Accepted Manuscript

A lightweight multi-layer authentication protocol for wireless body area networks

Jian Shen, Shaohua Chang, Jun Shen, Qi Liu, Xingming Sun

PII: S0167-739X(16)30696-3
DOI: http://dx.doi.org/10.1016/j.future.2016.11.033
Reference: FUTURE 3239

To appear in: *Future Generation Computer Systems*

Received date: 25 July 2016
Revised date: 17 October 2016
Accepted date: 28 November 2016

Please cite this article as: J. Shen, S. Chang, J. Shen, Q. Liu, X. Sun, A lightweight multi-layer authentication protocol for wireless body area networks, *Future Generation Computer Systems* (2016), http://dx.doi.org/10.1016/j.future.2016.11.033

A Lightweight Multi-layer Authentication Protocol for Wireless Body Area Networks

Jian Shen[a,b,c,*], Shaohua Chang[a,c], Jun Shen[a,c], Qi Liu[a,c], Xingming Sun[a,c]

[a] *Jiangsu Engineering Center of Network Monitoring, Nanjing University of Information Science & Technology, China*
[b] *Jiangsu Collaborative Innovation Center on Atmospheric Environment and Equipment Technology, Nanjing University of Information Science & Technology, China*
[c] *School of Computer & Software, Nanjing University of Information Science & Technology, China*

Abstract

Nowadays, the technology of Internet of Things (IoT) is getting more and more important which brings a lot of convenience to people's life and city's development. As a key application of IoT, wireless body area networks (WBANs) provides people high quality of life and high level of medical service. However, due to the sensitiveness of medical system, security and privacy issues in WBANs are very important. In previous research, there are no comprehensive authentication protocols designed for WBANs according to its characteristics of network structure. In this paper, we propose an efficient multilayer authentication protocol and a secure session key generation method for WBANs. Firstly, we design a one-to-many group authentication protocol and a group key establishment algorithm between personal digital assistance (PDA) and each of sensor nodes with energy efficiency and low computational cost. Then, we present a new certificateless authentication protocol with no pairings based on certificateless cryptography between PDA and application provider (AP), using ECC algorithm that provides low computational cost with high security. In addition, the validation of the proposed protocol can be proved. Finally, the security and performance analysis shows that our protocol is secure and efficient.

*Corresponding author
Email address: s_shenjian@126.com (Jian Shen)