Chapter 5
Security in E-Health Applications

Victor Pomponiu
University of Torino, Italy

ABSTRACT

Wireless sensor networks (WSNs) in e-health applications are acquiring an increasing importance due to the widespread diffusion of wearable vital sign sensors and location tags which can track both healthcare personnel and patient status location continuously in real-time mode. Despite the increased range of potential application frameworks the security breach between existing sensor network characteristics and the requirements of medical applications remains unresolved. Devising a sensor network architecture which complies with the security mechanisms is not a trivial task since the WSN devices are extremely limited in terms of power, computation and communication. This chapter presents an analysis of various WSN security techniques from the perspective of healthcare applications, and takes into consideration the significance of security to the efficient distribution of ubiquitous computing solutions.

INTRODUCTION

Nowadays in modern communication age, health and its related issues are very important since they involve all people. Actual health care system recompenses the medical doctors and hospitals for treating sick people, but does not prevent people from being sick. Due to the raising costs of health care services together with the growth of elderly population, the current medical system is subject to reform that requires several major changes in insurance companies, hospitals and patients.

The idea that emerges is that healthcare needs to move toward a more *proactive* behavior, which implies prevention and early detection of severe events, combined with the availability of scalable and accessible medical solutions. These requirements create a great need for pervasive

DOI: 10.4018/978-1-60960-469-1.ch005

electronic health (e-Health) environments, accessible from everywhere and that commit reduced financial and human resources (Aziz et al., 2008; Savastano, Hovsto, Pharow, & Blobel, 2008). As a consequence, e-Health has become an important research topic with developments in multiple domains like, health care, public health, data management, image processing, wireless networking and telecommunications.

Recently, networking and computing technologies started to penetrate the health care and medical treatment, bring important benefits, e.g., deployment of quality healthcare services at lower costs (BioHealth, 2008). The modern networks and communications technologies such as Wireless Sensor Networks (WSNs), Global System for Mobile communications (GSM), Universal Mobile Telecommunications System (UMTS), WiMAX, and Wireless, offer high data rates, and allow time-efficient transmission and processing of medical data.

Owing to these benefits Wireless Sensor Networks, that consist of several connected device called smart senor nodes, began to be widely used in medical environments (Fragopoulos, Gialelis, & Serpanos, 2009; Lorincz et al., & 2004; Malasari et al., 2007; Waterman et al., 2005; Wood et al., 2006). The sensors within a WSN are able to communicate with each other through wireless technologies, like IEEE 802.15.4/ZigBee and IEEE 802.15.1/Bluetooth, which are intended for cable replacement, ad hoc connectivity and low-rate medical applications (e.g., those provided near the patient's bed). Instead, 2.5G (e.g., GPRS) and 3G (e.g., UMTS) technologies are used to transmit information to devices residing on another network.

A particular case of WSNs are Body Area Networks (BANs), which are also called Wireless Body Area Networks (WBANs). Briefly, a BAN consists of several mobile and dense connected sensors, either wearable or implanted into the human body, which permanent monitors and logs patient vital body parameters, e.g., the blood-pressure, the blood-oxygen, and the ECG. The sensors are attached to the patient's body and connected, through Bluetooth and ZigBee technologies, to a central data-collecting unit. e-Health applications based on BANs (Konstantas, Jones, & Herzog, 2002; Lupu et al., 2007; Marti, Delagado, & Perramon, 2004; Ng et al., 2004; Stingl & Slamanig, 2008; Stoa, Balasingham, & Ramstad, 2007; Vouyioukas et al, 2008; S. Warren et al., 2005) are extremely valuable since they allow doctors and hospitals to monitor remotely, in real-time the patient health condition.

However, shifting from wires to wireless networks impose a deep analysis of the available technologies in order to find the most suitable ones for e-Health environment. Moreover, in order to increase the users' acceptance of these new technologies, protection and security mechanisms of sensitive data should be of the highest standard (Chevrollier & Golmie, 2005; Chhanabhai & Holt, 2007).

The characteristics of the modern e-Health applications impose security requirements such as protection, integrity and confidentiality of sensitive medical data, i.e., of the electronic health records (EHRs) and electronic personal records (EPRs) (Agrawal & Johnson, 2007; Katsikas, Lopez, & Pernul, 2008; Savastano et al., 2008). Considering the limited resources of such applications, is challenging to devise and distribute efficient solutions that are able to satisfy the security requirements.

In this chapter we discuss the security challenges and techniques for e-Health applications delivered over WSNs. To provide useful insights, we structure the rest of this chapter as follows: first, we give a brief overview of the wireless sensor networks along with a description of their main characteristics. Second, an overview of the latest healthcare applications based on WSNs is provided. A particular attention is devoted to the intrinsic vulnerabilities of wireless networks which can affect the effectiveness of medical applications. Then, we present the potential malevolent