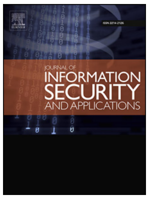
Journal of Information Security and Applications 41 (2018) 62–74

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa



A biometric security scheme for wireless body area networks

Peyman Dodangeh, Amir Hossein Jahangir*

Department of Computer Engineering, Sharif University of Technology, Tehran, Iran

ARTICLE INFO

Article history:

Index Terms:
Wireless body area network (WBAN)
Sensor networks
Security
Protocols
Secret sharing, Analysis, BAN Logic

ABSTRACT

Wireless body area networks (WBANs) are receiving significant interest as the next generation of wireless networks and emerging technology in the field of health monitoring. One of the most important factors for the acceptance of WBANs is the provision of appropriate security and access control mechanisms. Due to its nature in transferring the patients' sensitive data, WBAN has both classical and specific security requirements. In this paper, we survey such requirements and propose a new security scheme for satisfying them in WBANs. The proposed scheme deals with the overall network architecture, including intra- and inter-WBAN tiers, and proposes two mutual authentication and key exchange protocols for diverse WBAN environments. In our scheme, we use biometrics as one part of the solution for authentication and key exchange, and the simple password three-party key exchange protocol as the other part of the WBAN security. Our scheme meets security requirements along with energy-constraint considerations. We verify our scheme through BAN Logic. Unlike the majority of the existing security protocols, our scheme proposes a solution for entire WBANs communications, from biosensors to the medical server as a trusted third party.

1. Introduction

Nowadays, wireless communications have fundamentally improved people's life quality. Recent advances, both in wireless communications and microelectronic systems, have allowed the realization and establishment of large-scale, low-power, multi-functional, and low-cost networks. Wireless sensor networks (WSNs) have applications in many areas, such as intelligent home and office, transportation, environmental monitoring, control and automation, logistics, healthcare, security and surveillance, tourism and leisure, education and training, and entertainment [1,3]. The application of WSNs in healthcare introduces a special kind of network called Wireless Body Area Network (WBAN). However, there exist several differences between WSNs and WBANs [8]. WBANs were first introduced by T.G. Zimmerman in 1996 [2]; there has been a noticeable increase in the number of research studies since then, and now WBAN is in its fledging period. Furthermore, during the last few years there has been significant growth in the number of various implantable and wearable health monitoring devices, ranging from simple pulse monitors, activity monitors, and portable Holter monitors, to sophisticated and expensive implantable sensors (biosensors) [11].

WBAN is a wireless network used for communication between intelligent, miniaturized, low-power biosensors operating in or on the human body to remotely monitor the patients' health. Biosensors sense or gather certain body parameters such as the electrocardiogram (ECG), electroencephalogram (EEG), photoplethysmographic (PPG), body movement, body temperature, blood pressure, blood glucose, heart rate, and respiration rate levels, oxygen saturation [7]. They can send the gathered data to a controller like a smartphone or a laptop through short range medium access communication such as Bluetooth. Also, the actuators can take some specific actions according to the command they receive from the controller, like injecting the required dose of insulin to diabetics based on the measurements of the glucose level [59,9]. The common communication architecture for WBANs is based on a two-tier Intra- and inter-WBAN topology [13]. Some other research studies consider it consists of three tiers [7]. The intra-WBAN communications include the data exchanges between the biosensors (SNs) and the Mobile Node (MN), whereas inter-WBAN communications include the ones between the MN and the Medical Server (MS) and the storage server holds patient's Protected Health Information (PHI). The architecture of a typical WBAN is shown in Fig. 1. The MN processes the medical data collected from the intra-WBAN tier and transmitted to the MS for remote monitoring.

In recent years, many standards have been proposed for WBANs and short distance intra-WBAN communications. They include IEEE 802.15.1 Bluetooth, IEEE 802.15.3 UWB, and IEEE 802.15.4 ZigBee [63]. Meanwhile, IEEE has amended the 802.15.6 standard for wire-

* Corresponding author.
E-mail addresses: Dodangeh@ce.sharif.edu (P. Dodangeh), Jahangir@sharif.edu, Jahangir@sharif.ir (A.H. Jahangir).

https://doi.org/10.1016/j.jisa.2018.06.001
2214-2126/© 2018 Elsevier Ltd. All rights reserved.

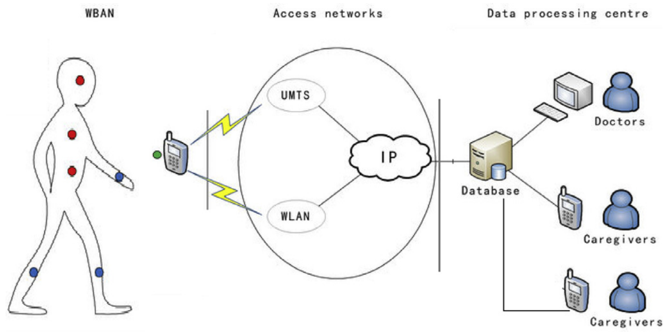


Fig. 1. WBAN Architecture.

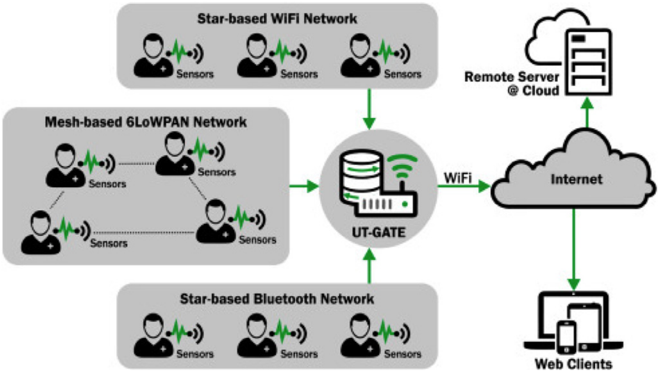


Fig. 2. e-Healthcare Architecture.

less body area networks in 2012, which regulates the technical requirements at each layer of WBANs.

WBANs provide health care anywhere, at any time, while reducing the burden on the medical sector and improving the quality of healthcare. Nowadays WBANs are part of larger systems which are known as e-healthcare systems [64–66]. An e-healthcare system consists of many software and hardware components collaborating to take care of patient's health remotely. These components comprise biosensors, mobile devices, wireless and wired networks, and data management software. The architecture of an e-healthcare architecture is depicted in Fig. 2.

Before widely applying sensor networks in healthcare, some psychological and socio-political questions in addition to a number of challenging system design issues, like security and performance, should be taken into account. In an information system like WBANs, it is essential to design and use a security mechanism to protect the information, as it is susceptible to breach either when it is stored or when it is transmitted. As the communication between WBANs parties takes place on the public Internet, the whole system is vulnerable regarding threats associated with open Internet [64]. So, implementing security requirements for these networks is crucial as human lives could directly rely on them.

As discussed earlier, biosensors have stringent resource limitations regarding energy and storage. The mobile node has more resources, though limited, as it uses a battery. Meanwhile, the plugged wireless network and the medical server are supposed to have unlimited resources. A trade-off always exists between the provided level of security and the performance of the system. However, it is required by law that the information be secure [15], in the sense that it must possess the characteristics of secure data: authenticity, integrity, and confidentiality. In Table 1, we have listed the security requirements in WBANs.

Secure key exchange and mutual authentication are the well-known mechanisms to provide security in WBANs. Usually, two types of cryptographic techniques are used in these mechanisms: symmetric and asymmetric. Asymmetric cryptography based key exchange protocols are not suitable for generic sensors due to their heavy overhead. For example, using a MIPS R4400 processor, the establishment of a key with a 128-bit operation of Diffie-Hellman costs 15.9mJ while the symmetric encryption of the same bit length on the same processor consumes 0.00115mJ of energy [16]. Nevertheless, there have been many studies aimed at applying lightweight asymmetric key cryptography to intra-WABN communications like TinyECC [17], hardware solutions [18] and Identity Based Cryptography (IBC) [19]. However, they still suffer from energy usage and performance overhead in comparison with symmetric key cryptography in authentication and key exchange applications. In the case of symmetric key cryptography in intra-WBAN communications, the pre-shared key between nodes is also needed for a periodic key update.

One of the promising solutions for enabling symmetric key cryptography with the key update property is to use biometric information as the random number needed for the cryptographic operation. Deriving the required inputs for the security mechanism from the body itself is, in fact, an attractive approach. Several studies have examined the use of various biometric features for the sake of security, like EEG or ECG [20]. The main criterion for the suitability of a biometric value for security purposes is its randomness in order to produce and/or communicate a secure key.

In this paper, we propose a security scheme which makes use of biometric characteristics derived from the human body to secure the keying material which in turn is used to secure the data communication in intra-WBAN and the authentication and key exchange in inter-WBAN. In fact, our scheme will secure the architecture of the WBAN by considering the security requirements, while it is efficient with regard to energy and storage. The remainder of the paper is organized as follows. We give an overview of the related works in Section 2, followed by the security requirement and the attacker model in WBAN in Section 3, and a detailed description of the proposed scheme to secure WBAN communications in Section 4. In section 5, the analysis of our scheme in terms of security services, storage, and energy cost will be presented. We will verify the correctness of our scheme using formal methods in Section 6. Concluding remarks and future research directions are given in Section 7 and 8 respectively.

2. Related works

Since major WBANs security solutions consider two heterogeneous, Intra- and Inter-WBANs, these solutions vary in the means they propose a reliable and secure communication scheme in medical body sensor networks. We have divided the related works into two major categories. The first deals with securing the WBANs communications whereas the second is about securing the e-healthcare system globally. The researches on the former category aim at securing low-level communications at the network layer between biosensors and the mobile node, while the second category focuses on secure schemes at the application level, especially authentication and anonymity of the patients and physicians when they connect to the e-healthcare system. The classification of different wireless medical security schemes is depicted in Fig. 3.

2.1. Security schemes based on Asymmetric Key Cryptography

Ibrahim et al. have proposed in [12] an anonymous authenticated key agreement protocol based on simple cryptographic primitives for WBANs. Several ECC-based authentication schemes are also presented in [14,20,22,23,72], where public and private keys are used to ensure the security of the intra-WBAN communication. Lee et al. have proposed in [23] an encryption scheme based