Resilient Wireless Sensor Networks for Cyber-Physical Systems

Waseem Abbas, Aron Laszka, and Xenofon Koutsoukos

Vanderbilt University, Nashville, TN 37212

Abstract

Due to their low deployment costs, wireless sensor networks (WSN) may act as a key enabling technology for a variety of spatially-distributed cyber-physical system (CPS) applications, ranging from intelligent traffic control to smart grids. However, besides providing tremendous benefits in terms of deployment costs, they also open up new possibilities for malicious attackers, who aim to cause financial losses or physical damage. Since perfectly securing these spatially-distributed systems is either impossible or financially unattainable, we need to design them to be resilient to attacks: even if some parts of the system are compromised or unavailable due to the actions of an attacker, the system as a whole must continue to operate with minimal losses. In a CPS, control decisions affecting the physical process depend on the observed data from the sensor network. Any malicious activity in the sensor network can therefore severely impact the physical process, and consequently the overall CPS operations. These factors necessitate a deeper probe into the domain of resilient WSN for CPS. In this chapter, we provide an overview of various dimensions in this field, including objectives of WSN in CPS, attack scenarios and vulnerabilities, notion of attack-resilience in WSN for CPS, and solution approaches towards attaining resilience. We also highlight major challenges, recent developments, and future directions in this area.

1 Introduction

A wireless sensor network is a collection of sensor devices organized into a wireless network. Traditionally, wireless sensor networks have been used as cost-effective means of monitoring spatially-distributed processes and phenomena. Their potential applications include military applications, such as battlefield surveillance and chemical attack detection, environmental applications, such as forest-fire detection and precision agriculture, and health applications, such as monitoring human physiological data [1].

A cyber-physical system is an integrated system of computational elements and physical processes, in which the physical processes are controlled by the computational elements [2]. Since the computational elements must have reliable information about the evolving state of the physical processes in order to control them, every practical cyber-physical system has to include sensor devices. These sensor devices monitor the physical processes, providing the computational elements with information that can be used for various tasks, such as state estimation and fault identification.
Finally, the output of the computational elements is fed into actuator devices that can influence the physical processes in the desired way, which closes the loop between the physical and cyber parts of the system.

In the case of spatially-distributed physical processes, however, the sensing task can prove to be challenging, as the sensor devices may need to be deployed over a larger area. For example, in order to provide intelligent traffic control for a whole city, we must have reliable information about the current traffic situation in various parts of the city. In order to have such information, we must deploy a large number of traffic sensors over vast area. With wired sensors, the cost of deployment could be prohibitively high and in some cases, it may even be physically or legally impossible. Consequently, wireless sensor networks, whose deployment is much simpler and more cost-effective, may act as a key enabling technology for spatially-distributed cyber-physical systems.

The rest of the chapter is organized as follows: In the remainder of this section, we illustrate the role of WSN in the context of CPS along with information-security goals in CPS. In Section 2 various applications of WSN for CPS are stated along with examples. An overview of different attack scenarios and vulnerabilities in WSN along with instances of such attacks in practical networks is provided in Section 3. In Section 4 the notion of attack-resilience in WSN is discussed along with the modeling issues and related challenges. Different approaches towards making WSN resilient against attacks, as well as a couple of detailed examples, are presented in Section 5. Finally, some future directions in this field are outlined in Section 6.

1.1 Cyber-Physical Systems and Sensor Networks

![Diagram](image)

**Figure 1:** Wireless sensor networks for monitoring and surveillance applications.

**Monitoring and Surveillance Applications** Traditional sensor network applications focus on acquiring, transmitting, and fusing data. In these applications, the physical and cyber parts do not form a closed loop, or in some cases, form a closed loop which includes human element. See Figure 1 for a simple illustration of the system architecture of such applications.

For example, in a typical habitat-monitoring application, sensors measure environmental properties, such as light, temperature, humidity, and barometric pressure, and transmit their data through the sensor network to a gateway. Then, the gateway transmits the data through a transit network to a base station, which provides WAN connectivity. Finally, the processed data is
displayed on a user-friendly interface to scientists. As another example, in a forest-fire surveillance application [4], sensors collect temperature, humidity, and illumination data and transmit it through the sensor network to a gateway node. The gateway node then forwards the data to a middleware, which stores the measurements in a database server and calculates forest-fire risk-levels from real-time and historical data. Finally, the results are displayed in a web application and if a forest fire is detected, alarms are automatically sent to fire stations or nearby residents.

![Figure 2: Wireless sensor networks for cyber-physical systems.](image)

**Cyber-Physical Systems** In cyber-physical systems, on the other hand, physical processes and computational elements are tightly integrated: physical processes, sensors, controllers, and actuators form a closed loop. Note that cyber-physical systems can still be supervised by human operators; however, there is a closed, real-time control loop which does not contain a human element. See Figure 2 for a simple illustration of the architecture of cyber-physical systems using wireless sensor networks.

Since sensor networks in cyber-physical systems are part of closed, real-time control loops, ensuring their security is more critical than in traditional sensor-network applications. In a CPS, malicious sensor data will result in incorrect control decisions, which are immediately executed by the actuators. Consequently, an attacker who has compromised a sensor network has some level of control over the physical process and may cause physical damage or financial losses using malicious control. For example, in a smart electric grid, an attacker who can tamper with real-time power-consumption data may be able to cause physical damage by simulating a rapid increase in consumption.

Therefore, security is a crucial issue for wireless sensor networks in cyber-physical systems. In the following subsection, we summarize the traditional goals of information security and how they can be applied to cyber-physical systems. For a general overview of WSN in CPS, we refer readers to the other book chapters and a survey of Wu et al. [5].

1.2 Information-Security Goals and Cyber-Physical Systems

Traditionally, the three key goals of information security are confidentiality, integrity, and availability (CIA). For cyber-physical systems, however, these properties are often listed in reverse order to emphasize that in many CPS, availability and integrity requirements have priority over the confidentiality objective [6 7].
Pages 4 to 21 are not part of this preview.
Acknowledgment

This work was supported in part by the National Science Foundation under Award CNS-1238959.

References


23


