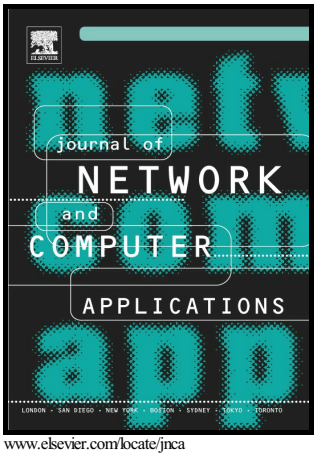
Key Management in Wireless Body Area Network:Challenges and Issues

Mohammad Masdari, Safiyyeh Ahmadzadeh, Moazam Bidaki



www.elsevier.com/locate/jnca

PII: S1084-8045(17)30149-2
DOI: http://dx.doi.org/10.1016/j.jnca.2017.04.008
Reference: YJNCA1905

To appear in: *Journal of Network and Computer Applications*

Received date: 3 May 2016
Revised date: 26 November 2016
Accepted date: 8 April 2017

Cite this article as: Mohammad Masdari, Safiyyeh Ahmadzadeh and Moazam Bidaki, Key Management in Wireless Body Area Network:Challenges and Issues, *Journal of Network and Computer Applications*, http://dx.doi.org/10.1016/j.jnca.2017.04.008

Key Management in Wireless Body Area Network:Challenges and Issues

Mohammad Masdari[1], Safiyyeh Ahmadzadeh[2], Moazam Bidaki[3]

[1]Department of Computer Engineering, Urmia Branch, Islamic Azad University, Urmia, Iran,
[2]Department of Computer Engineering, Urmia Branch, Islamic Azad University, Urmia, Iran,
[3]Department of computer engineering, Islamic Azad University, Science and Research Branch, Khorasan Razavi (Neyshabur), Iran

M.Masdari@Iaurmia.ac.ir
Safia.Ahmadzadeh@gmail.com
mBidaki@Iau-neyshabur.ac.ir

Abstract

The miniaturization of wireless sensors and medical devices have empowered the extension of Wireless Body Area Networks (WBANs) and E-Health care systems. However, in WBANs, wireless communications are exposed to a variety of passive and active security attacks. As a result, protection of privacy and integrity of the collected data from WBANs is of high importance. To mitigate these problems, numerous key management and security solutions have been designed for the WBANs in the literature, that this paper provides a comprehensive analysis of them. It mainly classifies the key management methods into the biometric and non-biometric categories and illustrates their main capabilities in detail. Furthermore, it provides a complete comparison of the security schemes and highlights their features and limitations.

Keywords: Body Area Networks, Security, Key management, IEEE 802.15.6, Biometric

1. Introduction

Wireless body area network or WBAN is an emerging technology which can be applied in the E-Healthcare systems [1-3]. WBANs consist of various types of sensors which can be placed on, around or in the human body to monitor body temperature, blood pressure, pulse oximetry, electrocardiogram (ECG), etc. [4]. The WBANs can be applied in numerous medical and non-medical applications. It can utilize implantable medical sensor nodes in the human body, which has a short-range wireless communication capability.

In E-Healthcare systems, the data collected by WBAN's sensors can be applied to alert the medical personnel of a hospital when a life threatening event occurs [5-9]. As a result, a lack of security while storing the data inside the WBAN or transmitting them outside the WBAN may lead to the loss of data privacy and integrity [10]. Such an environment raises security seriously pertaining to the privacy of critical medical data coupled with the resource limitations of the individual body sensor nodes [11, 12]. However, WBANs have few number of resource limited nodes which make establishing security more difficult than other conventional networks that can utilize high cost security mechanisms in terms of memory, CPU usage and energy consumption [13-15].

For WBAN communications, IEEE has presented IEEE 802.15.6 standard optimized for low-power in body or on the body sensor nodes to serve various medical and nonmedical applications [16-18]. The security considerations in the IEEE 802.15.6 standard include four elliptic curve-based key agreement protocols that are used for generating a master key [19]. However, in [19], Toorani presented a security analysis of these protocols and indicated that all of them have security problems and are vulnerable to different attacks [20].

To mitigate security problems of this standard and to satisfy the data confidentiality and integrity requirements of the WBANs [21], numerous cryptographic-based security schemes have been proposed in the literature. Generally, the effectiveness of each cryptographic security solution largely depends on the underlying key management method [22, 23]. Numerous key management schemes and methods have been proposed for the WBANS which apply various cryptographic-based, channel-based, clock-based or biometric-based methods for key generation, key distribution, key agreement, key refreshing and other key management-rated operations.