Chapter 14

SECURITY IN SENSOR NETWORKS: WATERMARKING TECHNIQUES

Jennifer L. Wong
University of California, Los Angeles
Los Angeles, CA 90095
jwong@cs.ucla.edu

Jessica Feng
University of California, Los Angeles
Los Angeles, CA 90095
jessicaf@cs.ucla.edu

Darko Kirovski
Microsoft Research
Redmond, WA 98052
darkok@microsoft.com

Miodrag Potkonjak
University of California, Los Angeles
Los Angeles, CA 90095
miodrag@cs.ucla.edu

Abstract

The actual deployment of the majority of envisioned applications for sensor networks is crucially dependent on resolving associated security, privacy, and digital rights management (DRM) issues. Although cryptography, security, and DRM have been active research topics for the last several decades, wireless sensor networks (WSN) pose a new system of conceptual, technical, and optimization challenges.

In this Chapter we survey two areas related to security in WSN. First, we briefly survey techniques for the protection of the routing infrastructure at the network level for mobile multi-hop (ad-hoc) networks. Secondly, we discuss
the first-known watermarking technique for authentication of sensor network data and information. We conclude the Chapter by providing a short discussion of future research and development directions in security and privacy in sensor networks.

Keywords: Wireless sensor networks, Security, Privacy, Digital Rights Management

14.1 INTRODUCTION

Wireless ad-hoc sensor networks (WSN) are distributed embedded systems where each unit is equipped with a certain amount of computation, communication, storage, and sensing resources. In addition each node may have control over one or more actuators and input/output devices such as displays. A variety of applications for sensor networks are envisioned, starting from nano-scale device networks to interplanetary scale distributed systems. In many senses, WSN are a unique type of systems which have unique technical and operational challenges. Among these, security and privacy are most often mentioned as the key prerequisite for actual deployment of sensor networks.

There are at least three major reasons why security and privacy in WSN is such an important topic. The first one is that sensor networks are intrinsically more susceptible to attacks. They are often deployed in uncontrolled and sometimes even hostile environments. Wireless communication on a large scale can be easily observed and interfered with. WSN nodes are both complex component systems with numerous weak points from a security point of view. In addition, they are severely constrained in terms of energy and therefore extensive on-line security checking is not viable. Finally, sensors can be manipulated even without interfering with the electronic subsystem of the node and actuators can pose strong safety and hazard concerns.

The second argument that emphasizes the role of security in WSN is the importance of protecting typical applications. WSN can not only have data about one or more users, but can also contain a great deal of information about their past and even future actions. In addition, they may contain significant amounts of information about a user's physiological and even psychological profiles. Furthermore, once the sensors are equipped with actuators both the sensors and the environment can be impacted in a variety of ways.

The third reason for security in WSN is, in a sense, the most scientific and engineering based reason. WSN require new concepts and a new way of thinking with respect to security, privacy, digital rights management, and usage measurement. The Internet was a great facilitator of computer and communication security on a large scale. Note that the Internet itself created opportunities for new types of attacks such as denial of service (DoS) and intrusion detection. It also created new conceptual techniques on how to defend the Internet infras-