Computers and Electrical Engineering 000 (2017) 1–10

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

An encryption algorithm based on combined chaos in body area networks☆

Wei Wang[a], Miaomiao Si[a], Yu Pang[a], Peng Ran[a,*], Huiqian Wang[a,*], Xiaoming Jiang[a], Yu Liu[a], Jun Wu[b], Wei Wu[c], Naveen Chilamkurti[d], Gwanggil Jeon[e]

[a] Chongqing University of Posts and Telecommunications, Chongqing 400065, China
[b] Kaize Company, Chongqing 400050, China
[c] Sichuan University, Chengdu 610064, China
[d] La Trobe University, Plenty Road and Kingsbury Drive, Melbourne, VIC 3086, Australia
[e] Department of Embedded Systems Engineering, University of Incheon, 12-1 Songdo-dong, Yeonsu-gu, Incheon 406-772, Republic of Korea

ARTICLE INFO

Article history:
Received 10 November 2016
Revised 29 July 2017
Accepted 31 July 2017
Available online xxx

Keywords:
Encryption
Body area networks
Chaos
Key space
Sensitivity

ABSTRACT

Data encryption of sensor nodes is very important in body area networks (BANs) since the physiological data of an individual are highly sensitive. However, past encryption methods have small key space, which makes them vulnerable to attacks. In this paper, we propose a new encryption algorithm based on combined chaos. Firstly, Logistic and Kent chaotic mappings are introduced to produce two sub-matrices, and then a combined matrix is generated to perform XOR operation with the original data for encryption. The experimental results indicate that the proposed algorithm has a large key space, high key sensitivity and excellent attack resistance ability, and is feasible in privacy protection of BAN system.

1. Introduction

With the increasing needs of networks and the prevalence of chronic diseases such as hypertension and diabetes, applications related to wireless networks around the human body attract great attention, so the wearable system, body area network (BAN), has emerged which connects nodes with sensors in, on or around a human body as shown in Fig. 1. BAN can obtain human vital signs, supporting the remote clinical diagnosis, emergency treatment and health information service. For the user, the vital-sign information is extremely private [1] and only accessible to the authorized agencies. Security is essential in BAN, which supports the identity authentication, the privacy protection and the information completeness.

Traditional encryption techniques are applied in many areas [2–5]. For example, reference [6] studies searchable encryption in cloud computing and proposes a content-aware search scheme based on conceptual graphs. Reference [2] uses encryption and watermarking techniques to protect the image content and image features well from the semi-honest cloud server, and deter the image user from illegally distributing the retrieved images. Reference [7] proposes a coverless image steganography scheme based on scale invarient feature transform and bag of feature to realize secret communication.

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Guest Editor Dr. M. Karuppiah.

* Corresponding authors.
E-mail addresses: ranpeng@cqupt.edu.cn (P. Ran), wanghq@cqupt.edu.cn (H. Wang).

http://dx.doi.org/10.1016/j.compeleceng.2017.07.026
0045-7906/

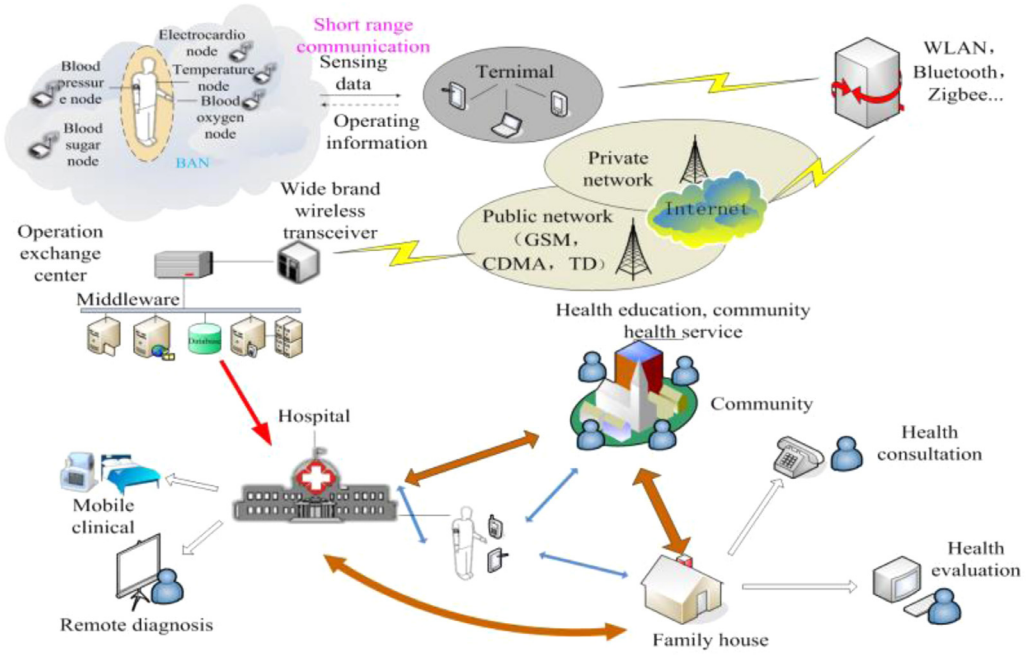

Fig. 1. The basic idea of BAN and its typical applications.

Reference [8] presents a framework for urban data sharing by exploiting the attribute-based cryptography to solve security issues in the cloud. Reference [9] studies a similarity search method for encrypted document based on simhash to find similar encrypted documents stored in cloud by submitting a query document.

Many encryption methods have been investigated and applied to BAN. A method is presented whose key is distributed beforehand [10]. When a sensor node sends the information, only the sensor nodes in the same system or the intelligent terminals can decrypt the received information. Reference [10] develops a group-based deployment model to improve key predistribution and proposes two key predistribution schemes including a hash key-based scheme and a polynomial-based scheme. However, since the source of BAN nodes is limited, the key predistribution schemes, key distribution center, RSA public key infrastructure and elliptic function public key infrastructure are not suitable for BAN applications. The algorithms of encryption and decryption mentioned before require a large number of operations, leading to rapid increase of power consumption. Considering the requirements of extreme low-power BAN nodes, the key pre-distribution scheme is not suitable for BAN system.

The second method uses the characteristics of the BAN channel as the key, which can randomly generate symmetric key between the sides of communication in the physical layer. Reference [11] generates the key in the receiver according to the value calculated of received wireless channel signal strength. Because of the inconsistent distance of the eavesdropper and the receiver, the signal intensity values will be different and the eavesdropper is unable to decrypt the data. Based on this achievement, reference [12] investigates channel characteristics for a dynamic BAN, and isolates a fast and a slow component, yielding keys at a fast rate and at a lower rate, respectively. The scheme using BAN channel encryption has been widely studied in recent years, but its keys are generated according to the signal intensity in the receivers. This method is too simple which may fail when the transmitters have the same distance with the eavesdropper and the receiver.

The third method generates the keys according to the physiological signs information. Different from the general sensor network nodes, the BAN nodes' parameters are the human physiological signs, which show different features according to different individuals. Even for the same individual, the values change slowly over time. Therefore, these parameters can be used as keys, especially the ECG signal which contains much information. Reference [13] conducts 512 points fast Fourier transform (FFT) of the ECG data for fixed time duration of 4 s, and selects the first 256 coefficients as the feature of ECG signals. This approach achieves better security performance in terms of several performance metrics such as false acceptance rate (FAR) and false rejection rate (FRR), and higher energy efficiency than other existing approaches. References [14] performs FFT and generate key using polynomial produced by obtained coefficients, which allows neighboring nodes to share the key without pre-deployment. Although the key generating approaches using physiological parameters are appropriate for BAN system, the eigenvalues of some parameters are similar without obvious changes over time, leading to weak encryption strength. The key generating process of these approaches is time-consuming, for example if the characteristics of heart rate variability (HRV) are selected as the key, the acquisition of ECG signals usually requires at least 5 min.

All above methods have obvious disadvantages of weak encryption strength leading to low resistance and sensitivity, so recently the chaotic encryption methods have been developed. Chaos is a kind of unpredictable and similar random

Please cite this article as: W. Wang et al., An encryption algorithm based on combined chaos in body area networks, Computers and Electrical Engineering (2017), http://dx.doi.org/10.1016/j.compeleceng.2017.07.026