Providing Privacy-Aware Incentives in Mobile Sensing Systems

Abstract:

Mobile sensing relies on data contributed by users through their mobile device (e.g., smart phone) to obtain useful information about people and their surroundings. However, users may not want to contribute due to lack of incentives and concerns on possible privacy leakage. To effectively promote user participation, both incentive and privacy issues should be addressed. 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 credit-based privacy-aware incentive schemes for mobile sensing systems, where the focus is on privacy protection instead of on the design of incentive mechanisms. Our schemes enable mobile users to earn credits by contributing data without leaking which data they have contributed, and ensure that malicious users cannot abuse the system to earn unlimited credits. Specifically, the first scheme considers scenarios where an online trusted third party (TTP) is available, and relies on the TTP to protect user privacy and prevent abuse attacks. The second scheme considers scenarios where no online TTP is available. It applies blind
signature, partially blind signature, and a novel extended Merkle tree technique to protect user privacy and prevent abuse attacks. Security analysis and cost evaluations show that our schemes are secure and efficient.

**Existing system:**

Our previous work designs a privacy-aware incentive scheme for a special scenario of mobile sensing where each sensing task requires only one data report from each user (such a task is referred to as a single-report task). An example of single-report task is “Report the noise level around you now,” which only requires each user to submit a single data report of his measured noise level. In the real world, however, there are many sensing tasks that require multiple reports submitted at different times from each user (such task is referred to as the multiple-report task). An example of multiple-report task is “Report the noise level around you every 10 minutes in the following week.” Many other examples can be found in various mobile sensing systems. Unfortunately, that work cannot be directly extended to support multiple-report tasks, since its cryptographic construction only allows each user to earn credits from one report. Although it is possible to create one task for each report and then apply that scheme, this will induce high overhead in computation and communication, and greatly increase the complexity of task management. For example, to collect the same amount of data that the
The Master of IEEE Projects

The aforementioned multiple-report task can do, one single-report task should be created every 10 minutes, and one set of cryptographic credentials should be computed, distributed, and processed for each task.

Disadvantage:

- Schemes provide anonymity for users
- Increase the cost of data collection
- A malicious user who has compromised other users’ mobile devices can steal those users’ security credentials such as cryptographic keys and anonymously use the stolen credentials to cheat and earn as many credits as possible without being detected

Above Diagram represent System Model
Proposed system:

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. 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. It applies blind signature, partially blind signature, and an extended Merkle tree to protect privacy and prevent abuse attacks.

Advantages:

- Short running time and lower power consumption.
- Efficiently support dynamic joins

Conclusion:

To promote user participation, we proposed two credit-based privacy-aware incentive schemes for mobile sensing, corresponding to scenarios with and
without a TTP respectively. Mainly based on hash and HMAC functions, the TTP-based scheme has very low computation cost at each node. Based on blind signature, partially blind signature, and extended Merkle tree techniques, the TTP-free scheme has higher overhead than the TTP-based scheme but it ensures that no third party can break user privacy. Both schemes can efficiently support dynamic joins and leaves. Implementations show that both schemes have short running time and lower power consumption.

**Hardware Specification :**

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Floppy Drive : 44 Mb.
- Monitor : 15 VGA Colour.
- Mouse : Logitech
- Ram : 512 Mb.
- MOBILE : ANDROID
Software Specification:

- Coding Language: Java 1.7
- Tool Kit: Android 2.3 ABOVE
- IDE: Android Studio

Reference:


