Focus Project: User-Controlled Wireless Privacy via Client-Oriented De-Identification

Project Objectives: This project addresses the challenge of strengthening control over location privacy for users of wireless devices such as smart phones.

Technology Rationale: As mobile devices and their network services continuously monitor our environment, they enable many novel applications with tremendous societal benefits. However, they also raise significant privacy challenges by making it difficult for users to control when information about their whereabouts can be sensed or revealed. To address this challenge, this project studies the hitherto relatively unexplored concept of incorporating a comprehensive set of de-identification techniques into clients, which limits device-specific information that could allow extended tracking and eventually identification of the device's user.

Technical Approach: This project aims to establish the theory, protocols, and practical guidelines for protecting wireless privacy through de-identification.

1. The establishment of a framework and quantitative models for the evaluation of location privacy risks.

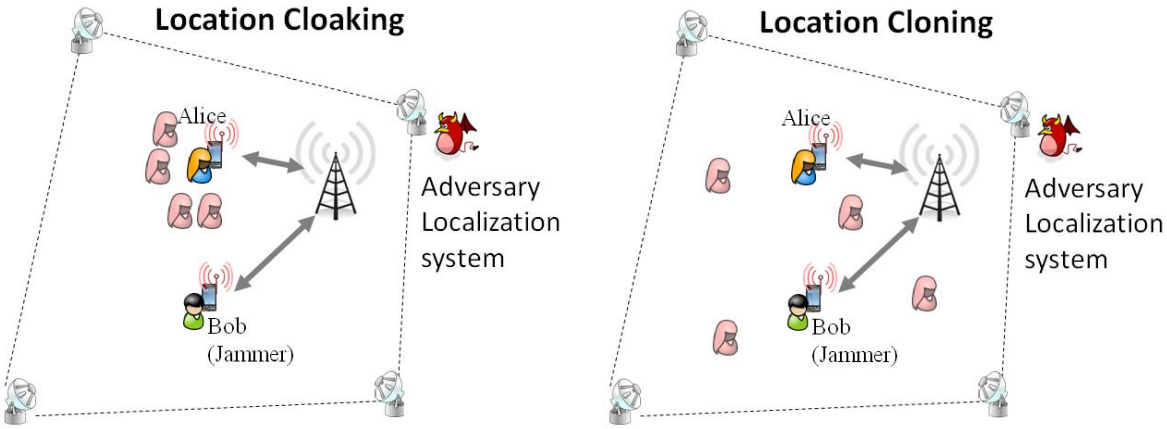
2. Protocol design that allow communication with wireless devices while limiting third-party location tracking risks, particularly at the physical layer.

3. Privacy tool design that provides users with feedback about their level of privacy based on their usage patterns of wireless devices.

4. Prototype system design that integrates these techniques into a commonly used wireless application such as mobile phone based traffic monitoring.

5. The development of a curriculum for mobile network systems and to conduct outreach activities that engage high school students and attract more students, particularly from under-represented groups, to the engineering profession.

Results to Date and Future Work Plan: Wireless users are vulnerable to attacks from adversaries using various passive localizations techniques. The adversaries can infer the location of wireless users by measuring time-of-arrival (TOA) or received signal strength (RSS) [1,2,3] from their signals at the physical layer. To defer the adversary tracking, we propose two novel techniques of **Location Cloaking** and **Location Cloning**.



Location Cloaking: It exploits the positive effects from jammers to hide the location information of wireless users. By transmitting noise-like jamming signals from a number of cooperative nodes in vicinity, Location Cloaking prevents adversaries from precisely localizing wireless users. Although stronger

jamming signal provides better privacy, such high power jamming can significantly degrade the network performance. Hence, we design privacy friendly coordination protocol for Location Cloaking so that the cooperative jammers coordinate their jamming powers properly to improve the location privacy while considering the network throughput efficiency.

Location Cloning: It thwarts the adversary's location tracking by creating a number of forged ghost locations via synchronized cooperative transmissions. Location Cloning also leverages neighboring users in creating a number of cloned ghost locations by synchronously transmitting dummy packets having same identity with users. The synchronized signal from multiple nodes is combined at the adversary sensors, which leads their tracking algorithm to faked ghost locations. In this research, we design a coordination protocol for the synchronized transmission of packets for ghost creations, and make a technical feasibility test using software-defined radios (GNU Radios) [4]. We are planning to show how much such ghost nodes can improve user location privacy through indoor test experiments.

References

[1] P. Bahl and V. N. Padmanabhan. RADAR: An in-building RF-based user location and tracking system. In Proc. of IEEE Computer and Communications Societies (INFOCOM), Tel Aviv, Israel, 2000.

[2] P. Chen. A cellular based mobile location tracking system. In Proc.of Vehicular Technology Conference, volume 3, pages 1979–1983, jul 1999.

[3] L. Doherty, K. Pister, and L. El Ghaoui. Convex position estimation in wireless sensor networks. In Proc. of IEEE Computer and Communications Societies (INFOCOM), volume 3, pages 1655–1663. Citeseer, 2001.

[4] http://gnuradio.org/redmine/wiki/gnuradio.

Contact:

Prof. Marco Gruteser