On Securing Networked Real-Time Embedded Systems

Kang G. Shin

Department of Electrical Engineering and Computer Science
The University of Michigan
Ann Arbor, MI 48109-2121, U.S.A.
kgshin@umich.edu

Abstract. There has been an exponential growth of applications that rely on diverse types of embedded real-time end systems and devices, such as smart phones, play stations, home appliances, consumer and industrial electronics, smart sensors and actuators. These applications require diverse types of Quality-of-Service (QoS) including timeliness, dependability, security and privacy, from the end systems/devices which are usually networked together via heterogeneous networking technologies and procotols.

We now know how to guarantee timeliness and, to a lesser extent, how to provide fault-tolerance, on both end systems and their interconnection networks. However, how to secure them is far less known, despite the growing importance of protecting information stored in the end systems/devices and exchanged over their interconnection networks. Morever, timeliness, fault-tolerance, security and privacy—which I will call simply QoS—must be supported simultaneously, often with a tight resource budget such as memory, computation and communication bandwidth, and battery power. Also, different applications require different combinations of QoS components, and hence, one-fits-all solutions are not acceptable.

This talk will start with generic aspects of QoS and then detail how to secure a sensor network for surveillance applications. Sensor networks, usually built with a large number of small, low-cost sensor devices, are characterized by their large-scale and unattended deployment that invites many critical attacks, thereby necessitating high-level security support for their intended applications and services. However, making sensor networks secure is challenging due mainly to the fact that sensors are battery-powered and it is often very difficult to change or recharge their batteries. To meet this challenge, we have been developing Lightweight Security Protocols (LiSP) that cooperatively build a unified, energy-efficient security framework for sensor networks.