Chapter 8
Cryptomodules in Wireless Networks Using Biometric Authentication:
Securing Nodes in Wireless Networks

Martin Drahanský
Brno University of Technology, Czech Republic

Martin Henzl
Brno University of Technology, Czech Republic

Petr Hanáček
Brno University of Technology, Czech Republic

František V. Zbořil
Brno University of Technology, Czech Republic

František Zbořil
Brno University of Technology, Czech Republic

Jaegeol Yim
Dongguk University at Gyeongju Gyeongbuk, South Korea

Kyubark Shim
Dongguk University at Gyeongju Gyeongbuk, South Korea

ABSTRACT

This chapter shows how cryptomodules can increase security of wireless sensor network and possibilities of biometric authentication against a node or the whole network. For secure operation of a wireless sensor network, security objectives such as confidentiality, integrity, and authentication must be implemented. These security objectives typically employ cryptography, therefore sensor nodes should be able to compute cryptographic algorithms and provide secure tamper-resistant storage for cryptographic keys. Use of dedicated secure hardware for this purpose and security threats are discussed. Two scenarios where the biometric authentication would be appreciated are introduced – smart home and storehouse with medicaments. Biometric generation of cryptographic keys, biometric authentication in wireless network and possible attacks on biometrics are presented. When designing and verifying communication protocols using informal techniques, some security errors may remain undetected. Formal verification methods that provide a systematic way of finding protocol flaws are discussed.

DOI: 10.4018/978-1-4666-9426-2.ch008

INTRODUCTION

The wireless networks are well known conception for various solutions, not only in academic (research) area, but are very often used in industrial solutions. However, their use in industrial solutions opens two very important questions – how we can secure the communication within the wireless network and how we can determine whether there is any possibility of authentication against a node or the whole wireless sensor network (WSN). The answers to these questions might be found in this chapter.

As an example we can take two different industrial solutions that can be used for wireless networks could be installed – see the following two subsections. In both cases, the above mentioned questions can be addressed, because they play a very important role in the whole process.

Smart Home Example

The first case could be a smart home (household) – the sensors collect information about various parts of the house and send it into the main central unit, where this data is processed and the commands are sent to actuators, which influence the actual situation of the house. Anyway the communication among wireless nodes has to be enciphered, because an attacker could corrupt the data exchanged among the units and this could influence the behavior of the whole system, e.g. the attacker can evoke a false fire alarm, which could lead to the lower security of the house in the expectation of arrival of firefighter, who has to get the access to the burning zone. This security change could be misused by the attacker to get into the house without big troubles. Another part of this topic is authentication of the house residents to the system that they will get the access into the house and the selected parts of the household will be adjusted to the settings of the concrete user. Therefore a (preferably) biometric authentication to a wireless network node is requested.

As a good example, we can take the RF Touch product from the company ELKO EP[1]. This company provides intelligent electronic systems and solutions for a comfortable household control. RF Touch is the main control unit of the new wireless system generation called RF Control. How this unit and the entire system work and what are its capabilities will be described in this chapter, based on Kubát (2011).

This RF control system (Wang 2009) allows the user to control and maintain the entire building - from lights and sun-blinds, through heating system, to garage door and garden swimming pool. Every RF unit connected to some specific device like light switch or heating thermo regulator is communicating with the RF Touch control unit by a wireless protocol, so there is no need to damage the walls and strain new wires when installing the system. The RF units are mounted between the original switch and the device, so the function of the primary switch is preserved.

The heart of the system is the RF Touch control unit, which identifies all connected peripheries (based on their name and physical address) and keeps a list of them sorted in various categories based on the theme of their role in the system (e.g. lights or heating). This main unit (ELKO EP 2010) communicates with the peripheries (sometimes called actuators) and is responsible for all the actions taken in the system. These actions may be invoked either by the user himself (sending real-time commands from any control device connected) or triggered automatically depending on any behavior scheme programmed in the device.

The unit itself is manufactured in two versions (RF Control and RF Touch 2010). The first is a standalone type designed to be hung on a wall or laid on a table. It is powered by a 12V DC adapter (2,1mm jack) or by 85-230V AC supply voltage (push-in terminal on the back side). The second type should