Security Requirement in Cryptograpic Health Monitoring System

Anupama S[1] Sudheesh S. R[2] Hari S[3]
[1]Student [2,3]Assistant Professor
[1,2,3]Department of Electronics & Communication Engineering
[1,2,3]Mount Zion College of Engineering Kadammanitta, Pathanamthitta, Kerala, India

Abstract— Wireless technology and its applications are most common in today's markets. The advantage and benefits of wireless system became attractive in all kind of industrial and non-industrial applications. In order to eliminate the complications of wired connection, it is possible to implement cryptographic wireless systems in medical fields. This technique is already developed and became a successful in recent years. In medical application, real time health monitoring for patients is very critical. So this paper gives a real time health monitoring system and need for its security requirements. The security and privacy is more essential in health monitoring. So it develops a WBAN system, under some aggregation and encryption scheme.

Key words: Real time health monitoring system, Cryptographic wireless system, WBAN, Aggregation, Encryption scheme

I. INTRODUCTION

Wireless sensing and communication technologies have wide range of applications. Such as, environmental, industrial and real time health monitoring. In this paper a real time health monitoring system, which is WBAN and its security requirement is explained. Wireless body area network is a remote health monitoring system and it is used to continuously monitor and collect the patient's physiological information. This data is collected and aggregated for further processing and analysis. The analysis is carried out for security and its privacy of health data.

Data aggregation is important to eliminate redundancy of data. In cryptographic network based health monitoring, it is possible to hack or eavesdrop the real time health information by attackers. There are mainly two types of attacks, passive and active attacks. Authentication and data privacy is takesplace by data encryption. Any alteration, violation of data will lead to face challenges and issues in medical treatment. So security and its needs are becoming more over important in this paper. Therefore, here I am also focuses on security requirement in WBAN.

II. SECURITY AND PRIVACY

The wireless body area network for remote health monitoring system has mainly two parts; [1] intra-body communication network and extra-body communication network.

The function of intra-body communication network is secure data generation and secures data aggregation. It comprises of an aggregator connected with a set of sensing nodes. The sensing nodes continuously monitor and collect the health information of patients. Whereas, extra-body CN is responsible for secure data transmission, secure data storage and finally medical data access. The given figure represents the prior challenge in WBAN communication system [2].

The three prior challenges can be resolved by advanced and improved methods of cryptographic systems. In WBAN sytem, three main stages involved in secure data access, they are :

- Secure data aggregation
- Secure data transmission
- Secure data storage

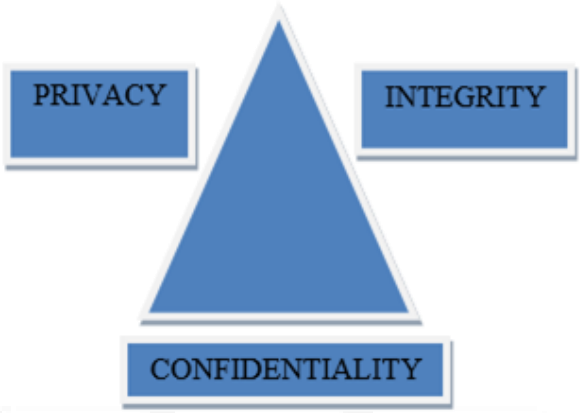

Fig. 1: Prior challenge in WBAN system

From these regularity point of view, we can identify that the imporance of security and privacy in this paper. The major security parameters [5] proposed in the papers are:

- Integrity: Integrity , which means that protects the nodes from maliciously altered messages. The receiver wants to be sure that the source is genuine here.
- Confidentiality: It ensures that acertain information, which is never disclosed to unauthorized entities. Personal or sensitive data are protected by it.
- Authentication: It ensures the service offered by node and it will be available to its users when expected in spite of attacks.
- Identity: It is an essential element in any security system, and it is reliable, robust, non malleable.

III. STSTEM MODEL

The system model for health monitoring is shown below. It ensuring the security parameters by DBDH with a secure privacy preserving data aggregation algorithm.

Sensing nodes (SN) are denoted by SN, consists of allowable number of sensors denoted by 'k' on a patient's body. An aggregator is connected wirelessly to the medical sensors (SN). It is uesd to collect individual health data and compute the aggregation on them. Medical server represents an individual server in the remote health monitoring system. Medical server is accessed by a trusted authority. That means a doctor, or agroup of experts analyses the data output from medical server.

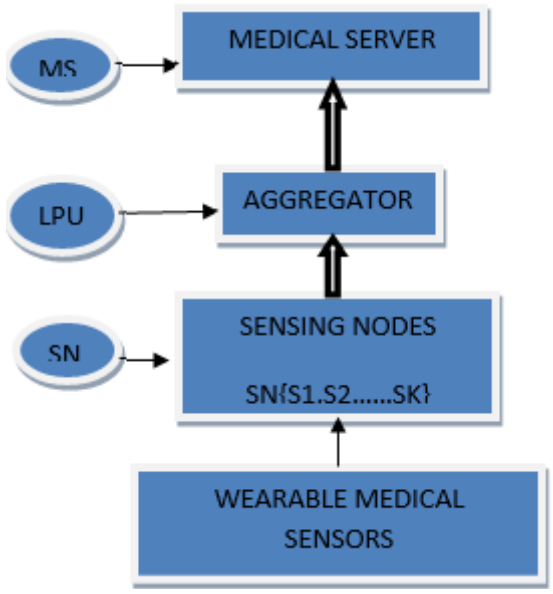

Fig. 2: General health monitoring system model

The SPPDA [4] provides security and privacy in cryptosystem. There are different types of privacy preserving algorithm. But most of them will not provide the basic three parameters; such as integrity, confidentiality and authentication. However security and privacy requirements is important in cryptographic system. It will prevents different attacks in cryptosystem.

There are two types of attacks; passive and active attacks. Passive attack may occurred as learning information from transmission content or eaves dropping on transmission. Whereas, the active attacker try to access or modify network information. So these attacks can be prevent by fulfil the major security and privacy requirements.

IV. Conclusion

The security and privacy preservation is very important in network system. In this paper, a health monitoring system is explained which is used to monitor humen's physiological information. This health data generation and aggregation requires privacy for to avoid some attacks. Different security requirements and need for privacy in cryptosystem takes a very much role in network environments. It is explained in this paper and also included about some types of networks attacks.

References

[1] Anees Ara, Student Member, IEEE, Mznah Al-Rodhaan, Yuan Tian and Abdullah Al-Dhelaan "A Secure Privacy-Preserving Data Aggregation Scheme based on Bilinear ElGamal Cryptosystem for Remote Health Monitoring Systems" , 2016 IEEE.

[2] S. Lim, T. H. Oh, Y. B. Choi, and T. Lakshman, "Security Issues on Wireless Body Area Network for Remote Healthcare Monitoring," Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC), 2010 IEEE International Conference on. pp. 327–332, 2010.

[3] J. Sun, X. Zhu, and Y. Fang, "Preserving Privacy in Emergency Response Based on Wireless Body Sensor Networks," Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE. pp. 1–6, 2010.

[4] S. Han, S. Zhao, Q. Li, C.-H. Ju, and W. Zhou, "PPM-HDA: Privacy-Preserving and Multifunctional Health Data Aggregation with Fault Tolerance," IEEE Trans. Inf. Forensics Secure. vol. 11, no. 9, pp. 1940–1955, Sep. 2016.

[5] Ashwani Kush & Ram Kumar "Wireless network security issues", DESIDOC Bulletin of technol, 2005.

