IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Volume-3, Issue-1 E-ISSN: 2347-2693

A Survey on Major Security Issues for Health Data in Wireless Medical Sensor Networks

C. Gayathri[1*] and D.Sathya[2]

[1*,2]*Computer Science & Engineering, Kumaraguru College of Technology, India*

www.ijcaonline.org

Received: Dec/22/2014 Revised: Jan/12/2015 Accepted: Jan/19/2015 Published: Jan/31/2015

Abstract— Wireless Sensor Networks (WSN) is an emerging technology that has the potential to transform the way of human life. Healthcare applications are considered a promising field for Wireless Sensor Network, where the patient's health can be monitored using Medical Sensors. Wireless Medical Sensor Networks (WMSNs) are the key enabling technology in healthcare applications that allows the wearable biosensors to collect the patient's vital body parameters to be collected by wearable biosensors. Currently WMSN healthcare research focuses on reliable patient communication, mobility of patient and energy-efficient routing. Security and Privacy protection of the collected data are the major issues to be solved in medical sensor networks. This paper deals with various techniques adopted for securing the medical data during the transmission and also deals with the avoidance of unauthorized access.

Keywords— Access Control, Data Transmission, Medical Sensor Networks, Security, Privacy.

I. INTRODUCTION

Wireless Sensor Network (WSN) is a self-configure network of small sensor nodes, where the sensor nodes can communicate among themselves using radio signals, and these sensor nodes can sense, monitor and understand the physical environment. It consists of spatially distributed sensors to monitor physical or environmental conditions and to pass the data through the network to a destination location. The bi-directional modern networks enable to control the activity of the sensors. The development of the wireless sensor networks was motivated by military applications such as battlefield surveillance and is also used in many industrial and consumer applications like industrial process monitoring and control, machine health monitoring, etc. The WSN is built of "nodes", where one or more sensor is connected to each node. Each sensor node consist of several parts, like radio transceiver with an internal antenna to an external antenna, microcontroller, electronic circuit for interfacing with the sensors and an energy source like a battery.

II.WIRELESS MEDICAL SENSORNETWORKS

WSNs deployed at a large scale in a distributed manner, and their data rates differs based on their applications, where the Wireless Medical Sensor Networks have direct human involvement are deployed on a small scale must support mobility (a patient can carry the devices), and WMSNs requires high data rates with reliable communication. Physiological conditions of patients are closely monitored by deploying Wireless medical sensor motes.

These medical sensors are used to sense the patient's vital body parameters and transmit the sensed data in a timely fashion to some remote location without human involvement. Using these medical sensor readings the doctor can get the details of a patient's health status. The patient's vital body parameters include heart beats, body temperature, blood pressure, sugar level, pulse rate.

WMSNs carry the quality of care across wide variety of healthcare applications. In addition, other applications that also benefit from WMSNs include sports-person health status monitoring and patients self-care. Several research groups and projects have started to develop health monitoring using wireless sensor networks, for example, CodeBlue, LiveNet, MobiHealth.

The wireless healthcare application offers many challenges, such as, reliable and secured data transmission, mobility of nodes, event detection, timely delivery of data, power management, node computation, etc. Deploying new technologies in healthcare applications without considering security often makes patient privacy vulnerable. For instance, the patient's physiological vital signals are very sensitive so the leakage of the patient's diseased data could makes the patient embarrassed. Sometimes revealing disease information can make it impossible for them to obtain insurance protection and also result in a person losing their job.

Further, wireless medical sensor networks cover a broad range of healthcare applications, such as Physiological data monitoring, activity monitoring in health-clubs, location tracking for athlete are the broad range of healthcare applications. WMSNs share individual data with physicians and insurance companies. Thus unauthorized collection and use of patient data by adversaries can cause life-threatening risks to the patient and make the patient's private matters publically available. For example, in a simple scenario, a

Corresponding Author: C. *Gayathri, gaitulip@gmail.com*

patient's body sensors transmit the body data to a nurse, the patient's privacy is breached when some attacker is eaves dropping. Later that attacker can post the patient data on social site and pose risks to the patient's privacy.

Indeed wireless healthcare can offer many advantages to patient monitoring, but the medical health data of an individual are highly vulnerable to various threats, so security and privacy become some of the big concerns for healthcare applications, when it comes to adopting wireless technology. A healthcare provider is subjected to strict civil and criminal penalties if HIPAA rules are not followed properly. Thus the security and privacy of the sensed data is the major concern in healthcare applications.

III. MAJOR ISSUES IN WMSN

A. Security Issues

It is worthwhile to assume the scale of deployment of healthcare applications using WMSNs, before discussing the security issues in wireless healthcare applications. Three wireless healthcare Scenarios, such as, a nursing home, home monitoring and hospital monitoring is considered.

Medical sensors, environmental sensors, mobile devices and wireless communication protocols are used by the wireless healthcare applications. Physiological healthcare information (PHI) are stored in a back-end server for offline analysis of PHIs. According to the nursing home scenario medical sensors are placed on a patient's body and sense the body parameters of the patients and transmit it in a timely fashion to the PDA which is held by a nurse. A nurse can analyze the real-time patient health conditions by querying the patient's sensors. Later nurse sends the patient's collected data to the central server either using Internet. Many ES are deployed in nursing homes that can form a wired or wireless network, sense the environmental parameters are sensed using the environmental sensors and are transmitted to a nurse or a remote centre.

An alarm is forwarded to the remote server using an environmental sensor in an emergency situation. In the home scenario medical sensors are embedded on a patient's body and the health data is captured from an individual and transmitted to a PDA in a timely fashion. When a patient is usually alone at home environmental sensors are required. The environmental conditions and patient movement parameters are sensed by the sensors placed at the corners of the room. Then it automatically sends the collected environmental and patient abnormal conditions to the PDA, which is held by a nurse. The home local station can directly communicate with environmental sensors using Zigbee or internet. An application program is implemented at the back-end network to analyze the patient physiological data. The same deployment and sensing scenario is applicable to the hospital environment, where groups of patients are monitored using a wireless medical sensor network by nurses or physicians using their PDAs. Thus security is more important while transmitting the sensed data from the sensors to the server.

B. Privacy Issues

Monitoring the patient's physiological data, emergency management, healthcare data access, electronic health records are the other wireless healthcare applications. Individuals share their health data with physicians, insurance companies and health-coaches. So privacy is a major concern from a social point of view. Thus privacy is defined as the "individual's right to control the acquisition, uses, and disclosures of their health data". The privacy of the health data is maintained by determining which data should be collected, used or disclosed. Any unauthorized collection of patient data may harm the patient's life. For example, an unauthorized person may use the patient data for their personal benefit and sometimes this may even pose life-threatening risks. As the medical data is very sensitive thus questions arises as who owns medical data, and how to control the access to medical data. In wireless healthcare applications, huge amount of health data are gathered and it requires attention on what is gathered, who has rights to access it and how that data is stored and controlled.

The privacy threats like: if a patient loses or share health data can pose significant financial, physical and emotional harm to the patients. An insider may misuse the data to obtain reimbursement or medical services. This may also cause access threats, where a patient is self-involved in the access threats, if they fail to convey their consent properly. For example, an insider may damage the patient's data and harm the patient for their personal reasons and also modify the medical records with a harmful intention, such as, illness conditions, severe allergies, and blood type, all of which pose life-threatening risks. Privacy issues in pervasive healthcare are misuse of medical information, leakage of prescriptions, eavesdropping on medical data, and social implications for the patient. Since the patient health data flows on a wireless channel, it is open to wireless threats, like eavesdropping and snooping.

Thus patient privacy could be breached if an illegal person captures the wireless data and misuses it. Leakage of prescriptions, for instance, to transfer prescription data from pharmacy/doctor to third parties, contains detailed information about a patient. Thus leakage of prescription data becomes a privacy issue. Eaves dropping on patient medical information: patient medical information drifts on the wireless links, which are easily monitored. Patient information are extracted by monitoring system records patient data from communication channels. While the patient data is transmitting from the body area network to the caregiver device, makes eavesdropping very simple for an attacker.

IV. DESIGN CHALLENGES OF WMSN

A. Scalable and Flexible Architecture

The network must preserve its stability. Introducing more nodes into the network means that additional communication messages will be exchanged, and the network should be flexible enough to scale any number of nodes.

B. Fault tolerance and adaptability

Fault tolerance means to maintain medical sensor network functionalities without any interruption due to failure of sensor node because in sensor network every node have limited power of energy so the failure of single node doesn't affect the overall task of the medical sensor network.

C. Node Deployment

Sensor nodes can be deployed randomly in patient area. After deployment, they can be maintained automatically without human presence.

D. Power Consumption

Wireless medical sensor node is microelectronic device equipped with a limited number of power source. Hence power conservation and power management is an important issue in wireless medical sensor network.

E. Limited Computational Power and Memory Size

It is another factor that affects WMSN in the sense that each node stores the data individually and sometime more than one node stored same data and transfer to the base station which wastes the power and storing capacity of nodes.

F. Security

Security is very important parameter in medical sensor network since sensor networks are data centric so there is no particular id associated with sensor nodes and attacker can easily get inside the network and stole the important data without the knowledge of sensor nodes of the network.

V. LITERATURE SURVEY

In the following related works cryptographic symmetric algorithms are used for encrypting the data while transmission. The symmetric key encryption is a cryptography technique that uses a shared secret key to encrypt and decrypt the data. Symmetric encryption algorithms are very efficient at processing large amounts of information and computationally less intensive than asymmetric encryption algorithms. In Fig.1, consist of various symmetric key algorithms such as mentioned in the below.

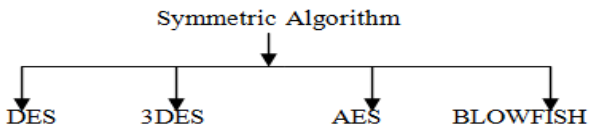

Fig. 1 Symmetric Key Encryption Algorithms

A. A Novel And Lightweight System To Secure Wireless Medical Sensor Networks

In [2], a lightweight and secure system for MSNs is proposed to provide a safe transmission of sensed data, the system employs hash-chain based mechanism and proxy-protected signature technique to achieve secure transmission of the sensed data and access control. The basic idea is as follows, the user registers to the network server, and the registered user is allowed to issue commands to access the collected PHI or control the biosensors according to their access privilege. To achieve this proxy-protected signature by warrant (PSW) is introduced into the system. An original signer and proxy signer are the two important participants. The original signer gives the proxy signer a warrant, and the proxy signer generates a proxy signature using the proxy key given by the original signer. The verifier validate proxy signatures with the public key of the original signer and also verifies the proxy key of the original signer. This prevents the unauthorized access and limits power consumption of sensor nodes.

B. A Secure Mobile Healthcare System using Trust-Based Multicast Scheme

In [1], in order to evaluate the behavior of each node a secured multicast strategy is proposed; in this only trustworthy nodes are allowed to participate in communications so that the misbehavior of malicious nodes is prevented. Trust is defined as "the degree to which a node is trustworthy, secure, or reliable during any interaction with other node". A criterion for choosing nodes for multicast technique is based on the trust value. By evaluating the node's trust enables the trust system to track the behavior of all the nodes, security evaluations feedback of other nodes are recorded, and corresponding reactions are made to the tracked behavior. By this correct nodes can be chosen to participate in the communication and malicious nodes can be avoided.

C. A Robust Watermarking Technique for Secure Sharing of BASN Generated Medical Data

In [9], the focus is on three secure sharing use cases, proof of ownership, where the data owner must prove the ownership of the data tracking, where the data owner must trace unauthorized sharing of the bio signal data and content authentication, and the data owner must prove whether the bio-signal data has been maliciously altered. To address these use cases, a robust watermarking technique is developed to embed security information into bio-signal data in order to protect the semantic fidelity of the data, the bio-signal waveforms are imperceptibly altered, and the watermark is not easily recovered, corrupted or spoofed by malicious attackers. Thus the integrity of the bio-signal is preserved by WM and the data owners can easily track the usage of their data.

D. SPOC: A Secure and Privacy-preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency

In [6], a secure and privacy-preserving opportunistic computing framework, called SPOC, is proposed for medical Healthcare emergency. Using SPOC smart phone resources including computing power and energy can be opportunistically gathered to process the computing-intensive personal health information (PHI) during m-Healthcare emergency with minimal privacy disclosure. To leverage the PHI privacy disclosure and the high reliability of PHI process and transmission in m-Healthcare emergency, an efficient user-centric privacy access control in SPOC, which is based on an attribute-based access control and privacy-preserving scalar product computation (PPSPC) technique, allows a medical user to decide who can participate in the opportunistic computing to assist in processing his overwhelming PHI data.

E. ECG-Cryptography and Authentication in Body Ares Networks and Authentication

In [10], a novel key agreement scheme that allows neighboring nodes in BANs to share a common key generated by electrocardiogram (ECG) signals. The improved Jules Sudan (IJS) algorithm is proposed to set up the key agreement for the message authentication. The ECG-IJS key agreement secures data communications over BANs without any key distribution overheads. In this the simulation and experimental results are presented, which demonstrate that the ECG-IJS scheme can achieve better security performance in terms of performance metrics such as false acceptance rate (FAR) and false rejection rate (FRR) than other existing approaches. Based on the IJS algorithm described earlier, propose an ECG-IJS key agreement to secure data communication in BANs. Thus privacy and authentication are preserved in energy efficient manner.

F. Traffic Models for MSNs

In [4], stochastic data traffic models for medical wireless sensor networks (WSN's) are presented that represent the traffic generated by a single WSN node monitoring body temperature and electrocardiogram (ECG) data. The models are based on public domain medical signal databases. For energy conservation, it is likely that some medical WSN nodes will employ source coding to reduce the amount of data that must be transmitted. The first scenario to consider is the straightforward case where the node simply transmits the raw 11 bit ECG data at the 360 Hz sampling rate. This can be represented using a standard 3,960 bps continuous bit rate traffic model. The second scenario is the more complex case where the node employs source coding. ECG signal compression is a very active research area. In the past, much of this work has focused on offline post-processing of ECG data for archival purposes. However, with the rising popularity of wireless medical data transmission, some research into ECG source coding for real time transmission has begun. The work considers lossy compression due to the very high compression ratios possible with lossy techniques.

In all the above works various symmetric key encryption algorithms are used for encrypting the data while transmission. Table a, provides the comparative study of different symmetric algorithms used for encryption.

Table a. Comparison of Symmetric key Algorithms

Algorithms	Key length	Block size	Round	Attack
DES	128,192 256 bits	128,192, 256	9,11, 13	Side channel attack
3DES	168 bits	64	48	Theoretically possible
AES	56 bits	64	16	Brute force
BLOWFISH	32-448 bits	64	16	Not yet

VI. CONCLUSION

Healthcare applications are considered a promising field for WMSNs, where patients can be monitored. Transmission in wireless environment needs safety and privacy of medical data. Symmetric cryptographic algorithms are used to provide security during data transmission and access control policies are adopted by attribute based signature technique. Thus the privacy and integrity of data is perceived while transmission in a wireless environment.

REFERENCES

[1] Azzedine Boukerche, and Yonglin Ren," A Secure Mobile Healthcare System using Trust-Based Multicast Scheme", IEEE Journal On Selected Areas In Communications, Vol. 27, No. 4, May **2009**,**316-325**.

[2] Daojing He, Sammy Chan, Member, IEEE, and Shaohua Tang, Member, IEEE," A Novel and Lightweight System to Secure Wireless Medical Sensor Networks", IEEE Journal Of Biomedical And Health Informatics, Vol. 18, No. 1, January **2014,23-32**.

[3] Denis Trcek And Andrej Brodnik, University Of Ljubljana," Hard And Soft Security Provisioning for Computationally Weak Pervasive Computing Systems In E-Health", IEEE Wireless Communications August **2013**,**45-53**.

[4] Geoffrey G. Messier and Ivars G. Finvers," Traffic Models for Medical Wireless Sensor Networks", IEEE Communications Letters, Vol. 11, No. 1, January **2007** ,**21-30**.

[5] Oscar Garcia-Morchon, Thomas Falck, Tobias Heer, Klaus Wehrle,"Security for Pervasive Medical Sensor Networks", Vol.12, No.2, June 5th **2009,126-**

134.

[6] Rongxing Lu, Member, IEEE, Xiaodong Lin, Member, IEEE, and Xuemin (Sherman) Shen, Fellow, IEEE," SPOC: A Secure and Privacy-preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency", IEEE Transactions On Parallel And Distributed Systems, Vol. 12, No. 2, May **2012**,**452-461**.

[7] Shu-Di Bao, Student Member, IEEE, Carmen C. Y. Poon, Student Member, IEEE,Yuan-Ting Zhang, Fellow, IEEE, and Lian-Feng Shen," Using the Timing Information of Heartbeats as an Entity Identifier to Secure Body Sensor Network", IEEE Transactions On Information Technology In Biomedicine, Vol. 12, No. 6, November **2008**,**155-162**.

[8] S. Moller, T. Newea, S. Lochmannb," Prototype of a secure wireless patient monitoring system for the medical Community", **2011** Elsevier B.V. All rights reserved.

[9] Vishwa Goudar and Miodrag Potkonjak," A Robust Watermarking Technique for Secure Sharing of BASN Generated Medical Data", **2014** IEEE International Conference on Distributed Computing in Sensor Systems.

[10] Zhaoyang Zhang, Honggang Wang, Athanasios V. Vasilakos, and Hua Fang," ECG- Cryptography and Authentication in Body Area Networks", IEEE Transactions On Information Technology In Biomedicine, Vol. 16, No. 6, November **2012,321-332**.

