ISSN:0975-1459
Journal of Pharmaceutical Sciences and Research
www.jpsr.pharmainfo.in

Secure Patient Data Transmission in Sensor Networks

A.Surendar[1], M.Kavitha[2]

[1]Assistant Professor,Vignan's University,Andhra Pradesh India.
[2]Assistant Professor,AVS College of Technology, India.

Abstract
In WMSN patient's health parameters are collected by wearable or implantable sensors which is implemented in hospitals, these PHI are stored in the database.
Adversary can drop messages by jamming the communication channel, modify messages. so problem may occur .
In existing project, they provide the security for that database using some techniques and fine-grained data access control.
In our project we propose Symmetric key encryption/decryption for more security purpose. This helps to avoid the modification of patient's details

I. Introduction

Recently, with the rapid development in wearable biosensor and wireless communication technologies, wireless medical sensor networks (MSNs) have emerged as a promising technique which will revolutionize the way of seeking healthcare at home, hospital, or large medical facilities [1], [2]. Instead of being measured face-to-face, with MSNs, patients' health-related parameters can be monitored remotely, continuously, and in real time, and then processed and transferred to medical databases. This medical information is shared among and accessed by various users such as healthcare staff, researcher-s, government agencies, insurance companies, and patients. Through this way, healthcare processes, such as clinical di-agnosis and emergency medical response, will be facilitated and expedited, thereby greatly increasing the efficiency of healthcare.

Fig. 1 shows the architecture of a typical MSN. A large scale MSN accommodates tens of patient area networks (PANs). Each PAN consists of some biosensor nodes and a local

In existing project ,they provide the security for that database using some techniques and fine-grained data access control.

In our project we propose Symmetric key encryption/decryption for more security purpose.

This helps to avoid the modification of patient's details.

deal with user authentication for medical data. Moreover, the collected data from a biosensor is transmitted to the controller in plaintext. Thus, an adversary can easily modify the medical data and/or inject polluted medical data into the network. Some researchers (e.g., [7], [8]) utilize physiological signals (e.g., heart rate interval, blood flow, and electrocardiography) obtained from the patient to enable biosensors to agree upon a symmetric (shared) cryptographic key in an authenticated man-ner. However, they demand that each biosensor can measure the same physiological parameter, this assumption is rather restrictive and makes this method not suitable for many MSN applications.

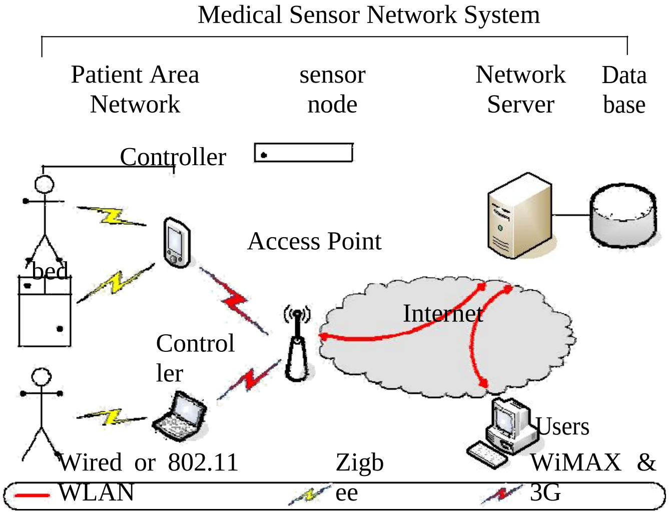

Fig. 1. The architecture of a typical medical sensor network.

II. Literature Survey

Sensor network for emergency response: challenges and opportunities, K. Lorincz, D. Malan, T. Fulford-Jones, A. Nawoj, A. Clavel, V. Shnayder, G. Mainland, S. Moulton, and M. Welsh,

Method : Code Blue

Code Blue integrates sensor nodes and other wireless devices into a disaster response setting and provides facilities for ad hoc network formation, resource naming and discovery, security, and in- network aggregation of sensor-produced data.

Advantages-RF-based location tracking

Drawbacks-Computation inefficient, cannot fulfill the stringent delay requirements in Medical Sensor Networks.

This security techniques are ill-protected against Denial-of-Service attacks.

Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey, P. Kumar and H.-J. Lee,

Method : Alarm-Net

Healthcare applications are considered as promising fields for wireless sensor networks, where patients can be monitored using wireless medical sensor networks (WMSNs).

Alarm-Net designed for patient health monitoring in the assisted-living and home environment.

Advantage-Alarm-Net facilitates network and data security for physiological, environmental, behavioral parameters about the residents.

Drawbacks-Monitoring and Eavesdropping on Patient Vital Signs.

Activity Tracking Threats-Location Threats

II. EXISTING SYSTEM

Wireless medical sensor networks (MSNs) is a key enabling technology in e-healthcare that allows the data of a patient's vital body parameters to be collected by wearable or implantable biosensors. However, the security and privacy protection of the collected data is a major unsolved issue, with challenges coming from stringent resource constraints of MSN devices, and the high demand for both security/privacy and practicality. In this paper, we propose a lightweight and secure system for MSNs. The system employs hash-chain based key updating mechanism and proxy-protected signature technique to achieve efficient secure transmission and fine-grained data accesscontrol. Furthermore, we extend the system to provide backward secrecy and privacy preservation. Our system only requiressymmetric-key encryption/decryption and hash operations and isthus suitable for low-power sensor nodes. This paper also reportsthe experimental results of the proposed system in a network ofresource-limited motes and laptop PCs, which show its efficiencyin practice. To the best of our knowledge, this is the first securedata transmission and access control system for MSNs until now sink (or user) data authentication. Thus, false medical data could be injected or treated as legitimate due to the lack of node authentication. Thirdly, IBE-Lite cannot resist node replication attacks. That is, an adversary can insert additional hostile biosensors into the network. Fourthly, the master key of each PAN consists of n secret keys, which are picked by the patient. Each doctor uses the secret key from the certificate authority to decrypt the messages encrypted by a sensor node. Once a doctor sends n user queries to a target PAN, he/she is able to generate the master key of the PAN. Thus, to ensure the security of IBE-Lite, the number of user queries has to be limited. Le et al. [12] presented a mutual authentication and access control protocol, which is based on ECC. A recent study [13] has shown that the scheme is susceptible to information-leakage attacks.

Although there are a lot of works about generic WSNs and mobile ad hoc networks (MANETs) security (e.g., [14]–[16]), these mechanisms are not directly applicable in MSNs due to the unique and challenging operational and security requirements of MSNs. For instance, the authors of [14] introduce a novel approach to ensure distributed privacy-preserving access control, which is built on a ring signature technique. Also, in [15], a self-contained public key-management scheme has been proposed for wireless ad hoc networks, in which a small controller of a target PAN) responds to the user's command. Fig. 2 illustrates the flows of security information of the proposed system. More detailed description will be provided in the following subsections.

IV. THE PROPOSED SYSTEM

Here we proposed a lightweight and secure system for wireless medical sensor networks (MSN).Each patient area network (PAN) consists of some biosensors and a controller. These biosensors collect his/her personal health information(PHI) like body temperature, blood pressure, heart bear rate, blood glucose level etc.. Sensors forward the information to the controller.

The security techniques are Hash-chain based key updating mechanism Proxy Protected Signature Technique During each and every transmission of medical data from sensor to medical server the hash key gets updated.

During user registration, the user receives the proxy key from the medical server. Using the proxy key the user enter into system and access the patient's medical data from the medical server. Here we provide the encryption and decryption mechanism using blowfish algorithm. The information which is travelled from sensor to network is encrypted using blowfish algorithm.

The information which is retrieved by the doctors is decrypted using blowfish algorithm

Advantages

- In this system computational and storage requirement on a biosensor is very low.
- It uses simple cryptographic operations i.e. hash operations. So there is no delay in this system.
- Proxy protected signature key is used for user authentication.
- Fine-grained access control is given for the user

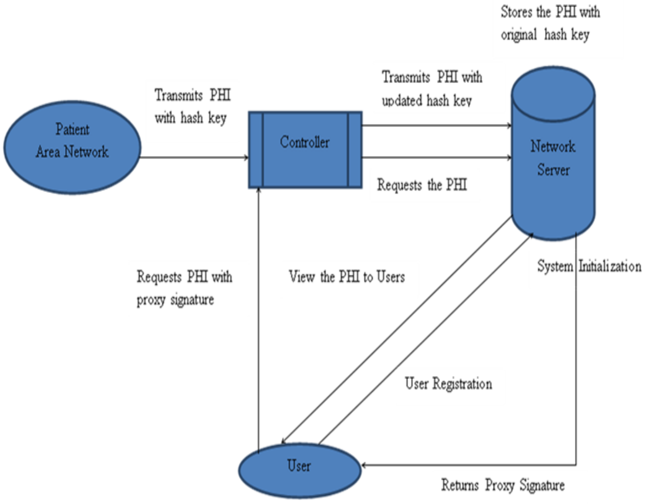

Figure 2 Architectural design

Modules

- System Initialization
- User Registration and Proxy Key Generation
- Transmission of Patient Health Information to Network Server
- Controller authentication
- Retrieval of Patient Health Information from Network Server

V.IMPLEMENTATION

SHA-1

SHA-1 is a cryptographic hash function. SHA stands for "secure hash algorithm". The four SHA algorithms are structured differently and are named SHA-0, SHA-1, SHA-2, and SHA-3.

In our work we use SHA-1 algorithm for key generation in patient area network.

In the patient area network the key is generated using the SHA-1 algorithm. During transmission to the controller one hash key is generated. Afterwards from the controller to the medical server new hash key is generated.

But the important thing is that the sensor and medical server only know the original hash key. In this data transmission the security level is fully depend on the hash key. Here we use SHA-1 algorithm for key generation

Blow Fish Algorithm

Blowfish has a 64-bit block size and a variable key length from 32 bits up to 448 bits and making it ideal for securing data.

It is a variable-length key block cipher. It is suitable for applications where the key does not change often, like a communications link or an automatic file encryption.

Blowfish is a symmetric block cipher that can be used as a drop-in replacement for AES or IDEA.

Blowfish was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms.

It has been analyzed considerably, and it is slowly gaining acceptance as a strong encryption algorithm

Much faster than AES and IDEA.

Advantages:

It is suitable and efficient for hardware implementation. Besides, it is unpatented and no license is required.

Blowfish has been subject to a significant amount of cryptanalysis, and full Blowfish encryption has never been broken.

Blowfish is also one of the fastest block ciphers in public use

VI. CONCLUSION

Here we proposed a secure and lightweight system for wireless medical sensor network. The medical data transmission is done in a secure manner using hash chain based key updating mechanism.Fine-grained access control was achieved using proxy protected signature technique.The two security techniques such as hash-chain based key mechanism and proxy key signature technique achieves the goal i.e. secure patient medical data transmission and access control in the wireless medical sensor network.

REFERENCES

[1] K. Lorincz, D. Malan, T. Fulford-Jones, A. Nawoj, A. Clavel, V. Shnay-der, G. Mainland, S. Moulton, and M. Welsh, “Sensor networks for emergency response: challenges and opportunities,” IEEE Pervasive Computing, vol. 3, no. 4, pp. 16-23, Oct. 2004.

[2] V. Shnayder, B.-R. Chen, K. Lorincz, T. R. F. Fulford-Jones, and M. Welsh, “Sensor networks for medical care,” Technical Report TR-08-05, Harvard University, 2005.

[3] K. Malasri and L. Wang, “Addressing security in medical sensor networks,” in Proc. ACM HealthNet, pp. 7-12, 2007.

[4] P. Kumar and H.-J. Lee, “Security issues in healthcare applications using wireless medical sensor networks: a survey,” sensor, vol. 12, pp. 55-91, 2012.

[5] D. He, J. Bu, S. Zhu, S. Chan, and C. Chen, “Distributed access control with privacy support in wireless sensor networks,” IEEE Trans. Wireless Commun., vol. 10, no. 10, pp. 3472-3481, Oct. 2011