Computers and Electrical Engineering 000 (2017) 1–14

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

An efficient secure communication for healthcare system using wearable devices☆

P. Vijayakumar[a,*], P. Pandiaraja[b], Marimuthu Karuppiah[c], L. Jegatha Deborah[a]

[a] University College of Engineering Tindivanam, Melpakkam, Tindivanam, Tamil Nadu 604 001, India
[b] Arunai Engineering College, Mathur, Tiruvannamalai, Tamil Nadu 606 603, India
[c] School of Computing Science and Engineering, VIT University, Vellore 632 014, India

ARTICLE INFO

Article history:
Received 7 December 2016
Revised 14 April 2017
Accepted 14 April 2017
Available online xxx

Keywords:
e-healthcare
Cloud
Authentication
Confidentiality
Wearable device

ABSTRACT

In the present healthcare scenario, mobile phones play a vital role in performing secure text communications between different entities such as doctors, patients, hospitals, ambulances and other healthcare systems. Therefore, an efficient alert system for sending the private and confidential SMS messages has been proposed in this research work to send SMS alerts to healthcare entities from a heart patient. Very few research works have been proposed for multicast communication in SMS and each research work exposes some drawbacks as well. Since the proposed approach needs only one mod operation, the computational overhead of the proposed protocol is very low. Thus, the main advantage of this proposed work is that the messages are sent in a computationally efficient way and the experimental results confirm that the proposed work ensures end-to-end security with lower computational and communication overheads than the recent works in the literature.

1. Introduction

The first SMS message was sent on 3rd December 1992 in England through a Vodafone GSM network [10] and the text of the first SMS was “Merry Christmas” [1]. On an average, 193,000 SMS messages are sent every day through different service providers in the world. Though SMS messages are used for many communications, their use in the medical domain and especially in the healthcare profession is all the more vital than in any other field. One of the important scenarios in which SMS communication has proved its mettle is providing alert messages about the health of a patient who has been hospitalized for heart related ailments. A patient might have recently suffered from a severe heart attack and needs continuous medication for the well being of his/her life. In such a situation, a system which constantly monitors the body parameters of the patient and analyzes the probability of another heart attack or any other severe ailment and sends an alert SMS will be highly useful. Atleast one of the entities which has received the Multicast alert SMS message will turn up to aid the patient and hence will provide immediate response to the patient.

The cellular networks do not provide confidentiality, authentication and end-to-end security [2,3]. In such situation, SMS messages will be in danger of facing hackers and eavesdroppers [8,17,20]. Moreover, the identity verification in this context is much more important as high profile patients are in need of authentication before establishing the communications. In

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

* Corresponding author.
E-mail addresses: vijibond2000@gmail.com (P. Vijayakumar), sppandiaraja@gmail.com (P. Pandiaraja), marimuthume@gmail.com (M. Karuppiah), blessedjeny@gmail.com (L. Jegatha Deborah).

http://dx.doi.org/10.1016/j.compeleceng.2017.04.014
0045-7906/

such scenarios, authenticating the patient, doctor and other entities involved should be given utmost importance. In terms of energy availability, processor and RAM availability, smart phones show lower performance. Hence, the objectives of the proposed protocol can be summarized as follows.

A) To set up a secure Multicast SMS alert system by monitoring the necessary parameters of patients and to send alerts during emergency situations.
B) To provide end-to-end security in terms of authentication and confidentiality.
C) To ensure low computational overhead during the key exchange for Multicast SMS communications.
D) To reduce the communication cost during the key exchange process.

To ensure a secure Multicast SMS alert system, necessary wearable devices such as sensors are embedded in the body of a patient to continuously monitor the health condition. The sensors continuously read the corresponding data and send them to the ARM (Advanced Reduced Instruction Set Computing Machine) controller attached to the body of the patient forming a Body Area Network (BAN). The ARM controller in turn makes use of a GSM (Global System for Mobile Communication) Module present in the body and forwards the data to the Health Analysis Manager (HAM) which is present in the public cloud. The HAM, makes use of fuzzy logic [11] to analyze the received data. If the analysis shows that a medication is being needed by the patient, then the HAM sends a message containing the required medication to the patient. If the analysis result suggests that an emergency situation prevails, then an emergency alert message is sent to the doctor, relative, ambulance, hospital and the patient. In order to send this message to a group of people, a computationally efficient and secure multicast communication system is proposed in this paper. Since the proposed work takes less mathematical operations, it is computationally efficient. Moreover, the proposed work takes only a less number of messages to be communicated between the patient mobile and to other parties to perform the secure multicast communication.

The rest of this research work based on Multicast SMS has been organized as follows. Section 2 clearly outlines the recent works in multicast communications, SMS communications, and e-healthcare domain. Section 3 provides the overview of the Multicast SMS alert system. The proposed work and its model are explained in Section 4. The detailed mechanism of the proposed protocol is also mentioned in this section. The security strength of the proposed protocol is analyzed in Section 5. Recent works and the proposed work are compared and the results are mentioned in Sections 6 and 7 conclude and give future directions in the scope of this research work.

2. Literature survey

Support for multicast SMS has been provided by cellular networks since a long time ago [12–14]. The significance of multicast communication and methods for implementing the same has been represented by a number of present day authors and many in the recent past [2,3]. Vijayakumar et al. in [4] proposed that the rotation based algorithms can be combined with merging and batch balanced algorithms to improve the efficiency, but the limitation in this proposed approach is that it works better for batch leave operations than batch join operations (JM $<$ LM). Also, the works proposed by Vijayakuar et al. [5,6] showed reduced computational complexity while ensuring the secure group communication.

Vijayakumar et al. [11] have also devised a new dual authentication scheme for improving the security of vehicles that are in communication with the VANET environment and dual key management scheme for secure data transmission. The newly proposed algorithm also takes single broadcast messages from TA to inform the group members in order to recover the updated group key. The schemes proposed by Vijayakumar et al. ensure authentication, but confidentiality is not given much importance. Moreover, it is not related to health environments.

Onashoga et al. [15] had proposed a secure method for sending multicast SMS messages for the e-governance applications in Nigeria. The reason for providing security and privacy to multicast SMS is that they have attempted to provide citizen centric services to the residents of Nigeria through mobile phones. Mark and John [16] applied for a patent regarding the provision of security to SMS during medical data exchange. In this novel work, it was illustrated that a mobile phone could be used as a tool for sending the data packets to the medical service station which receive the packets. To ensure the security to communication, the messages were encrypted and signed before being sent.

Lee et al. [18] proposed that portable mobile healthcare has the potential to reduce long-term costs to improve the quality of medical services, but it also faces many technical challenges. Chein and Tai [19] analyzed the application of a PDA (Personal Digital Assistant) and the Bluetooth technology to a wireless-type physiological signal measuring system and the feasibility of the system. Recently, a system which provides secure transmission of data in distributed wireless medical sensor networks (WMSNs) in hospitals was proposed by Othman et al. [21]. In this work, the WMSNs continually update the status of the patient under continuous supervision to the doctor to make emergency decisions on demand based on the sensitive data collected from the body of the patient. A work proposed by Han et al. [22] collects the vital parameters of a patient using a BAN (Body Area Network) and sends them to the cloud servers where the final decisions are made. This work preserves the privacy of the user with reduced communication complexity.

A new scheme proposed by Smys and Kumar [23] uses cloud assisted BANs to collect the important health data from the patient and send the analytical results to the caretaker, emergency care and the physicians with improved security. The main limitation of these works is the memory availability and the need for further reduction in communication complexity. Another work by Liu et al. mentioned in [24] provides certificate less secure authentication scheme in barns with

Please cite this article as: P. Vijayakumar et al., An efficient secure communication for healthcare system using wearable devices, Computers and Electrical Engineering (2017), http://dx.doi.org/10.1016/j.compeleceng.2017.04.014