BIOMETRIC-BASED AUTHENTICATION AND KEY MANAGEMENT SCHEME FOR WBANS

By

SUFYAN T. FARAJ * ALI J. DAWOOD ** EKRAM H. HASSAN ***

* Faculty Member, College of Computer, University of Anbar, Ramadi, Iraq.
** Faculty Member, College of Computer, University of Anbar, Ramadi, Iraq.
*** Student, College of Computer, University of Anbar, Ramadi, Iraq.

ABSTRACT

In recent years, the use of sensors to measure the biometrics and movements of human body has resulted in the design of wireless body area networks (WBANs). These consist of small, intelligent devices attached on or implanted in the body .The development of such networks is imperative for modern telemedicine and m-health. However, security remains a formidable challenge yet to be dealt with. WBANs have the advantage of the possibility of using random biometric measurements that use an intrinsic characteristic of the human body as the authentication identity or the means of securing the distribution of cipher keys. In this paper, the authors survey the most recent research directions in the field. Then, a distributed key management scheme, which makes use of key refreshment schedules, would be proposed to fairly and securely distribute key management responsibility among all nodes. Our scheme supports the use of biometric measurements to generate symmetric keys in WBAN scenarios.

Keywords: Authentication, Body Area Network, Biometric Measurements, Key Management, WBAN.

INTRODUCTION

Sensors can be used to observe and measure any kind of phenomena in real-time environments (chemical, biological, physical). Hence, using sensors to measure the biometrics and movements of human body has resulted in the design of Wireless Body Area Networks (WBANs). WBAN is an ad hoc network which consists of small, intelligent devices attached on clothing or on the body or even implanted under the skin which are capable of establishing a wireless communication link (Latre et al, 2011). Each intelligent device or sensor node called Biosensor Node (BN) forwards data to a central coordinator called Body Network Controller (BNC) or Personal Server (PS) which is typically a hand-held device (like PDA or smart phone) that is usually associated with the same patient to collect health data (such as temperature, heart rate, blood pressure, etc.) (Li et al, 2010). Then, the PS transmits data to a Medical Server (MS) (which can be a physician or staff) for required recommendations (Jang et al, 2008). Each WBAN is associated with only one body. It is also possible that multiple WBANs are associated with one central MS. The MS stores and processes information of all the WBANs those are associated with it, as shown in Figure 1.

Using a WBAN grants the patient a greater physical mobility and he/she is no longer compelled to stay in the hospital. Applications of WBAN include healthcare, life care and athlete examination. Healthcare includes care for inpatients especially those who are seriously ill, unconscious or under intensive care. Life care includes patients who live their lives normally but may require medical care at any time (Raazi et al, 2010). Reliable and secure WBAN deployments can significantly facilitate electronic-health (e-health) applications including mobile-health (m-health) practical settings. However, there are many security and privacy concerns that need to be addressed before reaching to a reliable and dependable full integration of WBANs in m-health platforms.

The aim of this paper is to propose a biometric-based key distribution and management scheme for WBANs which relies on symmetric cryptography. We will describe our proposal and report on our ongoing implementation and validation work in this direction. The reminder of this paper