ARC'14
مؤتمر مؤسسة قطر السنوي للبحوث
QATAR FOUNDATION ANNUAL RESEARCH CONFERENCE
Towards World-class Research and Innovation

A Fully Functional Secure Ubiquitous Healthcare Monitoring System

10.5339/qfarc.2014.HBPP1030

Waiser Mehmood, Be; Ammad Hassan; Farid Touati; Ochirkhand Erdene-ochir; Adel Ben Mnaouer; Brahim Gaabab

Corresponding author :
waiser.mehmood@qu.edu.qa
Qatar University, Doha, Qatar

Abstract

I. BACKGROUND & O BJECTIVES
Recent advances in sensing, communication and actuation are leading to the next generation of Telemedicine when integrated with Wireless Body Area Networks (WBANs). They have a great potential in fostering the provision of next-generation Ubiquitous Healthcare (U-Health). However, deploying new technologies in healthcare applications without considering security makes patient privacy vulnerable, especially when we deal with highly sensitive physiological data of a patient such as heart-rate, position, temperature etc.
Because traditional security mechanisms have been designed for the systems with sufficient resources, they cannot be applied directly to the extremely resource constrained WBANs devices. Our main objective is to provide a lightweight security mechanism suitable for WBANs and propose a fully functional secure healthcare platform to monitor remotely the patients' health status.
II. METHODS
The proposed healthcare system (Fig. 1) integrates heterogeneous devices and wearable medical sensors. It informs the healthcare professionals by sending Patient Health Information (PHI) from Body Sensors to Body Router (BR). BR uses wireless local area network to communicate with Gateway in indoor environment, and it communicates with Server through 3G/4G in outdoor environment. Gateway and Server request Hardware Address Resolution Process (HARP) for security.
To guarantee the system security, we propose (i) a new lightweight encryption scheme based on stream cipher, where the encryption key is changed after each round of transmission to provide strong confidentiality (ii) an authentication mechanism is provided through HARP to authenticate BRs with their unique ID assigned before deployment and to guarantee that only authorized healthcare professionals can access to patients' data thanks to their biometrical information.
III. RESULTS
In order to investigate the feasibility of the proposed secure healthcare system, all components have been implemented in an experimental testbed. Zolertia is used as a wearable BS, which is a MSP430 microcontroller based sensor node equipped with CC2420 RF transceiver for wireless communication. Cubox is used as a BR, which is a low power ARM architecture. PCs are used as Gateway/Server and HARP.
Firstly, the security tests of the encryption scheme have been provided to check the randomness quality. The results were significantly higher (from 0.342178 to 0.974321) than the indicated threshold value (0.01) recommended by National Institute of Standards and Technology (NIST). Secondly, the end-to-end delay was around 97ms with encryption scheme and 94ms without encryption. Thus, the communication overhead incurred due to the encryption algorithm for each round is nearly 3ms.
IV. CONCLUSION
Experimental results have shown that our U-Health solution is feasible in real-world scenarios. The proposed encryption scheme passed all randomness tests recommended by NIST and the security