Network and Complex Systems
ISSN 2224-610X (Paper) ISSN 2225-0603 (Online)
Vol.3, No.1, 2013-Selected from Inter national Conference on Recent Trends in Applied Sciences with Engineering Applications
www.iiste.org

Body Sensor Network: A Modern Survey & Performance Study in Medical Perspect

Ashwini Singh, Ajeet Kumar, Pankaj Kumar
Department of Electronics and Communication Engineering, NIT PATNA
ashwini.singh075@gmail.com, ajeetthebest@gmail.com, pankajsinha65@gmail.com

ABSTRACT
As because of modern emerging technologies, low power integrated circuits and wireless communication has enabled a new generation of sensors network. The incorporation of these sensors networks in Health care is very popular and plays a vital role in breath breaking situations. The deployment of monitoring hardware incorporated with various wireless standards plays a key role in regard to interoperability, invasion privacy, sensors validation data consistency and interference related issues. The goal of our paper is to make a comparative study in realm of modern wireless trends such as Bluetooth, Wi-fi, Zigbee and Wibree and related facets.
Index Terms– Wireless Body area network, Zigbee, Wi-fi, Bluetoooth

I. INTRODUCTION

Now a days, Wireless Sensors Network (WSN) has becomes a assured technology in the realm of advanced applications. The one of its latent position is in the form of unguided biomedical sensor network to determine physiological sign. Wireless Body Area Network (WBAN) is a unguided network utilized for interaction among sensor nodes in or about the human body in order to supervise critical body parameters and activities. These supervising signs are collected by a personal server, e.g. PDC or Smart phones which acts as a sink for the information of the sensors and send them to caregivers for proper health supervising.

The personal server have some memory in which some results are arranged which it gives to the patient at the time of emergency it acts like a feedback, if the situation is not handle by the PDC then it transfers the signal to caregivers by unguided media. There are different issues highlighted in the employment of WBAN technology. This survey executes a atomistic review on pronominal investigations that emphasis in procured related facts in WBAN as well as WLAN. This paper is arranged into the different parts which provides a short introduction of WBAN and WLAN and look out attributes of pronominal differences between them and fetch attributes of WBAN and pulls general architecture and handle postulates in WBAN and also intercommunicating much on security issues, we shall also see the features of short range wireless techniques and compare them according to their performance. And at last gear up related investigations in security bare for WBAN.

II. ATTRIBUTES OF WBAN

WBAN is a communication network between human and computers through wearable devices. To establish a interaction between these devices, unguided sensor network and ad hoc network techniques may be used. The tiny sensor senses the signals from the body and send it to the processor through unguided media[1]. But due to some emblematic features of WBAN current protocols create for these network are not always feasible to favour WBAN. To favour this level, TABLE 1 modifies the general differences between WSN and WBAN[2][3].

TABLE 1: THE COMMON DIFFERENCE BETWEEN WSN AND WBAN

	WBAN	WSN
Arrangement	The number of sensors nodes arranged by the users depends on various factors. WBAN doesn't engage redundant nodes.	WSN is often arrange in places that may not be easily accessible by operators which require more nodes to be placed to compensate for node failures.
Data rate	WBAN may occur in a more sporadic style and reliable data rate	WSN is plugging for event based monitoring where events can happen at erratic interval.
Portability	WBAN users may move around. WBAN nodes share the same mobility pattern.	WSN nodes are usually considered stationary.
Inactivity	Restoration of cells in WBAN nodes is much easier done when energy Salvation is definitely beneficial	Nodes can be physically unreachable after deployment. It may be necessary to maximize battery life-time in WSN at the expense of higher inactivity.

WBAN was introduced from real WSN (WPAN) technologies[4]. WPAN is a personal area network using unguided acquaintance consistently within a short range (≤ 100m). It is used for communication among the devices such as cell phones and computer peripherals, as well as personal digital collaborator (PDC). Permissive technologies for WBAN is Wibree, IrDA, Bluetooth, Zigbee , Wi-fi, Ultra-wide band(UWB), etc. Despite this the most promising wireless standard for WBAN application is Zigbee, suite for high level communication. It is IEEE 802.15.4 standard often used in mesh network form to transmit data over longer distances. This allow Zigbee network to be formed ad-hoc, with no centralised control or high power Tx/Rx capable to reach all of the devices. Zigbee is aimed at those applications that require low data rate, low battery life and secure networking. Zigbee is capable of handling large sensors network upto65000 nodes. Another WPAN technology is Bluetooth, IEEE 802.1.1 standard[4].

Basic requirement of WBAN include the requirements of WPAN, such as low power, low data rate unguided sensors network standard Zigbee. Despite the fact that Zigbee does not fetch majority of core technical requirements of WBAN features and the for a standard specifically designed for WBAN. Diagnosticate the great market potential and rapid technological enlargement in this field. The IEEE is ongoing an 802.15.6 standard optimized for low power WBAN favouring at a data rate from 10Kbps to 10 Mbps[1].

The exclusive endowment compared to majority of core WPAN are as follows:

- WBAN is a small scale network rather than WPAN is a relatively short range communication technique inclusive the communication in or on a human body with the maximum range of (≤100m).
- A star topology is basically used WBAN where communication is organised in the heart of sensor nodes and is directly linked to a master node. Despite, it cannot always meet the desired authenticity requirement. Thus a star-mesh hybrid topology extends the fashionable approach and creates mesh networking among central coordinates in multiple star networks.
- Gadgets incorporating WBAN are firmly limited in their computational capabilities and required scalable completion; data rate upto10Mbps, and power consumption upto40MW.
- Data that are detected, collected and transmitted in WBAN is comparatively sensitive; highly secure and confidential.
- Gadgets of WBAN closely surround the human body to consist of its transportation system are highly safety requirements.

III. ACCUSTOMED ARCHITECTURE

The proposed wireless area body network for health monitoring integrated into a border multitier medicine system & in this architecture ,WBAN is compared to other wireless network. In fig 1 a WBAN compared with other types of wireless network[2]. Each type of network has a typical enabling technology, defined by IEEE. A WPAN used IEEE 802.15.1 (Bluetooth) or 802.15.4 (zigbee) , a WLAN uses IEEE 802.11(Wi-fi) & WMAN IEEE 802.16 .The communication in a WAN can be established via satellite links. As declared before , admitting challenges faces by WBAN are in many ways similar to WSN, there are elemental differences between the two requiring special attention.

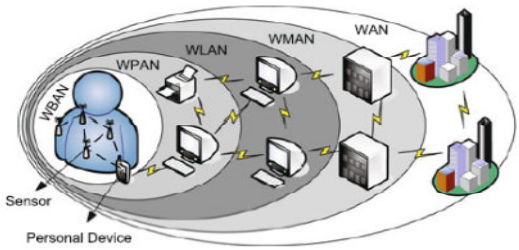

Figure 1: Positioning of a WBAN in the realm of wireless networks.

In TABLE 2, a schematic overview of differences between WSN and WBAN is given [2][3][4].

TABLE 2: SCHEMATIC ANALYSIS OF DIFFERENCE BETWEEN WSN AND WBAN IS GIVEN:

CHALLENGES	WSN	WBAN
Scale	Monitored environment (m/km)	Human body (cm/m)
Node number	Many redundant nodes for wide area coverage	Fewer, limited in space
Result accuracy	Through node redundancy	Through node accuracy and robustness
Node tasks	Node performs a dedicated task	Node performs multiple task
Node size	Small is preferred, but not important	Small is essential
Network topology	Very likely to be fixed and static	More variable due to body movement
Data rates	Homogeneous	Heterogeneous
Node replacement	Performed easily, nodes even disposable	Replacement of implanted nodes difficult
Node lifetime	Several years/months	Several years/months, smaller battery capacity
Power supply	Accessible and likely to be replaced more easily and frequently	Inaccessible and difficult to replace in an implantable setting
Power demand	Likely to be large, energy supply easier	Likely to be lower, energy supply more difficult
Energy scavenging source	Most likely solar and wind power	Most likely motion(vibration) and thermal (body heat)
Biocompatibility	Not a consideration in most applications	A must for implants and some external sensors
Security level Lower	Lower	Higher, to protect patient information
Impact of data loss	Likely to be compensated by redundant nodes	More significant, may require additional measures to ensure QoS and real-time data delivery
Wireless Technology	Bluetooth, Zigbee, GPRS, WLAN,…	Low power technology required
Impact of data loss	Likely to be compensated by redundant nodes	More significant, may require additional measures to ensure QoS and real-time data

IV. ENGROSSSMENT OF WBAN

We classify demand of WBAN into two categories i.e. system and security. Further detail is described in the following subsection.

A. System exigency

This subsection provides brief description of system requirements that viewed in three different aspects such as type of devices, data rate and energy.

a) Types of devices.

Sensor node: A device that responds to and gathers data on physical catalyst processes the data if necessary and reports this information wirelessly. It consists of several components which are sensor hardware, a power unit, a processor, memory and a transmitter or transceiver.

Gateway: It gathers all the information acquired by the sensor nodes and informs the users. The components area power unit, memory and transreciever. This device is also called a body control unit(BCU),body gateway or a sink.

Monitoring Server: It is consists of database for data storage and processing and analyzing software for delivering

system intended services.

b) Data rates

The reliability of the data transmission is provided in terms of the necessary bit error rate (BER) which is used as a measure for the number of packets lost. For a medical device, the reliability depends on the data rate. Low data rate devices can cope with a high BER while devices with a higher data rate require a lower BER. The required BER is also dependent on the criticalness of the data.

c) Energy

Energy consumption can be divided into three domains: sensing, communication and data processing[2][5]. Despite, the energy consumption for communication is more than computation in WBAN. Further, higher security requirements usually correspond to more energy consumption for cryptographic operations.

B. Security Requirements

The security and privacy of patient-related data are two indispensable components for the system security of the WBAN. By data security, it means the protection of information from unauthorized users while data being stored and transferred and data privacy means right of individuals to control the collection and use of personal information about themselves. Security and privacy issues are raised automatically when the data is created, transferred, stored and processed in information systems[8]. The Health Insurance Portability and Accountability Act (HIPAA) mandates that, as the sensors in WBAN collect the wearer's health data (which is regarded as personal information), care needs to be taken to protect it from unauthorized access and tampering[9][11]. Because WBAN systems and their supporting infrastructure are operated with extremely stringent constraints, they present a greater challenge in the areas of throughput, data integrity and data security when compared to traditional clinical systems. The security mechanisms employed in WBAN for the later need specific features that should be taken into account when designing the security architecture. Thus, the system needs to comply with the following major security requirements as in TABLE 3 [4][8][10].

TABLE 3: MAJOR SECURITY REQUIREMENTS IN WBAN

Major security requirement	Description
Data storage security requirements	
Confidentially	Patient-related data should be kept confidential during storage periods. Especially, its confidentially should be robust against node compromise and user collusion. Encryption and Access Control List are main methods providing data confidentiality.
Integrity assurance	Patient-related data must not be modified illegally during storage periods
Dependability	Patient-related data must be readily retrievable when node failure or data erasure happens.
Data access security requirements	
Access control (privacy	A fine-grained data access policy shall be enforced to prevent unauthorized access to patient-related data generated by the WBAN.
Accountability	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
Revocability	The privileges of WBAN users or nodes should be deprived in time if they are identified as compromised or behave maliciously.
Non repudiation	The origin of a piece of patient-related data cannot be denied by the source that generated it.
Other security requirements	
Authentication	The sender of the patient-related data must be authenticated, and injection of data from outside the WBAN should be prevented
Availability	The patient-related data should be accessible even under denial-of-service (DoS) attacks.

V. WBAN APPLICATIONS

The WBAN application targeted IEEE 802.15.6 standard are divided into medical and non medical application as given in fig.2. Medical application include collecting vital information of a patient continuously and forward it a remote monitoring station for further analysis[6]. The huge amount can be used to prevent the occurrence of myocardial infarction and treat various diseases such as gastrointestinal tract, cancer, asthma & neurological disorder. WBAN can also be used to help people with disabilities. For ex retina prosthesis, chips

can be planted in human eye to see at an adequate level. Non medical application include monitoring forgetting things, data file transfer, gaming and social networking application. In [7] gaming, sensor in WBAN can collect coordinate movements of character in the same, ex- moving cricket player or capturing the intensity of ball in tennis. The use of WBAN in social networking allows people to exchange digital profile or business allows people to exchange digital profile or business card only by shaking hands.

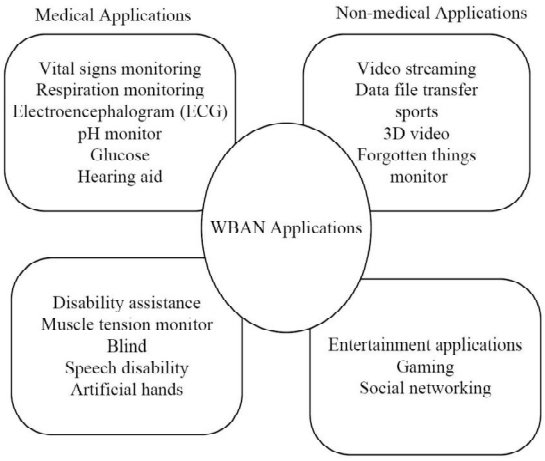

Fig. 2. WBAN applications

VI. RELATED RESEARCH

Several research groups have been developing the implantable or wearable devices for health monitoring in WBAN communications. However, these researches mainly focus on building system architecture and in lesser extent on developing networking protocols. Besides, it is difficult to discover solutions providing security for WBAN and security has generally been covered separately. Extending the scope of technology, there are several security protocols in general sensor networks. Security Protocols for Sensor Networks (SPINS) is a set of protocols for achieving security requirements like confidentiality, integrity and authenticity in sensor networks and uses several symmetric keys to encrypt the data as well as compute the Message Authentication Code (MAC)[4][11].

However, SPINS is only considered in general sensor networks, so that it is inadequate to apply in WBAN as it has environmental features like the human body and limited computing resources. Some researches show the security for sensor nodes in or on the human body in WBAN. They show that the sensors have to make use of cryptographic algorithms to encrypt the data they send to control node and the random number which is used in security protocols can be generated by biometrics[12]. Biometrics approach uses an intrinsic characteristic of the human body as the authentication identity or the means of securing the distribution of a cipher key to secure inter-WBAN communications. At initial stage, several security schemes of WBAN are established by the symmetric cryptosystem due to limited resources, but have problems like delaying the disclosure of the symmetric keys and providing weak security relatively since it is not resilient against physical compromise[13].

Furthermore, the complexity of sensor node's key managements in WBAN gives each component overload. On the contrary, some researches utilizing the asymmetric cryptosystem in mobile and ad hoc networks also have been proposed, and tried to examine the unique characteristics of WBAN[8][14]. One concern about the asymmetric cryptosystem is a resource constraint problem but recent work has shown that performing ECC consumes a lot less of memory and computing power[12][14]. These researches dealt with a scope of limited WBAN but they exclude the implanted sensor networks. The objective of WBAN is also the implementation of body area network that can contact with everywhere in, on, and out the human body. By comparison, each approach has several issues to be considered in terms of the security services in WBAN. Further, there is a trade-off between performance and security. Related to these, another research group has implemented these two heterogeneous cryptosystems in their research which provides security and privacy to WBAN. In [4], they believe that these two cryptosystems can be applied in the authentication of WBAN depleting each weak point of them at once. They primarily focus on the authentication in the overall coverage of WBAN including in-, on- and out body to provide the strong and adequate security for WBAN.

VII. CONCLUSION

WBAN is an emerging and promising technology that will change people's healthcare experiences revolutionarily. It brings out a new set of challenges in terms of scalability, sensor deployment and density, energy efficiency, security and privacy and wireless technology. In this survey, we have reviewed the current development on Wireless Body Area Network and we focused in security issues faced by this technology. In particular, this work presents an overview of the differences between Wireless Body Area Network and Wireless Sensor Network. We presented differences of architecture in WBAN and other type of Wireless sensor network. Several key applications will benefit from the advanced integration of WBAN and emerging wireless technologies. They include remote health monitoring, military, sports training and many others. It is also important to highlight here that WBAN poses with various type of security problems. Thus, we believe that WBAN requires a strong security system and part of it is authentication. A secured authentication system is extremely needed in various applications WBAN technology particularly in medical and military. The proposed protocol is potentially useful to be utilize in WBAN by satisfying their technical requirements keeping pace with the standardization of IEEE 802.15.6[4]. Our next step is to discover hybrid authentication protocol in providing a strong security system for WBAN.

ACKNOWLEDGMENT

This work is supported by National Institute of Technology, Patna as a part of partial fulfilment of Post Graduate degree in Communication systems for the academic year of 2011-2013.

REFERENCES

[1] Selimis, Georgios et al. "A Lightweight Security Scheme for Wireless Body Area Networks: Design, Energy Evaluation and Proposed Microprocessor Design," Journal of Medical Systems, 2011, pp. 1-10-10, doi: 10.1007/s10916-011-9669-2.

[2] Latré, Benoît, Bart Braem, Ingrid Moerman, Chris Blondia, and Piet Demeester. "A survey on wireless body area networks," Wireless Networks, vol. 17, 2010, pp. 1 18, doi: 10.1007/s11276-010-0252-4.

[3] Chen, M., Gonzalez, S., Vasilakos, A., Cao, H., & Leung, V. C. M. "Body Area Networks: A survey," Mobile Networks and Applications, vol. 16, 2011, pp. 171-193, doi:10.1007/s11036-010- 0260-8.

[4] Jang, C. S., Lee, D. G., Han, J.-W., & Park, J. H "Hybrid security protocol for wireless body area networks," Wireless Communications and Mobile Computing, vol. 11, 2011, pp. 277-288, doi: 10.1002/wcm.884.

[5] Jingwei Liu and Kyung Sup Kwak. "Hybrid security mechanisms for wireless body area networks," Ubiquitous and Future Networks (ICUFN), 2010 Second International Conference on , 2010, pp. 98- 103, doi: 10.1109/ICUFN.2010.5547221.

[6] IEEE P802.15.6/D01,Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs) used in or around a body, May 2010.

[7] S. Saleem, S. Ullah, and K.S. Kwak, A Study of IEEE 802.15.4 Security Framework for Wireless Body Area Networks, Sensors, vol.11, No.2, pp. 1383-1395, 2011.

[8] Lim, S., Oh, T. H., Choi, Y. B., & Lakshman, T.. "Security Issues on Wireless Body Area Network for Remote Healthcare Monitoring," 2010 IEEE International Conference on Sensor Networks Ubiquitous and Trustworthy Computing, 2010, pp. 327-332, doi: 10.1109/STUC.2010.61.

[9] Venkatasubramanian, K. K., Banerjee, A., & Gupta, S. K. S.. "PSKA: usable and secure key agreement scheme for body area networks," IEEE transactions on information technology in biomedicine a publication of the IEEE Engineering in Medicine and Biology Society, vol. 14, 2010, pp. 60-68.

[10] Mana, M., Feham, M., & Bensaber, B. A.. "SEKEBAN (Secure and Efficient Key Exchange for wireless Body Area Network)," Science And Technology, vol. 12, 2009, pp. 45-60.

[11] Liu, J., & Kwak, K. S.. "Towards Security Issues and Solutions in Wireless Body Area Networks," 6th International Conference on Networked Computing (INC 2010), 2010, pp. 1-4, doi: 10.1109/ICUFN.2010.5547221.

[12] Poon, C. C. Y., Zhang, Y. T., & Bao, S.-D.. "A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health," Communications Magazine IEEE, IEEE, vol. 44, 2006, pp. 73-81, doi: 10.1109/MCOM.2006.1632652.

[13] William, C., Tan, C. C., & Wang, H.. "Body Sensor Network Security : An Identity-Based Cryptography Approach," Proc. ACM Conference on Wireless Network Security (WiSec '08), ACM Press, 2008, pp. 148-153, doi: 10.1145/1352533.1352557.

[14] Sharmilee, K. M., Mukesh, R., Damodaram, A., & Subbiah Bharathi, V.. "Secure WBAN Using Rule-Based IDS With Biometrics And MAC Authentication," 2008 10th IEEE International Conference On EHealth Networking Applications and Services, IEEE, 2008, pp.102-107, doi: 10.1109/HEALTH.2008.4600119.