Advances in Information Security 65

Mauro Conti

Secure Wireless Sensor Networks

Threats and Solutions

Springer

Advances in Information Security

Volume 65

Series editor

Sushil Jajodia, George Mason University, Fairfax, VA, USA

More information about this series at http://www.springer.com/series/5576

Mauro Conti

Secure Wireless Sensor Networks

Threats and Solutions

Foreword by Luigi Vincenzo Mancini

Springer

Mauro Conti
University of Padua
Padua
Italy

ISSN 1568-2633
Advances in Information Security
ISBN 978-1-4939-3458-4 ISBN 978-1-4939-3460-7 (eBook)
DOI 10.1007/978-1-4939-3460-7

Library of Congress Control Number: 2015953798

Springer New York Heidelberg Dordrecht London

Printed on acid-free paper

Springer Science+Business Media LLC New York is part of Springer Science+Business Media (www.springer.com)

Foreword

This book by Dr. Mauro Conti focuses on the most important security challenges for WSNs, conducts a vast literature review on security threats and the currently proposed countermeasures, and proposes several novel mitigation approaches to each of the considered attacks. Moreover, Dr. Conti provides in-depth theoretical, analytical, and experimental discussions on each of the attacks and countermeasures. In particular, a security threat might result in hazardous situation when it comes to WSNs; this is because of their inherent hardware and software limitations in applying traditional security mechanisms, and of their frequent use in countless vital applications.

Over the years, I have dealt with various aspects of networks security, particularly in WSNs, together with my research group at the Dipartimento di Informatica della Sapienza Università di Roma, and with several renowned researchers all over the world. I believe that one of the main goals of adopting WSNs is to provide safety and comfort for humans. Therefore, we need to contemplate how this new technology would guarantee the goals of the designer without threatening the security and privacy of users.

Dr. Conti provides timely information for scholars and researchers desiring to design new WSN systems and applications, to be able to tackle the existing security challenges in these networks. Moreover, this book shines a light for early stage research on aspects related to key establishment, physical attacks, node capture attack, node clone attack, as well as security and privacy issues of specific WSNs services, such as data aggregation. The content of this book is the fruit of Dr. Conti's several years of research effort in security and privacy issues in WSNs, which have also led to numerous papers and patents.

It was my great pleasure to supervise the early research career of Dr. Conti as a promising Ph.D. student, to be involved in all the stages of this work, as well as collaborating with Dr. Conti afterwards. I believe this book by Dr. Conti is a key reference for WSN security challenges, and I hope you will enjoy reading this book.

Luigi Vincenzo Mancini
Sapienza University of Rome, Italy

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.

Mauro Conti

Acknowledgments

This book is a revised version of my Ph.D. thesis. I want to take this opportunity to express my gratitude to all the people that made this possible, and have been close to me during the years of my studies. I would like to thank in particular my Ph.D. advisor, Prof. Luigi Vincenzo Mancini, for sparking my research interest in security aspects of computer systems and communications; Prof. Sushil Jajodia, particularly for hosting my visiting period at George Mason University; and all the other people I had the chance to collaborate with during my Ph.D.: Roberto Di Pietro, Andrea Gabrielli, Alessandro Mei, Sanjeev Setia, Angelo Spognardi, Sankardas Roy, and Lei Zhang. Special thanks also to Prof. Cristina Pinotti and Prof. Srdjan Capkun for their valuable comments, which helped improving the quality of this work. Thanks also to Susan Lagerstrom-Fife and Jennifer Malat at Springer, for their guidance during the preparation of this book.

Furthermore, I would like to thank all the great scientists worldwide that collaborated with me at the early stage of my academic career, as well as all the passionate students and collaborators in my research group at the University of Padua: You really make my work so exciting and rewarding!

Last but not least, I would like to thank my family, for the continuous support, and for making all this possible!

Contents

Chapter 1
Introduction

The evolution of computing devices followed different paths. Despite the famous misquotation attributed to Thomas J. Watson Sr., then-president of IBM, ("I think there is a world market for maybe five computers."), during the 70's a new paradigm emerged: The Personal Computer. Computers intended to be used by a single person became so common that the market of personal computers overcame the one of Mainframes. With the introduction of computer networks and the miniaturization of the hardware a totally new paradigm has emerged since the last decade: The so-called Ubiquitous Computing. In particular, this paradigm aims to make "many computers available throughout the physical environment, but making them effectively invisible to the user" [228]. Recent advances in Micro Electro Mechanical Systems (MEMS), in wireless communications and in digital electronic made it possible the production of small, cheap and "smart" devices (that comes also with novel security and privacy issues [5, 6, 12, 17, 58, 151, 164]), such as smart-phones [44, 51, 59, 88, 97, 188, 243], PDAs, Radio Frequency IDentification (RFID) systems [56, 57, 191], Wireless Sensor Networks (WSNs), and many other technologies.

In this book, we focus on the security issues of the representative technology of Wireless Sensor Networks, introduced in the following section.

1.1 Wireless Sensor Networks

In this book, a sensor device is a small device that is able to sense environmental data (sound, light, temperature, etc.) and it is also able to communicate with any other sensor node in its communication range and compute the sensed/received data. A set of these sensor devices deployed in a given area constitutes a network with no pre-established architecture, so called Wireless Sensor Network (WSN). The usefulness of this type of network does not come from the single node capabilities, which are instead very limited, but from the collaboration of a large number of nodes. In a

M. Conti, *Secure Wireless Sensor Networks*, Advances in Information Security 65,
DOI 10.1007/978-1-4939-3460-7_1

WSN hundreds or thousands of nodes are usually deployed in a large area where they can sense the environment, compute and communicate the collected data in a very efficient and distributed way. Differently from other traditional wireless devices, sensor nodes do not communicate directly with a Base Station (BS)—a device that does not have the limitations of a sensor node—but mainly with other sensor nodes. So, sensed data are locally computed and forwarded to the BS. The lack of a pre-designed infrastructure implies that each node acts not only as a sensing node but also as an elaborating node and a routing point.

Current and future WSN applications are in different fields [127]: Supporting rescue operation, building surveillance, fire prevention, battlefield monitoring, and so on. Also, as often happens with new technologies, many applications can be designed and thought as far as the technology will be cheaper and widely available. A further description of the possible WSN applications is given in Sect. 1.1.1. In many applications of WSNs, the security of the network is a fundamental issue, as for: Confidentiality, integrity, authenticity, and availability. As an example assume a WSN is deployed for the safety of an area—e.g. for the detection of poisonous gas that could be potentially released during a concert or a big sport event. In this scenario, if the network is not secure we could have a false perception of safety, that can be even worse than the awareness that there is no safety at all.

1.1.1 Applications

Here, we recall some of all the possible application areas of the WSNs:

- Environmental applications [3, 33, 86, 226]. Some environmental applications of sensor networks include tracking the movements of birds, small animals, and insects; monitoring environmental conditions that affect crops and livestock; irrigation; macro-instruments for large-scale Earth monitoring and planetary exploration; chemical/biological detection; precision agriculture; biological, Earth, and environmental monitoring in marine, soil, and atmospheric contexts; forest fire detection; meteorological or geophysical research; bio-complexity mapping of the environment; and pollution study.
- Health applications [62]. Some of the health applications for sensor networks are providing interfaces for the disabled; integrated patient monitoring; diagnostics; drug administration in hospitals; constant monitoring of human physiological data; exact micro-drug release and non-invasive surgery; telemonitoring of elderly people.
- Other commercial applications [3, 86, 182]. Some of the commercial applications are monitoring material fatigue; building virtual keyboards; managing inventory; monitoring product quality; constructing smart office spaces; environmental control in office buildings; robot control and guidance in automatic manufacturing environments; interactive toys; interactive museums; factory process control and automation; monitoring disaster areas; smart structures with sensor nodes