COMPUTER METHODS AND PROGRAMS IN BIOMEDICINE 135 (2016) 37–50

journal homepage: www.intl.elsevierhealth.com/journals/cmpb

Secure anonymous mutual authentication for star two-tier wireless body area networks

Maged Hamada Ibrahim [a], *Saru Kumari* [b], *Ashok Kumar Das* [c,*], *Mohammad Wazid* [c], *Vanga Odelu* [d,e]

[a] *Department of Electronics, Communication and Computers, Faculty of Engineering, Helwan University, 1, Sherif St., Helwan, P.O.11792, Cairo, Egypt*

[b] *Department of Mathematics, Ch. Charan Singh University, Meerut, Uttar Pradesh 250 005, India*

[c] *Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500 032, India*

[d] *Department of Mathematics, Indian Institute of Technology, Kharagpur 721 302, India*

[e] *Department of Computer Science and Engineering, Indian Institute of Information Technology, Chittoor, Sricity, Andhra Pradesh 517 588, India*

ARTICLE INFO

Article history:
Received 10 February 2016
Received in revised form
8 July 2016
Accepted 11 July 2016

ABSTRACT

Background and objectives: Mutual authentication is a very important service that must be established between sensor nodes in wireless body area network (WBAN) to ensure the originality and integrity of the patient's data sent by sensors distributed on different parts of the body. However, mutual authentication service is not enough. An adversary can benefit from monitoring the traffic and knowing which sensor is in transmission of patient's data. Observing the traffic (even without disclosing the context) and knowing its origin, it can reveal to the adversary information about the patient's medical conditions. Therefore, anonymity of the communicating sensors is an important service as well. Few works have been conducted in the area of mutual authentication among sensor nodes in WBAN. However, none of them has considered anonymity among body sensor nodes. Up to our knowledge, our protocol is the first attempt to consider this service in a two-tier WBAN. We propose a new secure protocol to realize anonymous mutual authentication and confidential transmission for star two-tier WBAN topology.

Methods: The proposed protocol uses simple cryptographic primitives. We prove the security of the proposed protocol using the widely-accepted Burrows-Abadi-Needham (BAN) logic, and also through rigorous informal security analysis. In addition, to demonstrate the practicality of our protocol, we evaluate it using NS-2 simulator.

Results: BAN logic and informal security analysis prove that our proposed protocol achieves the necessary security requirements and goals of an authentication service. The simulation results show the impact on the various network parameters, such as end-to-end delay and throughput. The nodes in the network require to store few hundred bits. Nodes require to perform very few hash invocations, which are computationally very efficient. The communication cost of the proposed protocol is few hundred bits in one round of communication. Due to the low computation cost, the energy consumed by the nodes is also low.

* *Corresponding author.* Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500 032, India. Fax: +91 40 6653 1413.

E-mail addresses: iitkgp.akdas@gmail.com, ashok.das@iiit.ac.in (A.K. Das).

http://dx.doi.org/10.1016/j.cmpb.2016.07.022

Keywords:
Wireless body area networks
Authentication
Anonymity
Key agreement
Security
NS2 simulation

Conclusions: Our proposed protocol is a lightweight anonymous mutually authentication protocol to mutually authenticate the sensor nodes with the controller node (hub) in a star two-tier WBAN topology. Results show that our protocol proves efficiency over previously proposed protocols and at the same time, achieves the necessary security requirements for a secure anonymous mutual authentication scheme.

1. Introduction

WBAN is a branch of wireless sensor networks, which are useful in monitoring and improving health conditions of people, surveillance of elder people, disabled people, etc. It can further enhance the quality of life by monitoring and examining the vital signs (e.g. heart rate, blood pressure, blood sugar levels, etc.) of healthy people in order to predict and avoid future health problems. Consider the scenario of a patient equipped with a number of wearable and implantable sensors that constantly measure various health-related parameters. Sensors (nodes) are networked meaning that they have communication capabilities and can interact with each other, and with a central network controller node that provides coordination as well as long-term storage. WBAN connects with external entities such as hospitals, clinics, etc. through the Internet.

There are a wide range of enabled applications based on the WBAN, such as Emergency Medical Response System (EMRS), Ubiquitous Health Monitoring (UHM), Computer-Assisted Rehabilitation, and even promoting healthy living styles. In UHM, WBAN frees people from visiting the hospital frequently, and eases the heavy dependence on a specialized workforce in health-care. Thus, it is a desirable technique to quickly build cost-effective health-care systems, especially for countries that lack medical infrastructures and well-trained staffs. In addition, in an EMRS, temporary WBANs can be rapidly deployed with minimum human effort at a disaster scene so that the vital signs of injured patients can be monitored and reported to the remote health center in time, which is potentially capable of saving the lives of numerous people [1]. Fig. 1 illustrates the architecture of a complete health-care system and the star two-tier WBAN subnetwork, which is applied in our proposed protocol.

Security and privacy issues have been described as two of the most challenging problems of WBANs [2–5]. As an example, *it has been demonstrated that an attacker equipped with a low-cost device can eavesdrop on the data communicated with a pacemaker and may even induce a cardiac arrest to a targeted patient* [6]. Health-related data have been the focus of several attacks almost since

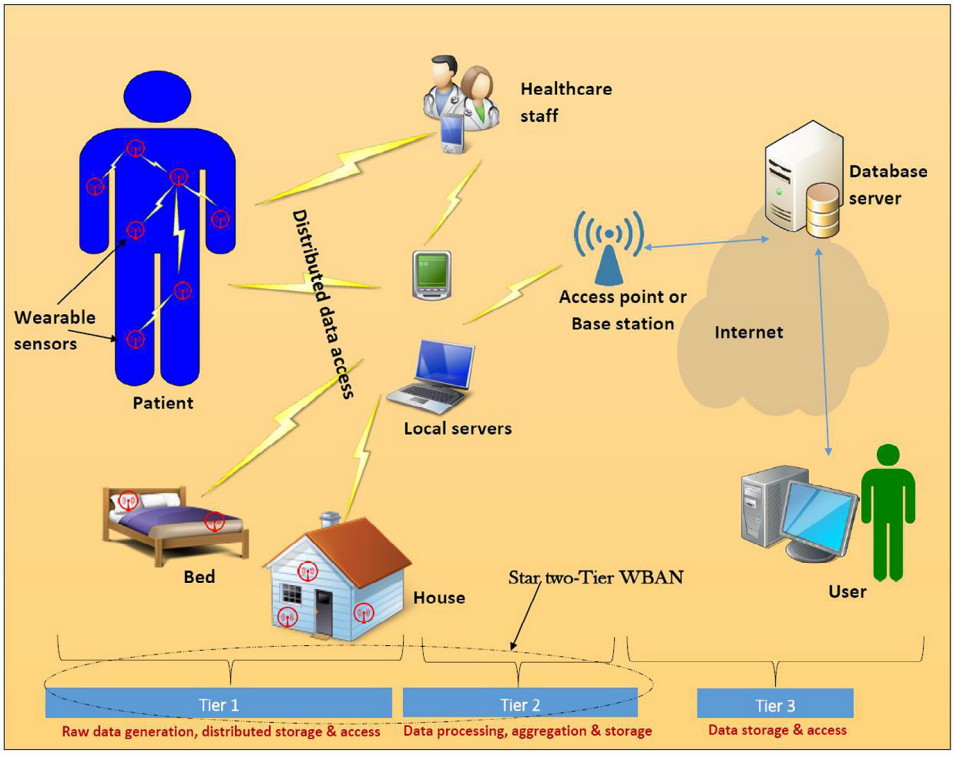

Fig. 1 – Architecture of a health-care system and the star two-tier WBAN subnetwork.