / sensors

- Ideal for embedded/head-less devices

8.2 Real-time data markets

8.3 Decentralized Bitcoin payment channel networks

- Duplex Payment Channels

- Lightning Network

8.4 Reputation

8.5 Preserving privacy

- Enigma

8.6 From opportunistic sensing to participatory sensing

9. CONCLUSIONS

10. ACKNOWLEDGMENTS

11. REFERENCES

[1] D. Christin. Privacy in mobile participatory sensing: Current trends and future challenges. *Journal of Systems and Software*, pages –, 2015.

[2] B. Guo, Z. Wang, Z. Yu, Y. Wang, N. Y. Yen, R. Huang, and X. Zhou. Mobile crowd sensing and computing: The review of an emerging human-powered sensing paradigm. *ACM Computing Surveys (CSUR)*, 48(1):7, 2015.

[3] N. Haderer, F. Paraiso, C. Ribeiro, P. Merle, R. Rouvoy, and L. Seinturier. A Cloud-Based Infrastructure for Crowdsourcing Data from Mobile Devices. In *Crowdsourcing*, pages 243–265. Springer Berlin Heidelberg, Berlin, Heidelberg, 2015.

[4] Q. Li and G. Cao. Providing privacy-aware incentives for mobile sensing. In *Pervasive Computing and Communications (PerCom), 2013 IEEE International Conference on*, pages 76–84. IEEE, 2013.

[5] H. Mousa, S. B. Mokhtar, O. Hasan, O. Younes, M. Hadhoud, and L. Brunie. Trust management and reputation systems in mobile participatory sensing applications: A survey. *Computer Networks*, 90:49 – 73, 2015. Crowdsourcing.

[6] M.-R. Ra, B. Liu, T. L. Porta, and R. Govindan. Medusa: A Programming Framework for Crowd-Sensing Applications. In *Proceedings of the 10th International Conference on Mobile Systems, Applications, and Services (MobiSys'12)*, June 2012.

[7] X. Zhang, G. Xue, R. Yu, D. Yang, and J. Tang. Truthful incentive mechanisms for crowdsourcing. In *Computer Communications (INFOCOM), 2015 IEEE Conference on*, pages 2830–2838, April 2015.

[8] X. Zhang, Z. Yang, W. Sun, Y. Liu, S. Tang, K. Xing, and X. Mao. Incentives for mobile crowd sensing: A survey. *Communications Surveys Tutorials, IEEE*, PP(99):1–1, 2015.