Security & Privacy for Urban Sensing Systems

Stylianos Gisdakis, Thanassis Giannetsos, Panos Papadimitratos

Networked Systems Security Group `http://www.ee.kth.se/nss`

Electrical Engineering - KTH

Introduction: Urban Sensing Systems

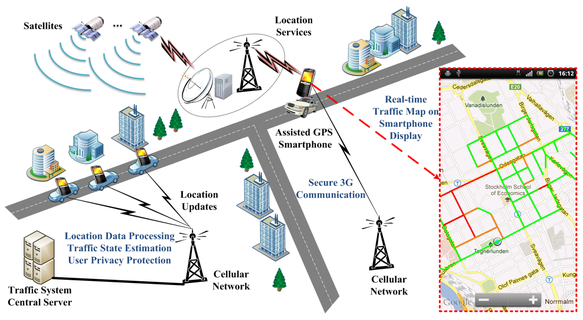

Figure 1: Crowd-sourced ITS

The capabilities of widespread mobile devices have paved the way for Urban Sensing Systems. This emerging paradigm enables direct user involvement in possibly large-scale and diverse data collection and sharing. Unavoidably, this raises significant privacy concerns, as participants may inadvertently reveal a great deal of sensitive information.

However, ensuring user privacy, e.g., by anonymizing data they contribute, may cloak faulty (possibly malicious) actions. Thus, urban sensing systems systems must not only be privacy-preserving but also accountable and reliable.

Challenges: *Protecting the system from the users and the users from the system.*

Protecting the system from the users and the users from the system

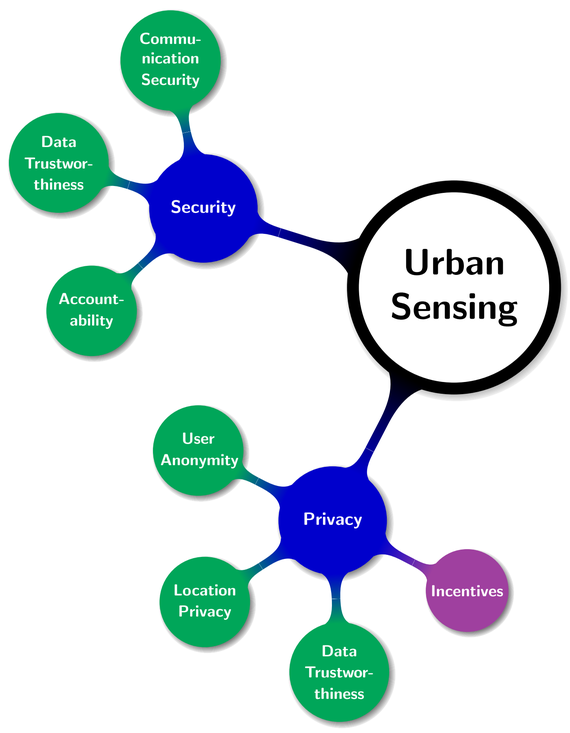

Figure 2: Security & Privacy Requirements

- Communication integrity, confidentiality and authentication
- Authorization & Access Control
- Non-repudiation & Accountability
- Anonymity & Unlinkability
- Data trustworthiness - User Remuneration

SPPEAR

Figure 3: SPPEAR Overview

- Security & Privacy architecture
- Scalable, dependable and applicable to any type of PS application
- Guarantees user non-identifiability and offers strong privacy protection
- Shuns out offending users without, necessarily, revealing their identity
- Formally verified security and privacy guarantees

SPPEAR Evaluation

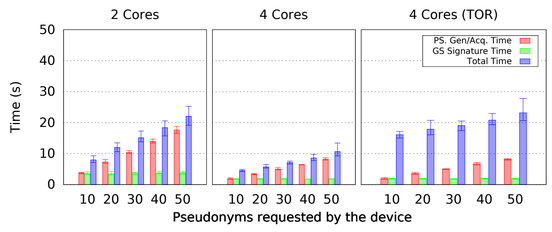

Figure 4: Authentication and Pseudonym Acquisition

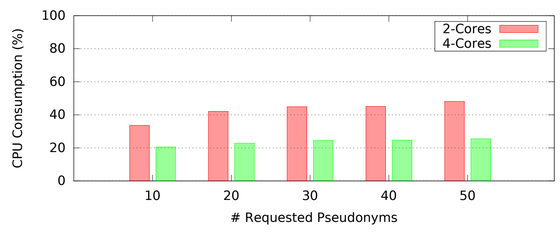

Figure 5: CPU consumption (mobile client)

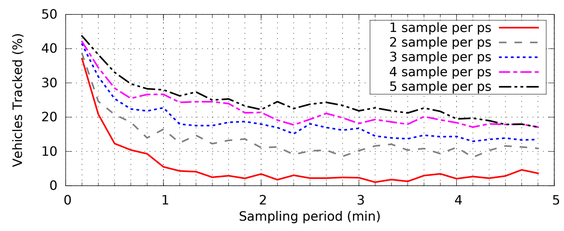

Figure 6: Privacy-protection of pseudonyms

Data trustworthiness?

- Malicious users might *pollute* the data collection process:
  - Claim congestion or traffic jams in the context of traffic monitoring campaigns
  - Suppress pollution alerts for environmental monitoring tasks
- Distort the system perception of the sensed phenomenon
- Assess the contributions of users
- Sift malicious contributions
- Remunerate and incentivize participation

SHIELD

Figure 7: SHIELD Overview

- Data-trustworthiness framework that leverages ML techniques to assess user-submitted data and sift malicious contributions
- Privacy-preserving incentive provision mechanism
- Resilient to dishonest users, Dolev-Yao adversaries and honest-but-curious and information sharing system entities

SHIELD Evaluation

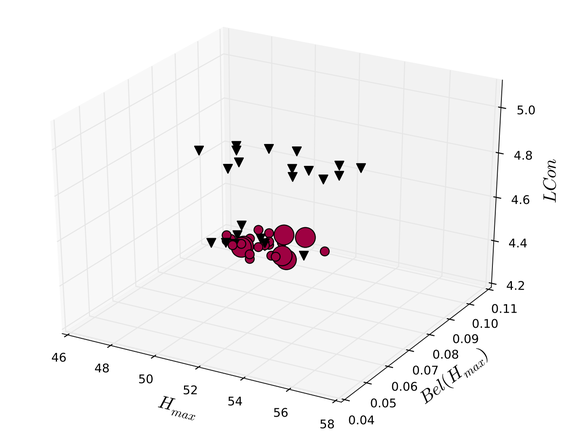

Figure 8: Clustering User Reports

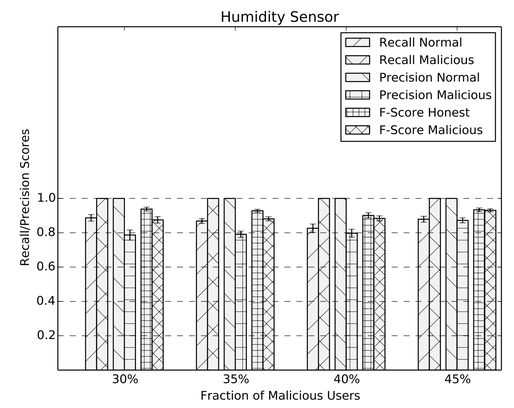

Figure 9: System Accuracy

References

[1] S. Gisdakis, V. Manolopoulos, S. Tao, A. Rusu, and P. Papadimitratos. **Secure and Privacy-Preserving Smartphone based Traffic Information Systems, IEEE Transactions on Intelligent Transportation Systems** - 2014.

[2] T. Giannetsos, S. Gisdakis, and P. Papadimitratos. **Trustworthy People-Centric Sensing: Privacy, security and user incentives road-map, Ad Hoc Networking Workshop (MED-HOC-NET)** Piran, Slovenia, 2014.

[3] T. Giannetsos, S. Gisdakis, and P. Papadimitratos. **SPPEAR: security & privacy-preserving architecture for participatory-sensing applications, ACM conference on Security and privacy in wireless & mobile networks** Oxford, UK, 2014.

[4] T. Giannetsos, S. Gisdakis, and P. Papadimitratos. **SHIELD: a Data Verification Framework for Participatory Sensing Systems, ACM conference on Security and privacy in wireless & mobile networks** NY, USA, 2015.