Chapter 14

Covert Communication in Wireless Sensor Networks for E-Health Applications

Fahimeh Rezaei
University of Nebraska-Lincoln, USA

Pradhunma Lal Shrestha
University of Nebraska-Lincoln, USA

Sushanta Mohan Rakshit
University of Nebraska-Lincoln, USA

Hamid Sharif
University of Nebraska-Lincoln, USA

ABSTRACT

In this chapter, the authors introduce a threat in Wireless Sensor Network (WSN) E-Health applications that can be used for leaking patients’ medical information, identity, personal data, and medical history. This threat is called covert communication, which establishes a secret path hidden within legitimate network traffic to transfer information. Based on the exploit used for this type of communication, covert channels have different categories and functionalities. The authors introduce various covert communication methods and their possible applications in transmitting e-health data secretly in WSNs. In addition, the authors discuss different methods and approaches to detect this type of communication in WSNs to prevent this form of malicious e-health information transfer.

INTRODUCTION

One of the most important applications of Wireless Sensor Networks (WSN) is the area of e-health, where several medical sensors monitor and collect the health information of a patient’s body. This information can be collected in a highly localized network type called Body Area Network (BAN), connected to the Local Area Network (LAN), eventually to be transferred to the hospital or healthcare center via Wide Area Network (WAN) communication. The collected medical information can then be accessed among various groups of doctors, researchers and hospital staff members, but otherwise should be highly access-controlled in accordance with corresponding regulations such as the Health Insurance Portability and Ac-

DOI: 10.4018/978-1-4666-8251-1.ch014
countability Act (HIPAA). Due to the fact that the healthcare information for each patient is confidential and needs to remain protected, the security of WSNs for this specific application is a significant concern. Hence, several research areas and activities are dedicated to e-health data protection and WSN system security to keep medical and personal identity information confidential and prevent malicious or accidental disclosure. Beyond the more traditional attacks and security solutions that are discussed in the literature we would like to introduce the reader to a different potential threat to WSNs that can be used by malicious parties to illegally access patients’ identity information, medical history, health status records and more. Although this threat, which is called covert communication, can be employed in other areas of WSNs, the existence of this secret path for leaking e-health information is significantly more dangerous.

This book chapter is organized as follows: In the background section, firstly, e-health WSN architecture and technologies are briefly introduced. This section is continued by current security concerns and areas that are previously discussed in literature. Then we introduce a possible threat that was not considered in literature for e-health applications and outline different methods and techniques that can be used for implementing this threat to leak medical data. In section V, we introduce some methods and techniques to detect this new threat and prevent establishing it for e-health WSN applications. Finally in section VI, we provide a summary and conclusion and the future research track in this area.

**BACKGROUND**

In this section we first provide a background regarding telemedicine and e-health using WSN devices and technologies. In addition, we review various security topics and concepts that are discussed in previous literature in the area of e-health.

**Wireless Sensor Networks in E-Health**

Employing recent technologies and smart devices for monitoring and recording biological changes in human body, mostly for medical applications is referred to as e-health. Evidently, taking advantage of e-health technologies and devices reduces dependencies on healthcare staff and specialists as well as frequently health center visits that are required for the patients to record their health condition. Moreover, due to the new and precise hardware and embedded system devices, measured parameters by these devices and new technologies are accurate and reliable. Using the new and high speed wireless technologies also provides an easy way to transfer medical data to a given database in a hospital or healthcare center. This database can be accessible by various groups such as doctors, nurses, researchers, insurance companies and other related groups readily and in a specific format that is required. Hence, the patient does not need to provide the same information to different group multiple times. Therefore, using e-health devices and technologies is reliable, cost effective and convenient for the patients and the parties that need to use patient’s medical data and history.

Generally monitoring devices are at least equipped by several sensors to record the biological signals, storage unit to saves the measured parameters and a communication module that can send collected data to a local database. A collection of different medical data or biological signals that can be monitored and measured by BAN devices are shown in Table 1 (Rezaei, Hempel, & Sharif, 2015), as well as their typical required data rate. These sensors are interfaced with a given wireless communication module that can support their required data rate and the redundancy of sending data within a specific time slot. For example if
Related Content

Eigencombining: A Unified Approach to Antenna Array Signal Processing
Constantin Siriteanu and Steven D. Blostein (2009). Handbook on Advancements in Smart Antenna Technologies for Wireless Networks (pp. 1-32).
www.igi-global.com/chapter/eigencombining-unified-approach-antenna-array/8450?camid=4v1a

Analysis of Bandwidth Efficiency in IEEE 802.11 and 802.16 Interworking Networks
www.igi-global.com/article/analysis-of-bandwidth-efficiency-in-ieee-80211-and-80216-interworking-networks/209433?camid=4v1a

Parallel Soft Spherical Detection for Coded MIMO Systems
www.igi-global.com/chapter/parallel-soft-spherical-detection-coded/40721?camid=4v1a

Efficient Channel Utilization and Prioritization Scheme for Emergency Calls in Cellular Network
www.igi-global.com/article/efficient-channel-utilization-and-prioritization-scheme-for-emergency-calls-in-cellular-network/121659?camid=4v1a