EAI Endorsed Transactions
on Scalable Information Systems
Research Article EAI.EU

Secure new node ID assignment for internet integrated wireless body area networks

Amit Kumar Gautam[1]* and Rakesh Kumar[1]

[1]Madan Mohan Malaviya University of Technology, Gorakhpur, Uttar Pradesh, India

Abstract

Internet integrated sensor networks have gained much importance and exponential growth in wireless body area networks (WBAN) over the last few years. These networks are used in health services to remotely monitor the health of patients and send/receive sensitive, time critical medical data. Because of the wireless and broadcast nature of WBAN, it is easy for an adversary to get, inject, or update the information transmitted in the medium or launch many security attacks. To protect the sensitive data of the patient, we propose a secure communication strategy for different sensors to form a WBAN. Here, a new node ID is assigned for sensors by using public key cryptography to communicate in the network. An energy utilization and communication cost analysis show that our approach incurs less communication overhead as compared with the recently proposed secure solutions in WBAN. The complexity analysis show that the proposed model works efficiently for secure communication in WBAN.

Keywords: Healthcare, Body area networks (WBANs), Security, New node joining, Cryptography

Received on 16 March 2020, accepted on 06 May 2020, published on 13 May 2020

doi: 10.4108/_____

*Corresponding author. gautam.biet@gmail.com

1. Introduction

The sensor network continuously provide services to various life changing application such as healthcare, agriculture, nuclear power plant monitoring, water monitoring, air pollution monitoring, weather prediction monitoring and earth sensing monitoring. As the critical applications adopt sensor network and tools, information must be protected, authenticated and secure [1].

One aspect of upcoming Internet is that everything having sensors and actuators have linked and incorporated in a bundle called Internet of Things (IoTs) [2]. Wireless Body Area Networks (WBAN) having sensors attached with the human body and an environment (such as rooms, operation table etc.) and forming WBAN have sensing, transmitting and processing capabilities and are integrated with Internet for immediate and fast healthcare services [3]. Due to security threats, data transferred from sensors should be shielded by an end-to-end (E2E) secured channel between the sensors and any communication object from the world. The establishment of secure channel needs to be authenticated. A strong key management schemes can permit two communication devices mutually authenticated and negotiated with secure keys which are used to protect the data from internal and external security attacks [4].