International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 4 Issue: 3
ISSN: 2454-4248
521 – 526

Analysis and Improvement in Tracking & Security of Wireless Body Sensor Network with the help of Quantum Cryptography: - A Retrospective View on Literature Survey

Dr. Shalini Rajawat
Professor (Computer Science and Engineering)
Vivekananda Global University, Jaipur

Dr. Vishal Goar
Assistant Professor (Computer Science and Engineering)
Govt. Engineering College, Bikaner

Abhishek Bhardwaj
Ph.D. Research Scholar (Computer Science)
Vivekananda Global University, Jaipur

Abstract: **-**The wireless nature of the network and the wide variety of sensors offer numerous new, practical and innovative applications to improve health care and the Quality of Life. Using a WBSN, the patient experiences a greater physical mobility and is no longer compelled to stay in the hospital. In this paper, we also present an idea to improve healthcare systems in India with the help of telecommunication and information technology by using wearable and implantable body sensor nodes which does not affect the mobility of the patients with extra security and advance feature. A WBSN should ensure the accurate sensing, tracking of the signal from the body, carry out low-level processing of the sensor signal and wirelessly transmit the processed signal to a local processing unit. In the proposed system, WBSNs, a sparse network of sensors are deployed either directly on the human body, inside the body or embedded in everyday clothes, to record and transmit health data. Body Sensors record and transmit data to a Body Central Unit which aggregates data sent by all Body Sensors and relays the aggregation to a hospital monitoring station from where healthcare professionals can remotely monitor the health parameters of patients or other individuals. This will help the authorized care giver easily diagnose the problem and make available the quick treatment to patient.

The security of these devices is very important factor to make secure the personal data of any patient. Thus no other unauthorized person can get information about the patient disease etc which help to protect privacy of user and data. The primary objective of this proposed work is to propose effective security and tracking technique for sensor body wireless network with the help of new and effective technique Quantum Cryptography which provides extra security from all type of dangerous attacks and threats.

Keywords:- *WBSN, Security, Telecommunication, Quantum Cryptography.*

*****

I. Introduction:

In wireless body sensor networks various sensors are attached on clothing or on the body or even implanted under the skin. The wireless nature of the network and the wide variety of sensors offer numerous new, practical and innovative applications to improve health care and the Quality of Life. Using a WBSN, the patient experiences a greater physical mobility and is no longer compelled to stay in the hospital. We also present an idea to improve healthcare systems in India with the help of telecommunication and information technology by using wearable and implantable body sensor nodes which does not affect the mobility of the patients with extra security and advance feature. A WBSN should ensure the accurate sensing, tracking of the signal from the body, carry out low-level processing of the sensor signal and wirelessly transmit the processed signal to a local processing unit. In the proposed system, WBSNs, a sparse network of sensors are deployed either directly on the human body, inside the body or embedded in everyday clothes, to record and transmit health data. Body Sensors record and transmit data to a Body Central Unit which aggregates data sent by all Body Sensors and relays the aggregation to a hospital monitoring station from where healthcare professionals can remotely monitor the health parameters of patients or other individuals. This will help the authorized care giver easily diagnose the problem and make available the quick treatment to patient.

The security of these devices is very important factor to make secure the personal data of any patient. Thus no other unauthorized person can get information about the patient disease etc which help to protect privacy of user and data. Important elements of security include data encryption, key management and authentication. Although sophisticated cryptography is the straightforward solution to achieve security goals. The primary objective of this proposed work is to propose effective security and tracking technique for sensor body wireless network with the help of new and effective technique Quantum Cryptography which provides extra security from all type of dangerous attacks and threats.

Objective and Importance of Proposed Research Investigation:-

In our proposed work, we propose a new security framework for Wireless Body Sensor Networks, with also focus on several terms. This Research Proposal mainly

 ISSN: 2454-4248
521 – 526

focuses on tracking and secure connectivity between health monitoring system and patient. The analysis indicates the need for future research on:

- Proposed system will try to effective tracking and monitoring of wireless device in the patient's body.
- Proposed system will provide and improve the current trends in broadcast the patient's body signals to its authorized caregiver.
- Proposed system will try to eliminate network security threats with the help of advance cryptographic technique which helps in the continuous flow of valid information, and to stop violating the privacy of network users and their data.
- Proposed system will try to improve the diagnosis system which helps to maintain the patient's health.

In this proposed work, we investigate the problems of modeling attacks on network and performance and design of network that are robust to attack. We investigate secure communication link establishment in sensor networks through quantum cryptographic key assignment. We also work the problem of quantifying the impact of jamming attacks on network traffic flows in order to provide robust network operation as well as user and data security. In this proposed system, we mainly focused and try to overcome from data loose, jamming due to attacks, security from different type of attack and accurate tracking of body sensor device while it is moving in body.

II. Literature Survey:

Le *et al.* [1] proposed a MAACE protocol where an authorized professional can access the patient's data. Their scheme provides mutual authentication and access control, which is based on elliptic curve cryptography (ECC). Furthermore, the authors claim their scheme can defend from real-time attacks, such as replay attacks, and denial-of-service attacks. Le *et al.*'s protocol provides enough security, but it is susceptible to information-leakage attacks, which could be dangerous for a patient's privacy. As a result, the patient's vital signs are exposed to unauthorized users, which is not acceptable for real-time healthcare applications.

Boukerche-Ren [2] proposed a secure mobile healthcare system using a trust-based multicast scheme. A multicast strategy is used that employs trust to evaluate the behavior of each node. By doing so, only trustworthy nodes are permitted to participate in communications, while the misbehavior of malicious nodes identifies them and they are successfully prevented from communicating which is dangerous for patient security.

Lin *et al* [3] proposed a strong privacy-preserving scheme against global eavesdropping for eHealth systems known as SAGE. The basic idea of SAGE is that a patient information database (PIDB) receives the personal health information (PHI) from patient's body sensors (e.g., accelerometer, blood pressure, oxygen saturation, and temperature sensors); it broadcasts the PHI to all physicians. Then only the applicable physician has access to the patient's PHI. In this system, all PHI information's are stored in the PIDB at the eHealth center. To achieve access control, only registered patients can store their data and only legal physicians can retrieve patients' data from the PIDB. Authors have proposed elliptic curve cryptography based privacy solution and demonstrate a formal proof for the proposed solution against strong eavesdropping. Several other excluding eavesdropping attacks are still becoming dangerous to existing system.

CodeBlue [4] is a popular healthcare research project based on a medical sensor network developed at the Harvard Sensor Network Lab. In this architecture, several medical sensors (e.g., pulse oximeter, EMG, EKG, and SpO2 sensor board onto the Mica2 motes are placed on the patient's body. These medical sensors sense the patient body data and transmit it wirelessly to the end-user devices (PDAs, laptops, and personal computers) for further analysis. The basic idea of CodeBlue is straightforward, a doctor or medical professional issues a query for patient health data using their personal digital assistant (PDA), which is based on a *publish* and *subscribe* architecture. Further, the CodeBlue architecture facilitates RF-based localization which is accurate enough to locate a patient's or medical professional's position. But until now security is still pending or they intentionally left the security aspects for future work.

UbiMon[5] (Ubiquitous monitoring environment for wearable and implantable sensors) is a BSN (Body Sensor Network) architecture composed of wearable and implantable sensors using an *ad hoc* network. UbiMon provide continuous monitoring of an individual's physiological states and capture transient as well as life threatening abnormalities that can be detected and predicted.

UbiMon detect the patient's abnormalities and provide immediate warning to the physician. Apart from this function, the LPU works as a router between BSN nodes and the central server using wireless communication. *CS (Central Sever)*: A CS feeds the patient data to the PD (Patient Database), and can analyze the patient's data on the basis of patient's condition, and detect potential life-

 ISSN: 2454-4248
521 – 526

threatening abnormalities. But the authors did not consider security for wireless healthcare monitoring, which is a paramount requirement of healthcare applications.

Biometric Techniques [6] WBSNs implicitly support biometric techniques for key generation and authentication, since they record and store physical data about an individual. The (improved) fuzzy vault technique uses a fuzzy extractor to extract uniform randomness" from its input, with the rationale that small changes to the input will not cause the extracted output to be different, as long as the changed input remains reasonably close to the original" input. One scientist extends this work for application in WBSNs, focusing on the intercommunication and authentication between sensors". Their key generation is based on extracting feature (F) from the person's ECG signal and generating a monic polynomial with root, F. Their work (ECG-IJS), like the improved fuzzy vault technique is based on accomplishing security by retaining a subset of the coefficients of the monic polynomial a secret. ECG-IJS works on the assumption that the communicating sensors on the human body that employ this technique have the ability to extract ECG signals or are connected to ECG sensors. Authentication in ECG-IJS is accomplished through verification of the hash of the data, encryption key and the subset of the coefficients. Although fuzzy extraction promises increased security in normal WSN applications, when it comes to applying ECG-IJS in WBSNs, one needs to consider the computational overheads added to the resource-constrained data collection sensors by the polynomial arithmetic and the additional overhead of attaching ECG sensors to each sensor on the body that collects data.

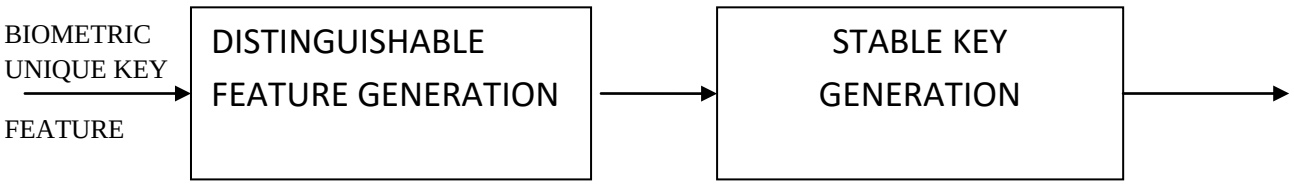

Figure 4: Biometric Based Technique

1. **Research Gaps Identified in the Proposed Field of Investigation:**

    1) Accurate Tracking of WBD
    2) Authentication
    3) Ineffective Encryption Technique
    4) Network Eavesdropping & Data Modification
    5) Less number of people Interaction
    6) Loss of data and personal information
    7) Jamming

Suggestions and Proposed Flow Chart of Research:

Wireless networks and their associated security challenges will continue to attract much research attention Thus, security in resource-constrained wireless networks already are and will continue to be of significant interest in the future. Sensor networks are comprised of sensors (or detecting elements) that sense the environment in which they are placed, record data about the environment, and relay the recorded data to a central monitoring station or base station, where data is aggregated. A simple example for this would be the monitors connected to patients in critical care units in hospitals, which monitor their parameters such as blood pressure, oxygen saturation, heart function etc.

In a remote healthcare setting, this enables doctors to monitor patients continuously, and keep tabs on events that could aggravate and potentially prove fatal to the patient at a future time. A Wireless Sensor Network (WSN) is a set up in which a group of sensors are equipped with independent power sources and processing circuits intended to `sense' or record data about specific parameters in the environment where they are deployed.

 ISSN: 2454-4248
521 – 526

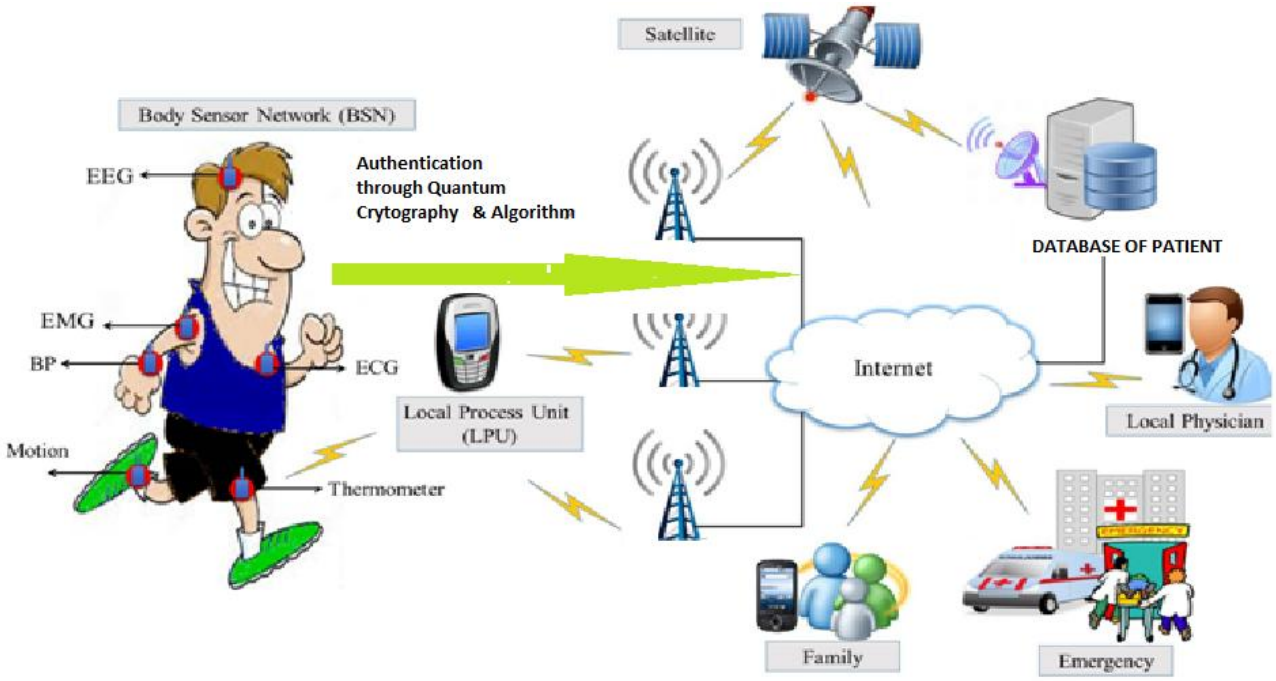

Figure 1: Proposed Methodology and Technique

In this proposed system first of all a WBS Device in the body of patient. Wireless sensors are well equipped and connected directly to the central communication unit. A doctor/ Authenticate person can easily access al related information from implanted device. An authentication process starts to access any information from WBSN. Quantum cryptography technique is used to provide security. Database of central communication center can automatically save all data (movement, activity etc of wireless device in human body). Patient and doctors both can access this data. Tracking of the wireless body device is controlled by central communication unit. CCU also receive signal time to time from wireless body device. Tracking of this device depends upon the travelling time of signals. Major security issues like confidentiality, integrity, dependability and authentication features will try to achieve by applying some quantum cryptography and some effective algorithmic functions.

III. Conclusion:

The main importance of this proposed research is to make secure the data of patient. The details of disease (personal information of patient) can not revealed at any case. The communication between patient and his doctor remains secret until the permission of both patient and doctor. A secure two way communication is trying to achieve in this proposed work.

Hazardous attacks like eavesdropping, Denial of service etc will achieve through this proposed work. This proposed works also helps us to recover data loose, tampering of data. Now a day's, except all of these jamming is very big problem. All type of data can be jammed any time due to it communication blocked. Time is very crucial factor in medical sector because it is related to life of human beings. In this proposed work we will try to resolve the problem of jamming too.

If any patient was diagnosed with a medical condition and his doctor advised him to be under constant monitoring. Understanding that his career was equally important, he advised him to wear wireless body sensors and use her cellular phone as part of a Wireless Body Area Network (WBSN) application to remotely monitor her health. It is very useful that patient work while her doctor was monitoring his health, Patient went back to her daily routine. This situation, a portion of it or something similar, could be part of daily activities for many people around the world. It makes our lives convenient and easier to manage.

Wireless networking allows for readily available access to a wealth of information without an infrastructure-based network, suggesting that WBSN will soon be ubiquitously deployed for personal, social, commercial, industrial, and military applications. Examples WBSN applications include home and health care networking, surveillance, inventory and product tracking, disaster recovery and rescue, medical patient monitoring, and tactical military applications. Another particularly useful application of WBSNs is in the military, where commanding officers could monitor the health of soldiers in the battle field.

References:

[1] Fagen Li, Jiaojiao Hong (2016), Efficient Certificateless Access Control for Wireless Body Area Networks", IEEE SENSORS JOURNAL, VOL. 16, NO. 13, JULY 1, 2016.

[2] Azzedine Boukerche, and Yonglin Ren (2009), "A Secure Mobile Healthcare System using Trust-Based Multicast Scheme" IEEE Journal on selected areas in communications,VOL. 27, NO. 4, MAY 2009.

[3] Xiaodong Lin, Rongxing Lu, Xuemin, Yoshiaki Nemoto, and Nei Kato, "SAGE: A Strong Privacy-Preserving Scheme Against Global Eavesdropping for eHealth Systems", IEEE Journal on selected areas in communications, VOL. 27, NO. 4, MAY 2009.

[4] Malan, D, Jones, T.F.,Welsh, M. Moulton, "CodeBlue: An *Ad-Hoc* Sensor Network Infrastructure for Emergency Medical Care". In Proceedings of the MobiSys 2004 Workshop on Applications of Mobile Embedded Systems *(WAMES 2004)*, Boston, MA, USA, 6–9 June 2004.

[5] Ng, J.W.P., Lo, B.P.L., Wells, O., Sloman, M., Peters, Toumazou, Yang, " Ubiquitous Monitoring Environment for Wearable and Implantable Sensors (UbiMon)". In Proceedings of 6th International Conference on Ubiquitous Computing (UbiComp'04), Nottingham, UK, 7–14 September 2004.

[6] Vijey Thayananthan and Ahmed Alzahrani, " Analysis of Key Management and Quantum Cryptography in Wireless Sensors Networks", *IJCA Special Issue on "Network Security and Cryptography" NSC, 2011.*

Bibliography:

[1] Pardeep Kumar and Hoon-Jae Lee, "Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey", *Sensors* 2012, *12*, 55-91; doi:10.3390/s120100055, ISSN 1424-8220, www.mdpi.org/sensors.

[2] Moshaddique Al Ameen and Kyung-sup Kwak, "Social Issues in Wireless Sensor Networks with Healthcare Perspective" The International Arab Journal of Information Technology, Vol. 8, No. 1, January 2011

[3] Shikha Pathania et al, International Journal of" Security Issues in Wireless Body Area Network " Computer Science and Mobile Computing, Vol.3 Issue.4, April-2014, pg. 1171-1178

[4] Narasimha Kamath A " A Survey on Data Privacy Approaches in Biomedical Sensor Network" International Journal of Computer Applications (0975 – 8887) Volume 105 – No. 13, November 2014.

[5] Vivek Katiyar, Narottam Chand," Recent advances and future trends in Wireless Sensor Networks" International Journal Of Applied Engineering Research, Dindigul Volume 1, No 3, 2010, ISSN 09764259.

[6] Jyoti S. Kamble, Amarsinh V. Vidhate, " Wireless Body Area Network Security"International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 12, December 2015 ISSN: 2277 128X.

[7] K.Suriyakrishnaan, D.Sridharan, "A Review Of Reliable And Secure Communication In Wireless Body Area Networks" Thirteenth IRF International Conference, 14th September 2014, Chennai, India, ISBN: 978-93-84209-51-3.

[8] Syeda Farha Shazmeen, Shyam Prasad " A Practical Approach for Secure Internet Banking based on Cryptography" International Journal of Scientific and Research Publications, Volume 2, Issue 12, December 2012 1 ISSN 2250-3153.

[9] M. Somasundaram+ and R. Sivakumar, "Security in Wireless Body Area Networks: A survey", 2011 International Conference on Advancements in Information TechnologyWith workshop of ICBMG 2011, IPCSIT vol.20 (2011) © (2011) IACSIT Press, Singapore

[10] Christos Douligeris *, Aikaterini Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state-of-the-art", Department of Informatics, University of Piraeus, 80 Karaoli and Dimitriou Str, Piraeus 18534, Greece Received 9 October 2003; accepted 13 October 2003

[11] S. Sangari and 2Martin Leo Manickam, "A Light-Weight Cryptography Analysis For Wireless Based Healthcare Applications", Journal of Computer Science 10 (10): 2088-2094, 2014 ISSN: 1549-3636 © 2014 Sangari and Manickam.

[12] Xu Wu , "A Lightweight Trust-based Access Control Model in Cloud-Assisted Wireless Body Area Networks", International Journal of Security and Its Applications Vol.8, No.5 (2014), pp.131-138 http://dx.doi.org/10.14257/ijsia.2014.8.5.13.

[13] Junaid Ahsenali Chaudhry 1, Shafique Ahmad Chaudhry, "Phishing Attacks and Defenses", International Journal of Security and Its Applications V ol. 10, No. 1 (2016), pp.247-256 http://dx.doi.org/10.14257/ijsia.2016.10.1.23

[14] Dragan Vidakovic and Dusko Parezanovic, "Generating Keys in Elliptic Curve Cryptosystems", International Journal of Computer Science and Business Informatics ISSN: 1694-2108 | Vol. 4, No. 1. AUGUST 2013

[15] Aikaterini Mitrokotsa · Melanie R. Rieback, "Classifying RFID attacks and defenses", Inf Syst Front (2010) 12:491–505DOI 10.1007/s10796-009-9210-z

[16] Lu Shi , "BANA: Body Area Network Authentication Exploiting Channel Characteristics", WiSec'12, April 16–18, 2012, Tucson, Arizona, USA.Copyright 2012 ACM 978-1-4503-1265-3/12/04

[17] Akansha Dhobley1, Prof. N. A. Ghodichor, Prof. S. S. Golait3, Dr. P. S Prasad, "Design and Implementation of Wireless Sensor Network for Health Care Monitoring in Hospitals via Mobile", International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 9, September 2015

[18] Rucha Fasate, Ms. A. Sakhare, Ms. Richa Sharma, "E-Health Care Monitoring System", International Journal of Research in Advent Technology, Vol.2, No.2, February 2014E-ISSN: 2321-9637

ISSN: 2454-4248
521 – 526

[19] Vishwa gupta, Gajendra Singh, " Advance cryptography algorithm for improving data security", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 1, January 2012 ISSN: 2277 128X

[20] Chiu C. Tan, "Body Sensor Network Security: An Identity-Based Cryptography Approach", WiSec'08, March 31–April 2, 2008, Alexandria, Virginia, USA. Copyright 2008 ACM 978-1-59593-814-5/08/03.