Computer Methods and Programs in Biomedicine 162 (2018) 165–175

Contents lists available at ScienceDirect

Computer Methods and Programs in Biomedicine

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

Multiuser communication scheme based on binary phase-shift keying and chaos for telemedicine

J.A. Michel-Macarty[b], M.A. Murillo-Escobar[a], R.M. López-Gutiérrez[b], C. Cruz-Hernández[a,*], L. Cardoza-Avendaño[b]

[a] Electronics and Telecommunication Department, Scientific Research and Advanced Studies Center of Ensenada (CICESE), Ensenada, BC, Mexico
[b] Engineering, Architecture and Design Faculty, Autonomous University of Baja California (UABC), Ensenada, BC, Mexico

ARTICLE INFO

Article history:
Received 2 February 2018
Revised 30 April 2018
Accepted 16 May 2018

Keywords:
Chaotic communication
Encryption
Binary phase-shift keying
Telemedicine
Multiuser network

ABSTRACT

Background and objectives: Currently, telemedicine is levered upon the improvement in communication network technology such as Body Area Sensor Networks (BASN) to provided biomedicine solutions. Nevertheless, information security is an important issue since biomedical data is exchanged through insecure channels, which exposes private information that can be intercepted by malicious intruder. Therefore, secure communication protocols for multiuser networks in telemedicine applications are a big challenge. Recent chaos-based encryption works have been conducted in the area of medical secure communications with high security capabilities. However, none of them has considered multiuser network, which is used in several e-health applications. Up to our knowledge, the proposed protocol is the first attempt to consider this service in secure telemedicine. In this paper, we propose a novel scheme based on binary phase-shift key (BPSK) and chaos to provide information security at biosignals in a multiuser network system transmitting data over single channel.

Methods: The proposed scheme uses the two-dimensional Hénon map with enhance pseudorandom sequences and CDMA technique to achieve multiuser encryption process and transmit data over a single channel. We use biosignals such as electrocardiograms (ECG) and blood pressure (PB) signals from PhisioBank ATM data base for simulation results at MatLab software. We evaluate the security and performance by determining the secret key space, secret key sensitivity, resistance against noise attack with quality analysis by using BER, MSE, and PSNR, encryption-decryption time, and throughput.

Results: In simulations tests, biosignals of ECG and BP in a BANS network are encrypted and transmitted over shared wireless channels and just authorized medical personal can retrieve such information with corresponding secret key from the cryptogram, that appears as noise to any intruder. The proposed multiuser scheme support high noise and interference attacks efficiently in contrast with classic chaos-based encryption works for telemedicine, where some scenarios are simulated with very low BER, very low MSE, and high PSNR between plain biosignals and recovered biosignals when high AWGN noise is added to encrypted-transmitted signal. In addition, the encryption process presents enough key space and high sensitivity at secret key. A comparative analysis of proposed method and recent existing works was also presented.

Conclusions: Patients can be monitored and diagnosed opportunely remotely and all their medical information is transmitted securely to the correct specialist. Also, it is possible to transmit several electrophysiological signals in a single channel in a secure multiuser network at low cost optimizing the use of available bandwidth for telemedicine applications.

1. Introduction

Telemedicine application had been developed since 1970s with a limited use of treating patients in remote places. Nowadays, telemedicine provides services and medical information to several purposes with use of telecommunication systems, such as re-

* Corresponding author.
E-mail addresses: antonio.michel@uabc.edu.mx (J.A. Michel-Macarty), mmurillo@cicese.mx (M.A. Murillo-Escobar), roslopez@uabc.edu.mx (R.M. López-Gutiérrez), ccruz@cicese.mx (C. Cruz-Hernández), lcardoza@uabc.edu.mx (L. Cardoza-Avendaño).

https://doi.org/10.1016/j.cmpb.2018.05.021
0169-2607/

mote diagnosis of people with chronic diseases (such as hypertension, asthma, cardiovascular, and diabetes), transfer of clinical data (treatment, prescription drugs, laboratory tests, physiologic monitoring data, hospitalization, patient insurance, etc.), and even surgical procedures.

As a result of new electronic medical devices and telecommunications technologies, health systems are much more complex with several advantages over traditional health systems. For example, electronic devices provide more reliable information over physiological parameters, which can be seen in remote location in real-time by using channels such as Internet. Nevertheless, Internet was designed to optimize information sharing rather than security. Therefore, applications of telemedicine are subject to several inherent security risk and medical information of patients must be process to provide confidentiality and privacy to avoid incorrect diagnosis, treatment or identity theft.

Recently, an evolution of medical services platforms is taking place, changing from desktop computers to mobile and wireless devices. Wireless technologies have potential to replace thousands of wires in a hospital, it is very reliable, and allows mobility for patients and doctors. In addition, it is a low cost solution to improve patient accessibility and it improves quality of life of patients [1]. This medical support is known as mobile health or e-health. E-health includes wearable medical devices interconnected with wireless technologies [2]. Medical security has been studied previously in this context, e.g. see [3–7].

Advances in embedded systems allow developing new medical devices less invasive [8]. Biosignals data could be store in remote locations and even in the "cloud". As private medical information travels through public networks, it is important to provide information security because malicious intruders could access such personal information [9]. Patients could be prejudiced or damaged if a malicious intruder access information regarding diseases or health issues. Wireless sensors are used on patients located in different rooms at the hospital in order to have continuous monitoring and this private information could be accessed by unauthorized people. Therefore, there is a need to protect from the source personal data in multiuser networks.

In last years, digital chaos-based cryptography have been proposed in literature for images, biometrics, telemedicine, alphanumeric text, among others, since chaotic systems present several properties such as non-linearity, "random" like dynamics, deterministic, inherent wide bandwidth, high sensitivity at initial condition, mixing, ergodicity, among others, which are related with confusion, diffusion, complexity, and randomness of cryptosystems. For example, authors presented in [10] a scheme of cryptanalysis and improvement of a chaos-based image encryption algorithm with circular inter-intra-pixels bit level permutation. An efficient method for image encryption based on the chaos theory and a DNA (Deoxyribonucleic acid) sequences database was proposed in [11]. In [12], authors presented a detailed survey of biometric cryptosystems and cancelable biometrics along with the open issues and challenges. Chaos-based encryption has been proved to be very useful in previous works achieving high security, see e.g. [13–18].

Currently, some advances of chaos-based cryptography in telemedicine have been proposed in literature. In [19], authors proposed a novel symmetric encryption algorithm based on logistic map with double chaotic layer encryption (DCLE) for privacy of clinical information such as electrocardiograms (ECG), electroencephalograms (EEG), and blood pressure (BP). In [20], Kenfack and Tiedeu presented a system for chaos-based encryption of electrocardiographic signals with colpitts chaotic oscillator. In [21], Lin proposed a chaotic visual cryptosystem using an empirical mode decomposition (EMD) algorithm for clinical electroencephalography (EEG) signals. The basic design concept is to integrate two-dimensional (2D) chaos-based encryption scramblers, the EMD algorithm, and a 2D block interleaves method to achieve a robust and unpredictable visual encryption mechanism. In 2017, Pandey et al. proposed patient's confidential data hiding scheme in electrocardiogram (ECG) signal and its subsequent wireless transmission. Personal data is embedded in ECG (called stego-ECG) by using chaotic map and the sample value difference approach. Statistical and clinical performance measures were presented to validate the proposed scheme [22]. Nevertheless, most of above cryptographic implementations encrypts limited data of just one user and it does not present robustness against noise attack, see. e.g. [19,21].

On the other hand, the binary phase-shift keying (BPSK) is a digital modulation process to transmit data by changing two phases (two binary digits) of a reference signal (sine or cosine). BPSK is a basic technique widely implemented in several wireless communications standards to achieve greater power efficiency and higher data rates, such as in Code-Division Multiple Access (CDMA), Wireless Local Area Network (WLAN), Cable modem, Bluetooth, among others. In hostile communications environments, spread-spectrum modulation can be used to provide security by spreading sequences like pseudo-noise sequences, but channel bandwidth and transmitting power is sacrificed to provide robustness against noise and interference. The multiple-access communication system is another application of spread-spectrum modulation, where several users (independent) share just one channel to communicate without synchronization mechanisms, such as in CDMA.

In relation to previous works related with phase-shift keying (PSK) and chaos, Carroll presented in 2017 an alternative to the synchronization problem of transmitter and receiver for encoding information. Chaotic signals are broad-band and unpredictable, making them potentially useful when the goal is low interference communications or even low probability of detection (LPD) communications. In this work, a set of randomly chosen chaotic sequences is used to synchronize a chaotic transmitter to a receiver and two methods are presented to encoding information [23]. In [24], authors proposed a binary phase shift keying-ultra wide band (BPSK-UWB) system in which multiple accesses are defined by chaotic time hopping. They showed that the performance of the proposed system depends on the invariant probability density of the used chaotic transformation. In addition, multi-user spread-spectrum modulation schemes and chaos have been proposed in literature, see e.g. [25–27].

Motivated by all this situation, in this paper we propose a novel secure multiuser scheme to provide privacy at bio-signals based in chaos and BPSK, so that patients can be monitored and diagnosed opportunely remotely and all their medical information is transmitted securely to the correct specialist by using just one channel. In addition, if correct physician has access to their corresponding medical information (e.g. cardiology or sport medicine for ECG and PB, neurology or neurosurgery for EEG, orthopedics, plastic surgery, pediatrics or psychiatry for EMG, etc.), the multiuser network can be more efficient with faster diagnosis. To the best of our knowledge, this work that uses spread spectrum with chaos for medical signals in BASN has not been reported before. The proposed scheme is based on N number of patients with M specialists, where the patient can have different wireless sensors to monitor and send their medical data to different specialists. The specialist in turn must distinguish which patient is involved. The encryption method support additive noise and interference from other signals as well as protection against intruders. In simulations tests, biosignals of ECG and blood pressure are encrypted and transmitted over shared wireless channels and authorized medical personal can retrieve such information from cryptograms that appears as noise to any intruder.

This paper is organized as follows: the proposed secure multiuser network scheme is described in Section 2. The experimental