Poster Abstract: Reliable People-Centric Sensing with Unreliable Voluntary Carriers

Cory Cornelius, Apu Kapadia, David Kotz, Dan Peebles, Minho Shin, Patrick Tsang
Institute for Security Technology Studies, Dartmouth College, USA

1 Introduction

As sensor technology becomes increasingly easy to integrate into personal devices such as mobile phones, clothing, and athletic equipment, there will be new applications involving opportunistic, people-centric sensing. These applications, which gather information about human activities and personal social context, raise many security and privacy challenges. In particular, data integrity is important for many applications, whether using traffic data for city planning or medical data for diagnosis. Although our AnonySense system (to be presented at MobiSys [1]) addresses privacy in people-centric sensing, protecting data integrity in people-centric sensing still remains a challenge. Some mechanisms to protect privacy provide anonymity, and thus provide limited means for accountability; data integrity becomes even more difficult to protect.

We propose SenseRight, the first architecture for high-integrity people-centric sensing. The SenseRight approach, which extends and enhances AnonySense, assures integrity of both the sensor data (through use of tamper-resistant sensor devices) and the sensor context (through a time-constrained protocol), maintaining anonymity if desired.

Our poster will include protocol details and experimental results from our prototype implementation.

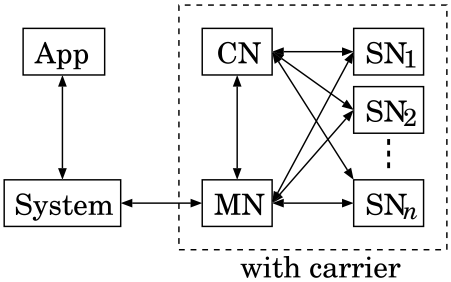
2 SenseRight

SenseRight leverages unmodified, untrusted mobile devices (such as smart phones or PDAs) carried by people who are willing to contribute sensor data (from body-area sensors) for application use. Our goal is to protect data integrity, in that the system accepts a report only if its sensor values are delivered intact from legitimate sensors (sensor-reading integrity), its sensor values are collected at a similar time (context consistency), and its values are collected under the desired condition (condition integrity). SenseRight also protects sensor values from eavesdroppers (confidentiality).

The SenseRight architecture is shown in the figure. The *system* abstracts central services that provide a task-based sensing model with the following operations: (1) an *application* (App) submits tasks to the system, (2) the system dispatches tasks to *mobile nodes* (MN), (3) the MN collects sensor readings (per the task's instructions) from *sensor nodes* (SN), and (4) the MN submits reports to the App through the system. The CN is a *certifier node* that safeguards data integrity through the SenseRight collection protocol, summarized below.

3 Protocol sketch

Overview. We imagine that the SN and CN are small, wearable mass-produced devices that have short-range wireless communications and limited computation capability, plus *tamper-resistant hardware* that makes it difficult for attackers to access their secret keys or to modify their firmware. A secure *initialization protocol* establishes a secure channel among the MN, CN, and SNs, and a secure *collection protocol* allows the CN to collect signed sensor readings from the SNs. The CN can prove the correctness of the reports through a *cryptographic signature* that only trusted CNs can generate. This three-component approach provides the desired security, privacy, and integrity properties and enables the use of off-the-shelf mobile devices with simple (cheap) sensor nodes.



Bootstrapping. The system certifies only valid, tamper-resistent CN and SN devices. The system provides each SN with a certificate that certifies the SN's public key and its list of sensors. The system provides each CN with a certificate that certifies the CN's public key for digital signature and/or group signature (for anonymous sensing).

Initialization. Prior to performing sensing tasks, the MN must have run the one-time initialization protocol. First, the MN uses SSL (Secure Sockets Layer) to authenticate the CN and establish an encrypted channel. Then, the CN uses TinySSL to authenticate each SN and establish an encrypted channel. Finally, the CN generates a fresh encryption key for each SN and securely distributes it to the SN and the MN.

Sensing. As specified by the task, the MN periodically requests readings from the SNs and tests a task-specific condition. When the condition is met, the MN asks the CN to collect sensor data within a task-specified deadline time Δ. The CN then collects and verifies sensor data from the SNs, then prepares a signed message containing the collected values, elapsed time, and task id.

Reporting. The MN, receiving signed data from the CN, reports to the system whenever an Internet connection becomes available. For each report, the system verifies that (1) the signature matches the message and uses a system-certified signature key, (2) the report includes all required sensor values, (3) the values meets the sensing condition, and (4) the elapsed time is short (less than Δ).

4 References

[1] C. Cornelius, A. Kapadia, D. Kotz, D. Peebles, M. Shin, and N. Triandopoulos. Anonysense: Privacy-aware people-centric sensing.

Proceedings of the International Conference on Mobile Systems, Applications, and Services (MobiSys), ACM, June 2008.