CPS: Medium: Secure Computing and Cross-Layer Anomaly Detection in the Internet of Things

Submitted by Soummya Kar on Mon, 05/06/2019 - 5:18pm

Project Details

Lead PI:	Soummya Kar
Co-PI(s):	Jose Moura Swarun Kumar
Performance Period:	01/01/19 - 12/31/21
Institution(s):	Carnegie-Mellon University
Sponsor(s):	National Science Foundation
Award Number:	1837607

372 Reads. Placed 482 out of 803 NSF CPS Projects based on total reads on all related artifacts.

Abstract: This project tackles the following question: "Can a network of mutually-distrusting devices perform resilient inference and computation while detecting anomalous behaviors despite heterogeneity in the types of data they sense, the networking technologies they use and their computational capabilities?" The context is the increasingly pervasive Internet of Things (IoT) with low-power end users or sensors relying on edge devices to process their data, and possibly the cloud. However, IoT brings forth a unique challenge, namely, the extreme heterogeneity at multiple levels: data sensed, communication technologies used (WiFi, Bluetooth, Zigbee), and computational capabilities, making it particularly vulnerable to security threats. The goal of this project is to develop a resilient IoT system and applications, with a focus on distributed inference and computing in the presence of threats, from injection of anomalous data to impersonation of the sensors themselves. The system will be demonstrated at scale through a heterogeneous and sensor-rich campus-scale IoT deployment. The proposed testbed offers a rich platform to engage Masters and undergraduate students as well as high-schoolers through outreach programs at the Carnegie Mellon University, e.g., Engineering@CMU, SPARK Saturday, and Project Ignite. Specifically, the project aims to develop novel methodological foundations and a cross-layer system design for secure distributed computing and inference and anomaly detection in the IoT. The proposed approach exploits heterogeneous sensing data at the end-user agents and their interaction with edge devices, to provide resilience to broad classes of Byzantine adversarial scenarios and Sybil attacks. The proposed distributed algorithms yield guarantees on attaining desired computation and inference objectives under broad conditions on the data and sensing models

and inter-agent connectivity. To defend against Sybil attacks that violate standard assumptions for Byzantine fault tolerance, the project aims to develop a technology-agnostic wireless fingerprinting based solution to detect anomalous devices and transmissions. The proposed solution involves a novel design of a deep neural network to extract wireless fingerprints cutting across radio technologies.

Related Artifacts

Other

- Secure Computing and Cross-Layer Anomaly Detection in the Internet of Things | Download