Challenges and Solutions to Mobile Data Authenticity

Hassan Abbas
Department of Computer Science
University of Helsinki

Mobile Data Analytics Seminar, Spring 2016
Outline

• Motivation

• Challenges

• Solutions
  ➢ YouProve
  ➢ Trustworthy Mobile Sensing
  ➢ Reputation Based System

• Summary
Motivation

- **Participatory Sensing** is a domain in which users use their smart phones equipped with sensors (accelerometer, gyroscope) to share data with the server.

- Events occurred in Libya and Egypt were covered by the local people as professional photographers could not reach there.

- Iran Election in 2009 was also covered by the local people because of political issues.
Challenges

• **Corruption attack** signifies that the corrupted data is being provided to the server. The data can be forged or modified by using any application software.

• **On-off attack** signifies that the corrupted data is being provided to the server at random occasions.

• **Collusion attack** happens when multiple users send false data in a coordinated way.

• **Sybil attack** refers to a situation when a single entity takes multiple identities.
Solutions

• **YouProve** is a framework for verifying how data is captured and modified on a mobile device equipped with sensors.

• It uses TPM (Trusted Platform Module) which is a hardware chip that reside on a user mobile device.

• Purpose of the TPM is to ensure that the data sensed by a mobile sensor and given to the server are captured by authentic sensor device.

• To achieve this TPM provides content (software configurations) signed by its private key.
Solutions

[Diagram of a system with labeled components: App, Fidelity reducer, OS, Type-specific analysis, D, D', Untrusted, Trusted, OS says: Analyzer says: D Δ D']

YouProve
Solutions

• Trusted analyzers are embedded in device firmware and allow untrusted applications to make modifications to the data.

• YouProve logs sensor data readings when the application requests to use the sensors. If the output generated by the application is from the logged data, it invokes a respective analyzer to compare the output to the input using different computer vision libraries.

• YouProve then embed the analyzer report with the software configurations of the device in a signed fidelity certificate.
Solutions

• YouProve overcomes corruption and sybil attack.

• Latency increases from 26 to 90 seconds in booting up the device of Nexus One with 512 MB Ram.

• Generation of a fidelity certificate can be done in 30 seconds of the images ranging from $1296 \times 972$ to $2592 \times 1944$.

• Audio latency ranges between 20 seconds to 64 seconds for a maximum of 5 minute audio clip with mp3 as the audio format.

• YouProve overcomes the technology challenge but still does not adequately covers the malicious users who forged the data when capturing.
Solutions

Trusted Mobile Sensing Architecture
• **Trustworthy Mobile Sensing** is used by allowing services to verify that the data was generated by a mobile device.

• It allows the applications or platform to apply transformations at the software level before passing it to the server.

• It uses Hypervisor-based system architecture which allows two operating system to be run in isolation on the device.

• The trusted OS sends data hash and software log to the server which is authenticated by the server.

• Data hash is authenticated using public key for the application and software log is authenticated by repeating the computations.
Solutions

- Trustworthy Mobile Sensing overcomes corruption and sybil attack.

- Major flaw in the approach is that by using the hypervisor and running two virtual machines on a device can consume a lot of energy.

- It does not take into account whether the data is captured correctly or not. It assumes that the user will capture the correct data and can forge it after the data is captured.
Solutions

• **Reputation System in Mobile Sensing** allows server to determine the trustworthiness of the user data before using them further.

• It performs outlier detection to remove the incorrect data.

• The system consists of two modules:
  • Watchdog module
  • Reputation module

• The watchdog implements the outlier detection function and generating a rating for each device at one particular instance for the data.
Solutions

• The ratings are then passed to the reputation module which builds a history (long term view) of the user data.

• It eliminates corruption, On/Off and collusion attacks.

• It also addresses the issues in which the data is captured incorrectly for instance noise monitoring application.

• It is the most powerful technique to authenticate the data.
Summary

• Three different approaches have been discussed in detail which resolves the issues.
  - YouProve
  - Trustworthy Mobile Sensing
  - Reputation based system

• Every technique is evaluated critically to highlight the short comings of that particular technique in respect to usage.

• Mobile data authenticity domain is still evolving and needs more precise solutions which covers technological aspect of the mobile devices as well as address human behavior in context to prevent the forgery of the data.