Computers and Electrical Engineering 000 (2017) 1–10

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

A provably secure password-based anonymous authentication scheme for wireless body area networks[☆]

Fushan Wei[a,b,*], P. Vijayakumar[c], Jian Shen[a], Ruijie Zhang[b], Li Li[d]

[a] School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing, 210044, China
[b] State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou, 450002, China
[c] University College of Engineering Tindivanam, A Constituent College of Anna University Chennai, Melpakkam, 604001, India
[d] International School of Software, Wuhan University, Wuhan, 430000, China

ARTICLE INFO

Article history:
Received 29 December 2016
Revised 19 April 2017
Accepted 19 April 2017
Available online xxx

Keywords:
Anonymous
Wireless body area networks
Password authentication
Zero-knowledge proof
Provably security

ABSTRACT

Wireless body area networks (WBANs) comprise many tiny sensor nodes which are planted in or around a patient's body. These sensor nodes can collect biomedical data of the patient and transmit these valuable data to a data sink or a personal digital assistant. Later, health care service providers can get access to these data through authorization. The biomedical data are usually personal and privacy. Consequently, data confidentiality and user privacy are primary concerns for WBANs. In order to achieve these goals, we propose an anonymous authentication scheme for WBANs based on low-entropy password and prove its security in the random oracle model. Our scheme enjoys strong anonymity in the sense that only the client knows his identity during the authentication phase of the scheme. Compared with other related proposals, our scheme is efficient in terms of computation. Moreover, the authentication of the client relies on human-rememberable password, which makes our scheme more suitable for applications in WBANs.

1. Introduction

With the rapid development of wireless communication and information technologies, we are now in the era of cloud computing [1], the Internet of things [2] and big data [3]. Nowadays, people no longer need come to hospitals and medical centers to get medical care services thanks to these advanced technologies. Instead, patients now can enjoy convenient e-health services almost anytime and anywhere [4,5]. E-health services mainly rely on wireless body area networks (WBANs). WBAN systems consist many tiny sensors which are planted in or around a human body with wireless communication ability (such as Wi-Fi, blue-teeth) to transmit collected data of a patient to a sink node. The sink node can be a smart phone, a personal digital assistant or any portable devices. The sink node stores the collected biomedical data (such as cardiac, blood pressure, heart beat) of a client. Later, medical care service providers can get access to these biomedical data to diagnose a patient [6].

WBANs greatly improve the life quality of patients and provide almost ubiquitous e-health services. However, WBANs also bring some challenges which should be solved before using this technology in real-life. The first challenge is security.

[☆] Reviews processed and recommended for publication to the Editor-in-Chief by Guest Editor Dr. M. Karuppiah.

[*] Corresponding author.

E-mail addresses: weifs831020@163.com (F. Wei), vijibond2000@gmail.com (P. Vijayakumar), s_shenjian@126.com (J. Shen), rjz_wonder@163.com (R. Zhang), lli@whu.edu.cn (L. Li).

http://dx.doi.org/10.1016/j.compeleceng.2017.04.017
0045-7906/© 2017 Elsevier Ltd. All rights reserved.

The biomedical data collected by WBANs should be dedicated to one system and not mixed with other users data. Moreover, these data should be protected and have limited access. Only authorized entities can get access to these data. Although security is the primary concern in many other networks [7], little attention has been paid to this issue for WBANs. Sensor nodes are usually tiny and hence are resource-constrained in terms of computation ability, communication bandwidth, battery and memory. Due to these constrains, traditional security solutions designed for other networks are not suitable for use in WBANs [8,9]. Another challenge is the protection of privacy [10,11]. The biomedical data of a patient is personal and sensitive. Patients don't want these personal data to be misused. The privacy of users in WBANs should be guaranteed in order to make more people use WABNs. In summary, data confidentiality, data integrity, access control, user authentication, data freshness and user privacy are fundamental security requirements for WBANs. To the best of our knowledge, the IEEE 802.15.6 standard is the most recently designed standard to fulfill these security requirements in WBANs. Unfortunately, it is found that the protocols in the IEEE 802.15.6 standard all have security problems and are insecure against different attacks [12].

Due to the security weaknesses of the IEEE 802.15.6 standard protocols, researchers pay attention to security requirements for WBANS and design different schemes to realize these requirements. In 2006, Poon et al. [13] proposed a biometric-based authentication scheme for WBANs. They used the inter-pulse interval as the biometric authentication factor. However, biometric characteristics suffer from freshness vulnerability [14]. In 2007, Singh et al. [15] presented a key establish protocol between body sensor nodes using cryptographically weak physiological data. They also put forward a key establish protocol between a sink node and a sensor node. In 2010, Venkatasubramanian et al. [16] designed a physiological value-based security scheme for WBANs. Their scheme can distribute a secure session key by hiding the message using physiological values. Venkatasubramanian et al. [17] also presented a key agreement scheme based on physiological signal. Their scheme enables sensor nodes in a WBANs to generate a symmetric authenticated secret key using physiological signals without using the famous Diffie–Hellman key exchange protocol. Zeng et al. [18] summarized the advantage and disadvantages of authentication schemes using non-cryptographic mechanisms and proposed a channel-based authentication scheme for WBANs. Cai et al. [19] proposed a scheme called Good Neighbor to realized authentication in WBANs. However, their proposal is not practical due to unrealistic assumptions. Shi et al. proposed an authentication scheme based on channel characteristics [20]. The authentication schemes for WBANs based on non-cryptographic mechanisms are efficient but not secure enough. To provide high-level security, Li et al. [21] presented a group authenticated key agreement protocol for WBANs. Their protocol enables a group of sensor nodes to generate a common session key. He et al. [22] proposed a cross-domain handshake protocol for WBANs using identity-based public key system. Recently, researchers pay attentions to anonymous authentication schemes for WBANs because these schemes can achieve both security of the biomedical data and privacy of the patient. Liu et al. [23] presented two anonymous authentication schemes for WBANs based on certificateless public key mechanism. They claim their scheme not only ensure the anonymity of the user, but also outperforms other schemes in terms of security properties and efficiency. However, He et al. [24] demonstrated that Liu et al.'s schemes are insecure against the impersonation attack. He et al. also proposed a provably secure anonymous authentication scheme based on bilinear pairings to overcome the shortcomings of Liu et al.'s schemes. Although He et al.'s scheme achieves many security requirements and is claimed to maintain high efficiency in terms of computation, it has the following problems. First, it only achieves weak anonymity because the application provider knows the real identity of the patient. Second, their scheme relies on the timestamp and the user has to store a secret key issued by the network manager. Last but not least, their scheme is based on the computation-expensive bilinear pairing operations [25,26], so it is actually computation inefficient contrary to the authors' claim.

In order to remedy the shortcomings of He et al.'s scheme, we propose an anonymous authentication scheme for WBANs based on Zhang et al.'s anonymous password authentication protocol [27]. The authentication factor of the user in our scheme is the most commonly used password mechanism [28], which makes our scheme more user-friendly. We prove the security of our proposal in the random oracle model under the DDH (Decisional Diffie–Hellman) hardness assumption. The performance comparison shows that our proposal not only achieves more security requirements, but also is quite efficient in terms of computation. Our contribution is three folds. First of all, we propose the first anonymous authentication scheme for WBANs which is based on low-entropy passwords. Secondly, our protocol achieves the strongest anonymity because both the network manager and the application provider do not know the real identity of the user. Last but not least, our protocol is very efficient in computation because we avoid using the computation-expensive bilinear pairing operations. Due to these merits, we believe our scheme is more suitable for real applications in WBANs.

The remainder of this paper is organized as follows. In Section 2, we introduce the security model of our scheme. We present our anonymous authentication scheme in Section 3. In Section 4, we prove the correctness, anonymity and security of our scheme. We compare the efficiency and security features of our scheme with other related schemes in Section 5. We conclude this paper in Section 6.

2. Security model

In this section, we present the security model used in the security proof of our scheme. Our security model combines the security models of [24] and [29].

There are three kinds of participants in an anonymous authentication scheme for WBANs: the network manager NM, the application providers APs and the clients. NM is in charge of the whole system and is trust-worthy. For simplicity, we