ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

Snalysis of ecg for securing wireless body sensor network (WBSN)

[1]Narasimman M, [2]Thanveer Ahmed LR, [3]Guru Rajkumar M, [4]Varun Kumar M

[1]*Student,SITE, VIT University, India.*
[2]*Student, SITE,VIT University, India.*
[3]*Student,CSE, Saveetha University, India.*
[4]*Faculty,SITE, VIT University, India.*

ARTICLE INFO

Article history:
Received 10 October 2015
Accepted 30 November 2015
Available online 24 December 2015

Keywords:
Human Physiological Signals, Health Monitoring System, Semiconductor devices, Wireless Body Sensor Network (WBSN), Wireless sensors.

ABSTRACT

With the increased advancement in wireless communication and semiconductor devices, Sensor networks have started to support a large number of applications. One of the major applications of the sensor network is Health Monitoring. WBSN (Wireless Body Sensor Networks) consists of a group of sensors implanted or wearied on the human body to sense the value of human physiological signals and communicate it to the physician for diagnosis. Since the data handled by the WBSN is sensitive human health data, security and privacy of the data has to be maintained. It is a challenge to design a security scheme for WBSN, as they are resource constraint. Cryptography techniques used for WSN (Wireless Sensor Network) cannot be used for WBSN as they are by design inadequate in resources. The latest method to implement security is by using the measured physiological values. In this paper analysis of the various biometric schemes which use physiological signals for addressing the security issues in WBSN is done.

© 2015 AENSI Publisher All rights reserved.

To Cite This Article: Narasimman M,Thanveer Ahmed L R, Guru Rajkumar M,Varun Kumar M., Snalysis of ecg for securing wireless body sensor network (WBSN). ***Aust. J. Basic & Appl. Sci.,*** *9(35): 187-190, 2015*

INTRODUCTION

In the advancement of technology in Health Care application Wireless Body Sensor Network (WBSN) have introduced as a new technology. However, the security privacy of a person is more important in WBSN as the Health information. A wireless body sensor network consists of a small device which is attached on the body and it is capable of performing a wireless communication link among it. It provides the health information of a person and monitoring a physiological signals. In this communicational link it needs to ensure the privacy and safety which leads to the security challenges. The importance of wireless sensors in this field is allowing monitoring the patient at home. The implementation of a wireless technology is to improve the quality of data resolution of data and mobility of patient may be increased. Data confidentiality is one of the most important aspect in wireless body sensor network security. The wireless body sensor network is consists of limited memory and computation capability. So, it has been proposed by a biometric based approach. It avoids the extra memory occupation in it. The Security is more important in WBSN i.e., networks can be authorized only by the user who can be query the monitor and the network. So, the medical data can be protected and not been corrupted the person's health information. Thus, to ensure the authenticated person to access the physical data. The benefits of using wireless communication in an existing technology are to monitor the person's physiological signal from our place. The WBSN is mainly focused on the distribution of nodes from a human body and the physiological signals can be monitored. The sensor can be measures the certain parameter of a human body. The Wireless body sensor network is an emerging new technology. To ensuring security and privacy in WBSN is essential for the human life. Ultimately, it is analysing the various biometric schemes and addressed by the existing proposed schemes. Identifying the requirements that a security solution to be confidential.

Corresponding Author: Narasimman M, Student,SITE, VIT University, India.
E-mail: Rocky.dinesh31@gmail.com

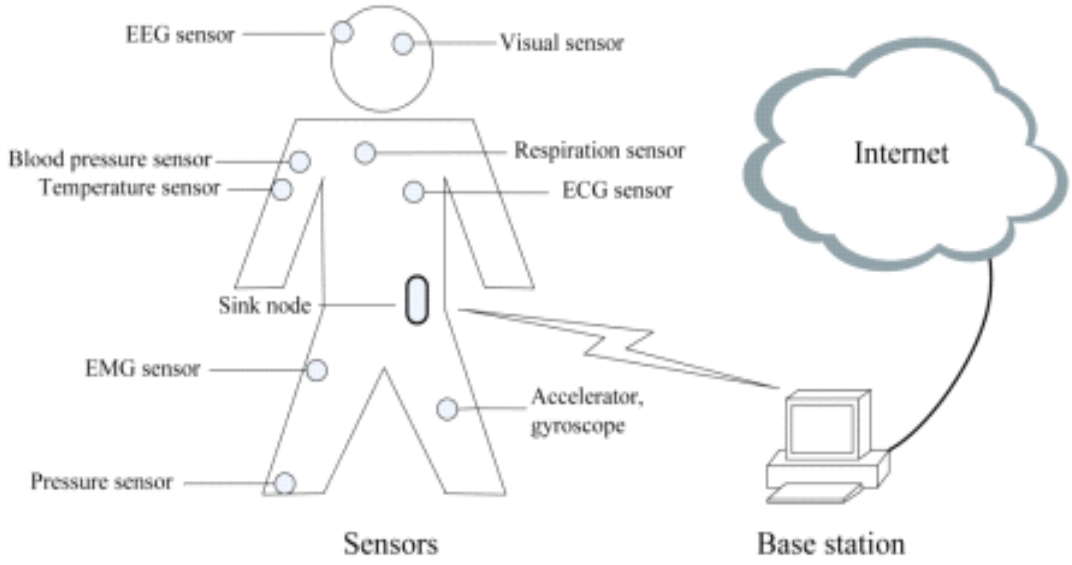

Fig. 1: Illustration Figure

II. Security And Privacy:

The health information of a patient's body is communicated through WBSN and it is strictly private and confidential. It should be encrypted to protect the patient's privacy. The Security and Privacy is mainly used to protect and it is a significant part of the available energy and it is energy efficient. Wireless Body Sensor Networks is potentially facing a lot of security threats. The particular security threats of biometric schemes can be categorized by outsider and insider attacks. Owing, to this security attacks the attacker can be launch different attacks without being detected. So, it can be able to threaten without any authentication access to health information and false data injection can be occurs. In the use of the body itself the cryptography keys for signals to agree the physiological signals value at similar time. It can be able to encrypt and decrypt the data to distribute it securely with privacy. This key establishment is to securing the communication in biomedical sensor networks. The requirements of this security and privacy is constraints of power memory, capability for computation, it is mainly for the sensors which is implanted into the body. It protects against the unauthorized of network resources

2.1. Security Requirements:

The Security Requirements exists one or more base stations operating as a data sinks and consists of gateways to IP networks.

- It is issued to avoid confusion with the Central Intelligence Agency.
- The elements of the security are considered as the three most crucial components of security.

2.2. Security Threats:

The particular threats that a wireless body sensor network has categorized into outsider and insider attack.The attacker node is not an authorized, to the participant sensor network. It will be a security threats to the participant and network authentication. The encryption and authentication access is used to prevent such an attack to gain any special access to the body sensor network. The signals can be used to encrypt and decrypt the symmetric keys to distribute it securely. The Signal Processing of an each node can be vulnerable to access. It can perform an authenticate to participants sensor network. Security threats occurs by accessing the participant signal from a sensor network.

III. Security Analysis:

It is one of the authorizing current technology in security. Security is the main concerns for every wired networks and wireless based networks. So, far the resources have implemented the physically implementing the sensor nodes and sensor networks for secure communication. The various protocols to provide the basic needs of the data security i.e., data Confidentiality, Integrity and Authentication. In security each of the authentication mechanisms are simulated in the operations, power consuming, energy consumption and security level to be analysis for security. Security should be implemented on all the necessary cryptographic computations and computed to reduce the energy consumption. Security services are offered access control, data encryption, integrity and authentication. It is used to develop the improved wireless body sensor network protocols for improving the nodes. The existing security has required intensive computation and memory which is limiting factor in wireless body sensor network. Therefore, number of security mechanism is already exist few security analysis is used for the wireless sensor network.

3.1. Confidentiality:

It is used to protect the sensed data and exchanges between the communication sensor nodes. The Access must be restricted to those unauthorized to view the data. Data encryption is a common method of ensuring confidentiality. The constitute standard procedure includes biometric verification and security tokens and key tokens to analyzing the authentication user to access the data.

3.2. Integrity and Authentication:

Integrity is necessary to enable the sensor node to detect modified, injected or replayed the data. It is a secret key to guarantee data integrity. The Authentication is the procedure of identifying the right node. Integrity involves maintaining the consistency, accuracy and trustworthiness of data and its entire life cycle. Data must not be changed and the step must be taken to ensure i.e.,data cannot be altered by unauthorized user. It measures include file permission and user access controls. In an Integrity, version control may be used to prevent the enormous changes or any accidental deletion by authorizedusers becoming a problem. In addition, the data in place to detect can be seen where any changes in data that might occur as a result of non-human casedevent such as Server Crash. Some data might easily capture and it includes even cryptographic key checks for verification

3.3. Availability:

It is one the best ensured rigorously maintaining of all hardware. The attacks like Denial-Of-Service (DOS) i.e., bringing down the network itself may have some serious consequences to the health information data of a person. The maintaining a correct functioning of operating system environment is more important i.e., free of software may be conflicts. However, Symmetric key is not as public key cryptography, which makes the design secure applications

IV. Health Monitoring System:

The goal of this health monitoring system is to provide the public health officials with the tools that enhance their ability to safeguard the health communities to save. It provides the automatic system updates and ensures the security of all identifiable patient information. Then, the system discovers a potential health threat, an immediate notification is sent to the user authenticated person in health monitoring system.In earlier days, the system allows continuously to monitor patient's status where these systems require the sensor to be placed bedside monitors or PC's. So, in this system the patient cannot be move from a particular place and the limits is applicable for the systems. But, now there is no bedside monitoring system. Because, it is controlled and monitored by wireless body sensor networks. It is emerged as a new technology, the patient's health is monitored continuously and patient can be easily moved from a particular place.We can also reach to continuous health monitoring by using adhoc wireless networks and it can be transmitted over a short-range. The patient's physiological signals are monitored and accessed by the sensor and it is transmitted to the remote base station to PC or monitor and store to analysing it. The sensors on patient's body can be able to sense the health rate/Blood Pressure (BP) and so on. It can be able to detect the abnormal conditions. The health monitoring system allows an individual to closely monitor the changes of a signals and vital signals and provide an optimal health status. It is one of the most valuable system to monitor the physiological signals of a person's health information data.

4.1. Biometric Key Distribution:

In this key, the wireless body sensor network consists of group of biomedical sensors which is deployed on the human body. The biomedical sensor which performs the function of monitoring health information and transmitting it to the control sensor by one or multiple hops then, the signals are collected and forward to the external device for the further processing. In this key it represents by using fuzzy construction by key encoding and decoding. The existing biomedical sensor devices are used to read the Interpulse information (IPI) signals of ECG which is consists to perform the key in a public domain ECG database in the physiobank. ECG biometrics for secure communications in WBSN. The basic idea was to represent the ECG biometrics in an ordered set and transform the problem of key agreement into the problem of set reconciliation, so as to decrease the necessary transmission bits of the public information. Experiments showed the new approach could remarkably reduce the communication bits for key agreement and achieve lower energy consumptions.

4.2. Technical Challenges:

In technical challenges, the cryptography biometric key requires the exact right keys when biometrics are fuzzy and noisy, even the same physiological values are monitored from the different locations of the same body in the same time will suffer from distortions to a certain extent. It is used to generate or conciliate accuracy keys using the noisy biometrics. Moreover, the energy costs of sensing and computation are immediately so small i.e., almost negligible compared to the expensive cost of communication in wireless body sensor network and then the security and threats will be reduced using the biometric key distribution.

Therefore, the biometric key is used to transmit the physiological signal information to the health monitoring system and the security is high using this biometric key distribution.

4.3. Advantages:

1. Reasonable cost
2. High Accuracy Performance
3. Energy Consumption is supported to the key length and it consumes low energy consumption.

4.4. Disadvantages:

Low memory size.

Conclusion:

In this paper, we analyze the essential characteristics of the wireless body sensor network and the health monitoring system which is used to provide the public health officials with the tools that enhance these ability to safe the information. Security and Privacy is mainly used to protect the health information and also prevent from the false data injection. Thus, it is controlled and monitored by the health monitoring system. Then finally, analyzing the biometric key distribution and its level of security, performance and the characteristics of the physiological signals for securing wireless body sensor network. Our future work will continue to improve the current system and the physiological signal to expand the biomedical health care application.

REFERENCES

Bhattacharya, J., R.P. Kanjilal, 1999. “Assessing determinism of photoplethysmographic signals”, IEEE Trans. On Systems, Man, and Cybernetics-part A systems and humans, 29: 406-410

Cherukuri, S., K. Venkatasubramanian and S.K.S. Gupta, 2003. ”BioSec:A Biometric Based Approach for Securing Communication in Wireless Networks of Biosensors Implanted in the Human Body”, Proc. of the 2003 International Conference on Parallel Processing Workshops, Taiwan, Oct. Health Insurance Portability Accountability Act (HIPAA)

Cherukuri, S., K.K. Venkatasubramanian and S.K.S. Gupta, 2003. “BioSec: A Biometric based Approach for Securing Communication in Wireless Networks of Biosensors Implanted in the Human Body,” Proc. IEEE Int’l Conf. Parallel Processing Wksp., pp: 432-439.

Directive, 2002. /58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector.

Hash, J., P. Bowen, A. Johnson, C.D. Smith and D.I. Steinberg, 2005. "An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule," Nat. Inst.Stand. Technol., NIST Spec. PUbl., pp: 800-866.

Lo, B., S. Thiemjarus, R. King and G.Z. Yang,2005. ”Body Sensor Network: A Wireless Sensor Platform for Pervasive Healthcare Monitoring”, Adjunct Proceedings of the 3rd International Conference on Pervasive Computing, pp: 77-80.

Perrig, J., Stankovic and D. Wagner, 1993. “Security in Wireless Sensor Networks”, Communications of the ACM, Vol. 47, No. 6, June 2004. W.-K.Chen, Linear Networks and Systems (Book style).Belmont, CA: Wadsworth, pp: 123-135.

Perrig, R., V. Szewczyk, D. Wen, Culler and D. Tygar, 2001. “SPINS: Security Protocols for Sensor Networks”, in Proceedings of the 7th Annual International Conference on Mobile Computing and Networks (MOBICOM 2001).

Petersen, S., V. Peto and M. Rayner, 2004. ”Coronary heart disease statistics”, British Heart Foundation, London.

Poon, C.C.Y., Y.T. Zhang and S.D. Bao, 2006. ”A novel biometrics method to secure wireless body area sensor networks for telemedicine and health”.IEEE Communications Magazine, 44(4): 73-81.