

## WASP Project Course 2021

# Secure & Privacy-Preserving Participatory Sensing of Wireless Interference

## Background

Wireless communication, whether unidirectional or bidirectional, can be easily disrupted, especially when it is easy to interfere legitimate transmissions, causing a denial of service, or degradation of the communication quality (e.g., lower data rates). One option to manage interference or counter jammers is to map the environment, towards detecting the affected area. Such information can be used to remove the source of interference and network disruption, or before this is possible, warn users. This can be crucial for a broad gamut of systems and applications that rely on uninterrupted, reliable and good quality connectivity. Having timely information on disruptions and outages can be an important dimension of public well-being and safety.

The challenge lies in how to collect such information - if network infrastructure is available, e.g., base stations or access points or road-side units, they can perform each their own detection of interference. However, it is necessary to detect degradation on the side of users, which may not be perceived by the network infrastructure. Or, more broadly, it is the quality of communication/networking the users get that is important.

Participatory sensing, or mobile crowd sensing, can be invaluable: users perform their own measurements (interference, communication quality) and they can contribute such data in real-time. A server can collect this data and detect the affected area. However, it is not straightforward to ensure the security of the data collection and reassure the contributing users that their privacy is safeguarded. This is what this project plans to achieve: create a demonstrable system that, in a secure and privacy preserving manner collects data from participating users' devices, and detect interference and network degradation.

## Participants

**Industrial partner:** TBD

**Industrial supervisor:** TBD

**Academic supervisor:** Prof. Panos Papadimitratos, papadim@kth.se, Networked Systems Security Lab, KTH Royal Technical

**Coordinating WARA representative:** Jesper Tordenlid, Emma Jonsson, WARA-PS

**Suggested WASP PhD students:** Cihan Eryonucu, Marco Spanghero; more are most welcome.

## Challenges to investigate

- Collection of interference measurements in the system/band of interest (e.g., WiFi, Cellular).
- Collection of measurements on communication/connectivity quality.
- Aggregation of geo- and time-stamped collected data at a server, when collecting devices have network access and can reach the server.
- Secure and privacy-preserving aggregation of the collected data
  - Ensure that only ‘approved’ participants submit data, which are not modified en-route
  - Ensure that the aggregation service cannot
  - Assess the quality of the data at the server and reject inconsistent/faulty
- Creation of a dynamically updated map of interference/quality of connectivity
- Secure and privacy-preserving provision of location-based updates to users querying for data or having subscribed for alerts.

## Resources

Networked Systems Security Lab space and equipment, in conjunction with WARA-PS platforms/facilities and premises.

## Deliverables

- Implementation and evaluation of components as per the ‘challenges’ bullet list.
- Small scale campaign for data collection, with controlled environment.
- Simple demonstration.

## References

H. Jin and P. Papadimitratos, “Resilient Privacy Protection for Location-Based Services Through Decentralization,” *ACM Transactions on Privacy and Security (ACM TOPS)*, vol. 22, no. 4, pp. 21:1--36, September 2019

S. Gisdakis, T. Giannetsos, and P. Papadimitratos, “Security, Privacy, and Incentive Provision for Mobile Crowd Sensing Systems,” *IEEE Internet of Things Journal (IEEE IoT)*, vol. 3, no. 5, pp. 839--853, October 2016.

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 (IEEE ITS)*, vol. 16, no. 3, pp. 1428--1438, 2015

S. Gisdakis, T. Giannetsos, and P. Papadimitratos, "SHIELD: A Data Verification Framework for Participatory Sensing Systems," in *ACM Conference on Security & Privacy in Wireless and Mobile Networks (ACM WiSec)*, New York, NY, USA, June 2015

## **Keywords**

Security; privacy; wireless systems; interference; network quality of service; location based services; data collection, quality and analytics.