NeTS-NOSS: PARIS: A Framework for Privacy Augmented Relaying of Information from Sensors

PI: Wade K. Trappe
Co-PI: Yanyong Zhang

PROJECT SUMMARY

Over the past few decades, progress in wireless technologies and distributed computing has initiated a shift in the purpose for which networks are used. As the utility of affordable and power-efficient sensors is realized, it is expected that a broad spectrum of remote-sensing applications will emerge. These sensor-driven applications will have a significant impact not only commercially by providing strategic and timely data, but will also lead to radical social changes as sensors will become integrated in our daily lives and will be essential to how we make decisions. Due to the fact that sensor networks will affect our social fabric, one of the most notable challenges looming on the horizon and threatening successful deployment of sensor systems is privacy.

Providing privacy for sensor networks is complicated by the fact that sensor networks consist of affordable, readily-available, low-power radio devices. As a result of the availability of the underlying sensor technology, adversaries will be able to gain access to communications between sensor nodes. A first line of defense for protecting sensor communications involves employing cryptography. However, these methods cannot address the complete spectrum of privacy issues that will arise in sensor networks. Specifically, security solutions are inadequate for protecting the privacy of contextual information surrounding a sensor application, such as the source’s location, or the time at which a measurement was made, or even the size of sensor data packets.

This proposal presents a coordinated effort by two faculty members at the Wireless Information Network Laboratory (WINLAB) of Rutgers University to tackle the problem of privacy in networks of sensors. The research component of this proposal will develop a suite of privacy solutions, called the Privacy Augmented Relaying of Information from Sensors (PARIS) framework. PARIS addresses the following critical contextual privacy topics for sensor networks:

- **Source Location Privacy:** The physical or virtual location of communication participants may be sensitive information that is undesirable for an adversary to know.

- **Temporal Privacy:** Paired with the location of the data source is the time at which the data was created. Together, the availability of spatial and temporal information to an adversary constitute a serious privacy breach as this information allows an adversary to track the information origin.

- **Data Size/Traffic Privacy:** The size of a message can allow an adversary to infer many things. Although an adversary might not be able to decrypt sensor messages, by observing the size of the packets and the amount of traffic crossing the sensor network, he might be able to deduce information about the situation in which the data was generated.

The proposed research takes the viewpoint that the existing networking stack can be suitably modified to protect privacy for sensor communications. Since sensors are low-powered devices, the proposed investigations will carefully examine tradeoffs that exist between improved privacy preservation and resource-efficiency.

**Intellectual Merit:** The task of protecting the privacy associated with a sensor application’s context is complicated by the fact that existing privacy solutions, such as those used on the Internet, do not address the complete spectrum of privacy issues that arise in sensor networks, and are too resource-intensive to be deployed on sensor devices. The intellectual merits of the proposed activities are primarily targeted at uncovering sensor specific privacy issues, and developing efficient and effective contextual-privacy solutions for networks of sensors. In order to develop a robust and effective strategy for protecting the privacy of sensor communications, the proposing team takes the viewpoint that a theory-meets-systems strategy is necessary since systems-level issues will play a critical role in any deployed solution, while the theoretical attacks of today are often the realizable attacks of tomorrow. By combining theoretical models and systems implementations, the results will be synergistic, providing insights that would not have been available by either a theoretical or a systems approach alone.
**Broader Impact:** The broader impact resulting from the proposed activities is reflected by the fact that the research and education programs each provide a different angle for facilitating the deployment and adoption of sensor systems. In particular, due to the fact that sensor networks promise to have broad-reaching social and economic impact, it is critical that the challenge presented by various privacy threats is addressed before sensor systems become a communal asset. The proposed research program will remove this hurdle by developing and validating a suite of privacy solutions that address a targeted set of privacy threats. As part of the validation effort, this project will implement several software modules on the ORBIT wireless networking testbed, and will make this software available for other researchers to build upon. The proposed educational component seeks to make today’s students competitive in the future information technology workforce by giving students the tools needed to face the rapidly changing environment that is arising from advancements in sensor networking. This will be accomplished by introducing curricula that teaches students about the technology and social issues underlying sensor networks, security and privacy, as well as by encouraging undergraduate students to participate in the proposed research program.