

# Preface

Recent technology progress, particularly in the areas of computer networks and hardware miniaturization, allowed the emergence of a set of novel computing and application scenarios referred in different ways, including “Internet of Things”, “Mobile Computing”, “Pervasive Computing”, or “Ubiquitous Computing”. Despite the specific meaning of those terminologies and their peculiarities, all those concepts involve the presence of small or tiny devices that communicate (possibly in a wireless way) and collaborate among them to achieve a common goal. In many of these emerging application scenarios, the security of the service and infrastructure, as well as the privacy of the involved parties, is a fundamental feature.

In this book, we focus on a representative technology in this arena: Wireless sensor networks (WSNs), i.e., networks made of tiny resource-constrained devices that have sensing and wireless communication capabilities. In particular, we present a comprehensive approach for building secure WSNs, taking into account different “levels” of security threats: from the basic need of nodes trusting and confidentiality between nodes (via means of establishing secret keys), toward physical attacks such as node capture (physical removal) or node cloning (physically building a new node, cloning the crypto material from an honest one), up to the security of specific applications, where we consider in particular data aggregation, which is a key service in WSNs that can be used to tackle with their energy constraints. Finally, as a representative case, for the data aggregation service we also look at possible privacy aspects, e.g., preserving the privacy of nodes participating in the aggregation—which in practical scenarios might be for example users of smart-metering or other services.

The main contributions of this book can be summarized as follows:

- With respect to the **establishment of pair-wise secret keys** between nodes, we present a new probabilistic solution, the enhanced cooperative channel establishment (ECCE) protocol that overcomes some of the limitations of existing solutions. In fact, ECCE presents higher probability for any pair of nodes to establish a secure channel and a higher resilience rate (i.e., the attacker needs a

bigger effort to corrupt the channel). This contribution has been partially published in [46, 47], and is described in Chap. 2.

- With respect to the **node capture attack** (i.e., physical removal from the network), which is the first step for an attacker to perform several other attacks that are crucial for WSNs (e.g., clone attack or the confidentiality violation), we design the first approach to detect the capture of a node leveraging the network mobility—in order for the nodes to trace the presence of the other nodes. The results of our study show that the newly proposed solutions can be practically implemented in sensor networks, and under certain mobility conditions (e.g., a certain average node speed) they perform better than solutions that do not leverage the network mobility. This contribution has been partially published in [45, 49, 53], and is described in Chap. 3.
- With respect to the **node cloning attack**, we first identify the properties that a distributed clone detection protocol should possess, then we design a randomized, efficient, and distributed (RED) protocol for detection of the node replication attack. RED shows better properties and performance when compared to the state of the art. In particular, it is not affected from an important issue that influenced protocols in the literature, i.e., the predictability of the position of the witnesses—hence making the process of detection less effective in practical scenarios. This contribution has been partially published in [50, 52, 54, 55], and is described in Chap. 4.
- With respect to specific WSN services, we focus on **data aggregation security**. The question was to find whether a WSN service can be secure, despite the possible presence of the adversary. Owing to the constrained resources of WSNs, nodes cannot send their own sensed data independently to a collecting point, hence the use of an aggregation protocol is fundamental (and so their security). In this scenario we design the first secure protocol for secure computation of the median aggregate. This contribution has been partially published in [190, 192–194], and is described in Chap. 5.
- With respect to **data aggregation security**, the challenge was to provide privacy to the single node collaborating in the data aggregation process. In many sensor network applications, the data sensed by a single node can be related to a user (or a number of users): Information on patients' health in a hospital, water consumption in a city, etc. Then, in order to protect the people's privacy, the data aggregation protocol that works in this type of context must protect the privacy of each single node. In particular, it should not be possible to relate a given sensed data to a given sensor node. We present the first data aggregation protocol that guarantees the privacy of a node not only against the other nodes but also against the Base Station, which is the entity that eventually collects the aggregated data. This contribution has been partially published in [60, 240], and is described in Chap. 6.



<http://www.springer.com/978-1-4939-3458-4>

Secure Wireless Sensor Networks

Threats and Solutions

Conti, M.

2015, XIII, 169 p., Hardcover

ISBN: 978-1-4939-3458-4