Computers and Electrical Engineering 000 (2017) 1–21

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks☆

Sravani Challa[a], Ashok Kumar Das[a,*], Vanga Odelu[b], Neeraj Kumar[c], Saru Kumari[d], Muhammad Khurram Khan[e], Athanasios V. Vasilakos[f]

[a] *Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500 032, India*
[b] *Department of Computer Science and Engineering, Indian Institute of Information Technology Chittoor, Sri City 517 588, India*
[c] *Department of Computer Science and Engineering, Thapar University, Patiala 147 004, India*
[d] *Department of Mathematics, Ch. Charan Singh University, Meerut 250 005, India*
[e] *Center of Excellence in Information Assurance, King Saud University, Riyadh, Kingdom of Saudi Arabia*
[f] *Department of Computer Science, Electrical and Space Engineering, Lulea University of Technology, Lulea 971 87, Sweden*

ARTICLE INFO

Article history:
Received 9 September 2016
Revised 4 August 2017
Accepted 7 August 2017
Available online xxx

Keywords:
Wireless healthcare sensor networks
User authentication
Session key
Elliptic curve cryptography
AVISPA
BAN logic
Formal security

ABSTRACT

We first show the security limitations of a recent user authentication scheme proposed for wireless healthcare sensor networks. We then present a provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks. The proposed scheme supports functionality features, such as dynamic sensor node addition, password as well as biometrics update, smart card revocation along with other usual features required for user authentication in wireless sensor networks. Our scheme is shown to be secure through the rigorous formal security analysis under the Real-Or-Random (ROR) model and broadly-accepted Burrows-Abadi-Needham (BAN) logic. Furthermore, the simulation through the widely-known Automated Validation of Internet Security Protocols and Applications (AVISPA) tool shows that our scheme is also secure. High security, and low communication and computation costs make our scheme more suitable for practical application in healthcare applications as compared to other related existing schemes.

1. Introduction

Developments in telecommunication and information technology helped in eliminating distance barriers while providing health care. Over the years, telemedicine using radio and telephone has been replaced with video-telephony, distributed client/server applications and devices that support home-care. This has facilitated remote monitoring of patients and thus has improved medical facilities in rural communities. Technology also allows doctors in multiple locations to share information and discuss cases. Apart from decreasing the number of required outpatient visits, use of telemedicine reduces the

☆ Reviews processed and recommended for publication to the editor-in-chief by area editor Dr. G. Martinez Perez.

* Corresponding author.

E-mail addresses: c.sravani@research.iiit.ac.in (S. Challa), iitkgp.akdas@gmail.com, ashok.das@iiit.ac.in (A.K. Das), odelu.vanga@gmail.com, odelu.vanga@iiits.in (V. Odelu), neeraj.kumar@thapar.edu (N. Kumar), saryusiirohi@gmail.com (S. Kumari), mkhurram@ksu.edu.sa (M.K. Khan), th.vasilakos@gmail.com (A.V. Vasilakos).

http://dx.doi.org/10.1016/j.compeleceng.2017.08.003
0045-7906/© 2017 Elsevier Ltd. All rights reserved.

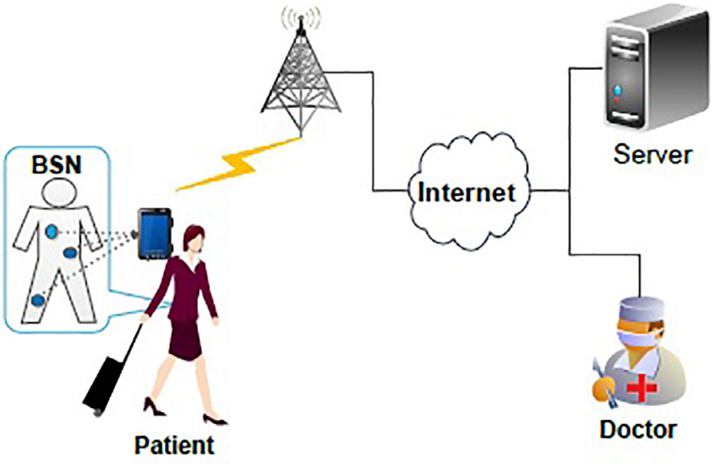

Fig. 1. A typical healthcare-monitoring scenario (Source: [1]).

overall cost of medical care. Telemedicine can be delivered using networks linking hospitals with community health centers in rural areas.

Wireless Sensor Networks (WSNs) for medical applications has been garnering a lot of attention in recent years due to advantages over wired alternatives such as enhanced mobility, reduced risk of infection, low cost etc. An emerging aspect of the telemedicine is the Wireless Body Area Network (WBAN), where each patient belonging to the system is provided with the body sensor nodes that collect and monitor vitals such as temperature, heart beat, blood pressure etc., irrespective of the patient's condition and location. The collected information is then received by a smart mobile device using any one of bluetooth, wi-fi, etc. The smart device forwards the information to a remote health care facility over a wi-fi or 3G/4G network. A typical healthcare-monitoring scenario is demonstrated in Fig. 1, which is adapted from the scheme [1]. Along with providing continuous monitoring by instantly updating patient's vitals for hospitals to store and process using wearable sensor devices, WSNs also help to detect emergencies sooner.

Multiple technical challenges need to be faced while setting up a WSN for health care. Along with the obvious limitations in a WSN, such as scarce energy reserves, processing and memory constraints, limited network capacity etc., any health care network imposes a definite requirement of quality of service, system reliability and above all, privacy and security. Since most sensor network deployment consists of stationery nodes that transmit data with focus on best effort data collection at the base station at a relatively low rate, there is a huge gap between the design of such networks and requirements of telemedicine. Also, as the sensor nodes are usually deployed over an unattended area, it may lead to a compromise of patient privacy either due to eavesdropping attacks or sensor node capture physically by an adversary.

1.1. Related work

This section outlines various authentication schemes proposed to secure health care sensor networks. Over the years, many researchers have come up with schemes to strengthen the security of wireless medical care networks. Malasri and Wang [2] implemented a secure key exchange protocol using Elliptic Curve Cryptography (ECC) to establish a shared key between sensor node and base station along with a two-tier architecture for user data authentication with the help of biometrics. Hu et al. [3] proposed a real-time hardware and software based protocol for monitoring cardiac patients. Wireless ECG communication unit, called a mobile platform, is integrated together. Although the scheme provides privacy and integrity, it does not include strong user authentication. Huang et al. [4] proposed a three-tiered sensor-based hierarchical architecture for monitoring health. Wireless Sensor Motes (WSM) and Wearable Sensor Systems (WSS) were placed strategically in each tier to broadcast data. Advanced Encryption Standard (AES)-based authentication and encryption is used at the WSS, while a polynomial-based encryption is used at the WSM to establish point-to-point secure communication.

In recent years, Le et al. [5] came up with a scheme supporting access control and mutual authentication using ECC. Also, they argue that the scheme is secure against known attacks like replay and denial-of-service attack. However, it has been proved that this scheme is vulnerable to eavesdropping compromising patient privacy. Das [6] proposed a two-factor user authentication protocol for WSNs claiming that the scheme is secure against known attacks like password-guessing, user impersonation, replay, node compromise and stolen-verifier attacks. However, Khan and co-workers [7,8] showed that this protocol is not secure against user impersonation and insider attack. Also, the scheme does not support mutual authentication and message confidentiality between the user and the sensor.

Please cite this article as: S. Challa et al., An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks, Computers and Electrical Engineering (2017), http://dx.doi.org/10.1016/j.compeleceng.2017.08.003