Accepted Manuscript

Authenticated key management protocol for cloud-assisted body area sensor networks

Mohammad Wazid, Ashok Kumar Das, Athanasios V. Vasilakos

PII: S1084-8045(18)30296-0

DOI: 10.1016/j.jnca.2018.09.008

Reference: YJNCA 2208

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

Received Date: 17 May 2018

Revised Date: 30 July 2018

Accepted Date: 14 September 2018

Please cite this article as: Wazid, M., Das, A.K., Vasilakos, A.V., Authenticated key management protocol for cloud-assisted body area sensor networks, *Journal of Network and Computer Applications* (2018), doi: https://doi.org/10.1016/j.jnca.2018.09.008.

Authenticated key management protocol for cloud-assisted body area sensor networks

Mohammad Wazid [a], Ashok Kumar Das [b,*], Athanasios V. Vasilakos [c]

[a] *Cyber Security and Networks Lab, Innopolis University, Innopolis 420500, Russia*
E-mail: wazidkec2005@gmail.com
[b] *Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500 032, India*
E-mail: iitkgp.akdas@gmail.com, ashok.das@iiit.ac.in
[*] *Corresponding author*
[c] *Department of Computer Science, Electrical and Space Engineering, Lulea University of Technology, Lulea 971 87, Sweden*
E-mail: th.vasilakos@gmail.com

Abstract

Due to recent advances in various technologies such as integrated circuit, embedded systems and wireless communications, the wireless body area network (WBAN) becomes a propitious networking paradigm. WBANs play a very important role in modern medical systems as the real-time biomedical data through intelligent medical sensors in or around the patients' body can be collected and sent the data to remote medical personnel for clinical diagnostics. However, wireless nature of communication makes an adversary to intercept or modify the private and secret data collected by the sensors in WBANs. In critical applications of WBANs, there is a great requirement to access directly the sensing information collected by the body sensors by an external user (e.g., a doctor) in order to monitor the health condition of a patient. In order to do so, the user needs to first authenticate with the accessed body sensors, and only after mutual authentication between that user and the body sensors the real-time data can be directly accessed securely by the user.

In this paper, we propose a new user authentication and key management scheme for this purpose. The proposed scheme allows mutual authentication between a user and personal server connected to WBAN via the healthcare server situated at the cloud, and once the mutual authentication is successful, both user and personal server are able to establish a secret session key for their future communication. In addition, key management process is provided for establishment of secret keys among the sensors and personal server for their secure communication. The formal security based on broadly-accepted Real-Or-Random (ROR) model and informal security give confidence that the proposed scheme can withstand several known attacks needed for WBAN security. A detailed comparative analysis among the proposed scheme and other schemes shows that the proposed scheme provides better security & functionality features, low computation and comparable communication costs as compared to recently proposed related schemes. Finally, the practical demonstration using the NS2 based simulation is shown for the proposed scheme and also for other schemes.

Keywords: Authentication, key management, body area sensor networks, formal security, NS2 simulation.

1. Introduction

Information and Communication Technology (ICT) improves the healthcare quality and safety of the patients. It also increases the efficiency of healthcare system and its service delivery. In Wireless Body Area Network (WBAN), several intelligent medical sensors in or around the patients' body are deployed for real-time healthcare monitoring and support. The sensors are mobile and small size intercommunicating devices which are either wearable or implanted into the human body for monitoring the vital signs of a patient, such as heart rate, blood pressure and blood glucose meter. In WBAN, patient's health data is transmitted in the form of multimedia data, such as text, audio, image, and video [1]. Patient's health data is further used by the healthcare experts (ie., doctors, nursing staffs) to provide them the required medical assistance. However, there are challenges with WBANs that need to be carefully addressed before deploying such kind of networks. Firstly, the sensing devices have limited resources (for example, limited battery backup, bandwidth, memory, and computational capability). Therefore, it is desirable to design a lightweight communication protocol that should be utilized in WBAN. Secondly, it is related to privacy along with security of the patient's health data. Therefore, while deploying a WBAN, it is mandatory to provide privacy, confidentiality, authentication, and integrity to patient's health data which is in transit as well stored somewhere (i.e., healthcare server). A typical scenario of a cloud-assisted body area sensor network is given in Fig. 1. In this architecture, there are health servers over cloud, personal servers (i.e. personal digital assistant (PDA) devices where the personal private data from body area network is stored) and body sensors. Body sensors are deployed in a patient's body which monitor the physiological conditions of a patient, such as heart rate and blood glucose level, and then transmit the sensing data to their personal server that collects the private