ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

A Study on Security in Wireless Body Sensor Networks

R. Sudha [1], P. Nivetha [2]

Asst. Professor, Dept. of Computer Science, PSG College of Arts & Science, Coimbatore, India [1]

Research Scholar, Dept. of Computer Science, PSG College of Arts & Science, Coimbatore, India [2]

ABSTRACT: Body sensor networks is a wireless network of wearable computing devices.BSN is used in various applications. In medical field, BSN plays a major role. Sensors are both wearable and implantable in our body. With the help of sensors, we can monitor the patient's health. In this paper it comprises of applications of WBAN, requirements of security, security attacks and security mechanisms.

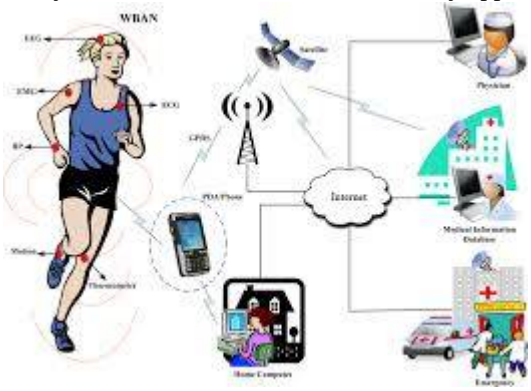
KEYWORDS: BSN, sensors, security, nodes, applications, protocols

I. INTRODUCTION

A body sensor network is one of the parts of wireless sensor network. Body area network is mainly used to monitor the patient's health. In Body sensor network, sensors are very small in size. In our body, sensors can be placed in two ways namely wearable or implantable. With the help of sensors, we can monitor the patient's heart rate, pulse, pressure, temperature. In BSN, less number of nodes will be used when we compare with WSN. In BSN, security plays a vital role.

II. APPLICATIONS OF WBAN

WBAN is used in many fields such as medical field, military applications, social welfare and sports.



WBAN

2.1 Medical field:

In medical field, BSN is used to monitor the patient's health condition day-to-day. With the help of monitoring, we can easily know the status of the patient and we can avoid the occurrence of critical situations. We can monitor the patient in both clinical as well as family environment. Because of regular monitoring, we can diagnose the patient in the earlier stage to treat them. [1][8][11]

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

2.2 Social welfare:

In social welfare, electronic systems are in need to monitor the disabled patients, old age peoples and children. We can analyse the needs of the patients by using BSN. With the help of sensors, we can avoid the real time problem of the patients by using the recognition technology and alarms. The system provides messages regarding patient's health status [1] [18] [11].

2.3 Sports:

In sports, sensors are used to improve their skills, correcting the postures and for providing scientific training. With the help of sensors, we used to capture the motion of the athletes and evaluate them. The purpose of BSN is to recognize the motion and to detect the physiological status. Coaches can take a closer look at the strong and weak points of an athlete by measuring various body conditions like change in heartbeat, oxygen level etc. during a race and other real life scenarios. This can help in improving their shortcomings and in improving their skills. [1][8][11]

2.4 Military applications:

In military applications, BAN is used to monitor health, location & high temperature and hydration levels. With the help of sensors, we can predict the arrival of the opponent, physiological conditions of the opponent and we can protect and prevent us from the victims. The Army Research Laboratory (ARL) has accomplish experiments using auditory sensor arrays hanging below tethered aerostats to sense and confine fleeting signals from mortars, weaponry and arms fire. We can administer the patient when they are at home. [1][8][11][13]

2. 5 WBAN for animals:

With the help of WBAN, we can monitor the animals in the forest by using sensors. It is used to diagnose the disease & health status of the animals. By early prediction, we can avoid and protect the animals from diseases. It may be used for diagnosing different infectious diseases in human being as well as animals. It is very important matter, if want to improve human health and control diseases first we have to improve animals health and control diseases that provide food to the human being [1][8][11].

III. SECURITY REQUIREMENTS IN WBAN

Security is the major challenge in WBAN. When we compare WSN with BSN, in WSN there were many solutions regarding security. But in BSN, it will not be applicable. In BSN, we can secure the data with the help of security requirements. [20]

Some of the security requirements in WBSN are:

- Data storage security requirements
- Data access security requirements
- Other security requirements

3.1 DATA STORAGE SECURITY REQUIREMENTS

In data storage security requirements it includes confidentiality, integrity assurance and dependability. [19][20][13][2]

Confidentiality

The term data confidentiality means protecting the patient's data. Because, while storing if any data gets leak, it will affect the patient health. It is hard to protect the data from masquerades or disclosures. Here, confidentiality plays a vital role in order to provide security with the help of encryption techniques. [19][20][13]

Integrity assurance

There may chance for corrupting the data by third parties while transmitting due to lack of integrity. We can use authentication protocols in order to secure the data. By using integrity assurance, patient's details are protected from unauthorized users. To protect the data both confidentiality and integrity are needed [2][13][20].

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Dependability

Due to node failures, sometimes we can't retrieve the patient's details. With the help of dependability data can be retrieved even node failure occurs. In medical field, if we can't access the data in critical situations it becomes as a critical issue. [19] [20]

3.2 DATA ACCESS SECURITY REQUIREMENTS

In data access requirements it includes access control, accountability, revocability and non-repudiation [13][2][19][20].

Access control

Access control is one of the security techniques. The purpose of access control is used to protect the data from unauthorized persons. In access control, it has two credentials namely locks and login.

Accountability

If anybody is using the patient data for improper treatment (or) wrong purpose, it can be easily identified. When a user of the WBAN abuses his/her privilege to carry out unauthorized actions on patient-related data, he/she should be identified and held accountable. [19]

Revocability

It means when the nodes are behaving differently it should be removed on time. The privileges of WBAN users or nodes should be deprived in time if they are identified as compromised or behave maliciously.

Non-repudiation

The term non-repudiation means providing acknowledgements while sending the message whether it is sent (or) not. It will be helpful when problem occurs. The origin of a piece of patient-related data cannot be denied by the source that generated it. [19]

3.3 OTHER SECURITY REQUIREMENTS

It includes authentication and availability. [19][20]

Authentication

It is used to detect whether the received data is from the authorized user or not. The sender of the patient-related data must be authenticated, and injection of data from outside the WBAN should be prevented. It is used in both medical and non-medical applications. [3][19]

Availability

The term availability means the patient's information should be accessible any time by the physicians. The patient-related data should be accessible even under denial-of-service (DoS) attacks. [5][19]

IV. SECURITY ATTACKS IN WBAN

Some of the security attacks occur DOS (Denial of service) are:

- Jamming
- Tampering
- Link
- Collision
- Unfairness
- Exhaustion
- Neglect and greed
- Homing
- Misdirection

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

- Flooding
- Encryption
- Black holes
- De synchronization [8][9]

V. SECURITY MECHANISM

WBAN deals with much security mechanism.

Cryptography

Cryptography function includes encryption, authentication, and integrity in order to develop secure application with the help of cryptography function. We can provide security & privacy from the malicious attacks. It depends on the computation and communication capability of the sensor nodes. Energy, memory, execution time are needed in order to execute security mechanisms with the help of cryptosystem [20] [6].

Key management

This protocol is used to develop a secure application. The protocols are used to set up and distribute varied forms of cryptographic keys to nodes within the network. It consists of three key management protocols. They are:

- Trusted server
  -Provides stronger security to hierarchical networks.
- Key pre-distribution
  -Easy to implement
- Self enforcing[7][3][20]
  -It employs public-key infrastructure.

Secure routing

In BSN, secure routing protocols should be used to transmit data from one end to another in order to provide high level security. Routing is crucial service for end-end communication. There were several routing protocols for sensor networks. But secure routing protocols plays a vital role.

Security protocol

In sensor networks, security protocols provide data confidentiality, two- party authentication and data freshness which can be implemented in BSN with lower power consumption. It has different security modes. They are

- No security
- Encryption only(AES-CTR)
- Authentication only(AES-CBC-MAC)
- Encryption and authentication(AES-CCM)[20]

RC5

RC5 algorithm is used to provide security strength than DES. The standard key length of RC5 is 128bits has managed to withstand years of cryptanalysis. [6] According to security strength, RC5 involves data dependent rotations which may help frustrate differential cryptanalysis and linear cryptanalysis since bits are rotated to random positions in each round. There is no obvious way in which an RC5 key can be weak other than by being too short. The standard key length of RC5 is 128 bits has managed to withstand years of cryptanalysis. Also the RC5 block cipher has built-in parameter variability that provides flexibility at all levels of security and efficiency. RC5 is better than DES in security strength and implementation efficiency [7].

VI. CONCLUSION

In this paper we discuss about how BSN is used in various applications like medical fields, social welfare, sports etc., In BSN, there were many security attacks occur in different layers also discussed. In BSN, the major issue is security. To overcome the issue different security mechanisms also discussed in this paper. With the help of these mechanisms we can protect the secured data from hackers.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

REFERENCES

1. Aarti sangwan and Partha pratim bhattacharya "Wireless Body Sensor Networks: A Review" published in International Journal of Hybrid Information Technology, Vol.8, No.9, pp.105-120, 2015.
2. Aashima Arya , Naveen Bilandi "A Review: Wireless Body Area Networks for Health Care" published in International Journal of Innovative Research in Computer and Communication Engineering ,Vol. 2, Issue 4, pp.3800-3806, April 2014
3. P.Abina, K.Dhivyakala,L.Suganya,S.Mary Praveena "Biometric Authentication System for BodyArea Network" published in International Journal Of Advanced Research In Electrical, Electronics And Instrumentation Engineering, Vol. 3, Issue 3, pp.7954-7964, March 2014.
6. Dhanashri H. Gawali and Vijay M. Wadhai "RC5 ALGORITHM: POTENTIAL CIPHER SOLUTION FOR SECURITY IN WIRELESS BODY SENSOR NETWORKS (WBSN)"published in International Journal Of Advanced Smart Sensor Network Systems (IJASSN), Vol 2, No.3,pp:1-7, July 2012.
7. Syed Furqan Qadri, Salman Afsar Awan, Muhammad Amjad, Masood Anwar, Suneel Shehzad " APPLICATIONS, CHALLENGES, SECURITY OF WIRELESS BODY AREA NETWORKS (WBANS) AND FUNCTIONALITY OF IEEE 802.15.4/ZIGBEE" Sci.Int.(Lahore),25(4),697-702,2013.
8. Benny P L Lo and Guang-Zhong Yang "KEY TECHNICAL CHALLENGES AND CURRENT IMPLEMENTATIONS OF BODY SENSOR NETWORKS"
9. Ajit, Amita Malik "Security in Body Area Network: A Survey" published in International Journal of Enhanced Research in Management & Computer Applications, Vol. 3 Issue 5, pp: (70-76) , May-2014.
10. Stefina Macwan, Nikhil Gondaliya, Nirav Raja," Survey on Wireless Body Area Network" published in International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 2, pp.107-110, February 2016.
11. A.Siva Sangari, J.Martin Leo Manickam **"**LIGHT WEIGHT SECURITY AND AUTHENTICATION IN WIRELESS BODY AREA NETWORK" published in Indian Journal of Computer Science and Engineering (IJCSE) ,Vol. 4No.6,pp:438-446,Dec 2013-Jan 2014
12." A Secure Transmission Protocol for Wireless Body Sensor Networks" published in JOURNAL OF SOFTWARE, VOL. 9, NO. 8, pp:2043-2049,AUGUST 2014.
13. Xiaochen Lai , Quanli Liu , Xin Wei , Wei Wang , Guoqiao Zhou and Guangyi Han "A Survey of Body Sensor Networks "Sensors 2013, 13, pp: 5406-5447.
14. P Usha, N Priya "Survey on Security Issuses in WBAN " published in International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 1, pp:482-485,January 2015.
15. Prameela.S, P. Ponmuthuramalingam "Wireless Body Area Network– A Study" published in International Journal of Advanced Research in Computer Science and Software Engineering , Volume 5, Issue 9,pp:580-584, September 2015 .
16. Ankur Hooda, Sonia Sharma, Anima "Wireless Body area network" published in International Journal of Electronics,communication & Instrumentation Engineering Research and Deveopment, vol.3, Issue 1,pp: 203-210, Mar 2013.
17. M.somasundaram and R.Sivakumar "Security in wireless body area networks- A survey" published in 2011 International conference on Advancements in information technology with workshop of ICBMG, vol.20, pp:18-23, 2011.
18. Vahid Ayatollahi Tafti, MD Asri Ngadi, and Johan Bin mohamad sharif "Requirements and challenges in body sensor networks-survey" published in Journal of theoretical and applied information technology , vol.72 No.2 ,pp:227-238, Feb2015.
19. Ramesh kumar & Rajeshwari mukesh "State of the art: security in wireless Body area networks" published in International Journal of computer science & Engineering Technology, vol.4 No.05,pp: 622-630,may 2013.
20. Shahnaz saleem, Sana Ullah,Hyeong seon Yoo "On the security issues in wireless body are networks" published in International Jouranal of Digital content technology & its applications, vol3, no 3, September 2009.

BIOGRAPHY

1**.** Prof. R.Sudha is working as an Assistant professor in PSG College of arts & science, Coimbatore. She has published many papers regarding sensor networks.

2. Miss. P.Nivetha is pursuing M.Phil in PSG College of arts & science, Coimbatore. She is undergoing research on sensor networks.