Accepted Manuscript

A robust and anonymous patient monitoring system using wireless medical sensor networks

Ruhul Amin, SK Hafizul Islam, G.P. Biswas, Muhammad Khurram Khan, Neeraj Kumar

PII: S0167-739X(16)30150-9
DOI: http://dx.doi.org/10.1016/j.future.2016.05.032
Reference: FUTURE 3056

To appear in: *Future Generation Computer Systems*

Received date: 1 September 2015
Revised date: 23 May 2016
Accepted date: 25 May 2016

Please cite this article as: R. Amin, S.H. Islam, G.P. Biswas, M.K. Khan, N. Kumar, A robust and anonymous patient monitoring system using wireless medical sensor networks, *Future Generation Computer Systems* (2016), http://dx.doi.org/10.1016/j.future.2016.05.032

Available online at www.sciencedirect.com

ScienceDirect

(2016) –23

Journal Logo

A robust and anonymous patient monitoring system using wireless medical sensor networks

Ruhul Amin[1], SK Hafizul Islam[2,*], G.P. Biswas[1], Muhammad Khurram Khan[3], Neeraj Kumar[4]

Abstract

In wireless medical sensor network (WMSN), bio-sensors are implanted within the patient body to sense the sensitive information of a patient which later on can be transmitted to the remote medical centres for further processing. The patient's data can be accessed using WMSN by medical professionals from anywhere across the globe with the help of Internet. As the patient sensitive information is transmitted over an insecure WMSN, so providing the secure access and privacy of the patient's data are various challenging issues in WMSN environments. To provide secure data access, in the literature very less number of user authentication protocols are available. But, most of these existing protocols may not be applicable to WMSNs for providing user's anonymity. In this article, we propose an architecture for patient monitoring health-care system in WMSN and then design an anonymity-preserving mutual authentication protocol for mobile users. We used the AVISPA tool to simulate the proposed protocol. The results obtained indicate that the proposed authentication protocol resists the known attacks. In addition, the BAN logic model confirms mutual authentication feature of the proposed protocol. Moreover, an informal cryptanalysis is also given, which ensures that the proposed protocol withstands all known attacks. We perform a comparative discussion of the proposed protocol against the existing protocols and the comparative results demonstrate that the proposed protocol is efficient and robust. Specifically, the proposed protocol is not only effective for complexity and robustness against common security threats, but it also offers efficient login, robust mutual authentication, and user-friendly password change phases.

Keywords: Wireless medical sensor network; Password authentication; User anonymity; Hash function; AVISPA tool; BAN logic.

1. Introduction

With the advancement of wireless communication and mobile technologies, health-care industry utilizes these technologies in patient monitoring system, where the medical professional can monitor patient's health from anywhere and anytime. The medical professional monitors various health conditions of a patient through wireless communication using the mobile and the sensor devices. The sensor devices sense the health information of the patient, and send it to the medical professional via a gateway node of the WMSN. Since the sensitive patient information is transmitted through an open channel, so there is a big concern of message security against various types of active and passive attacks. To make secure communication between medical professional and patient, user authentication with session key agreement protocols [1, 2, 3, 4, 5] are widely used. In such protocols, after sharing a common session

*Corresponding author. (SK Hafizul Islam)

Email addresses: amin_ruhul@live.com (Ruhul Amin[1]), hafi786@gmail.com (SK Hafizul Islam[2,*]), gpbiswas@gmail.com (G.P. Biswas[1]), mkhurram@ksu.edu.sa (Muhammad Khurram Khan[3]), neeraj.kumar@thapar.edu (Neeraj Kumar[4])

[1]Department of Computer Science and Engineering, Indian School of Mines, Dhanbad 826004, Jharkhand, India

[2]Department of Computer Science and Information Systems, Birla Institute of Technology and Science, Pilani 333031, Rajasthan, India

[3]Center of Excellence in Information Assurance, King Saud University, Riyadh, Saudi Arabia

[4]Department of Computer Science and Engineering, Thapar University, Patiala 147004, Panjab, India