An Analytical Review of WBAN (Wireless Body Area Network)

[1]Harpreet Kaur, [2]Manwinder Singh,
[1]M.Tech Student, [2]Associate Professor,
[1]Electronics & Communication Engineering,
[1]Rayat Institute of Engineering & Information Technology, City S.B.S Nagar,Country India

Abstract: The development of wireless communication technologies and sensors has started the development of a Wireless Body Area Network (WBAN). The wireless nature of the network and various sensors provides a variety of new, intelligent and innovative applications to enhance health compliance and replace health care applications. In the past few years, some studies have focused on the establishment of systematic design of health compliance to enhance the technical requirements specifically designed for WBAN. However, as part of the communications media, WBAN faces a variety of security issues such as information loss, authentication, and access control. This article reviews the key aspects of WBAN in many applications. We have provided the WBAN infrastructure to provide solutions for on-demand, emergency and normal traffic. We further have discussed WBAN's in-vivo antenna design and low-power MAC protocol. In addition, we briefly have introduced some WBAN applications by examples.

IndexTerms **-WBAN (Wireless Body area network), BAN Network Coordinator (BNC), sensor network.**

I. INTRODUCTION

WSN (Wireless sensor network) is used for monitoring some of the metric in varied applications, such as, habitant observing, environment checking, shrewd homes and checking of farmer field [1]. The scattering of remote sensor s takes place because of the detection of the regions to the screen field. WBAN (Wireless body area network) is a novel rising sub field for WSN. The main usage of WBAN is mainly checking. The remote sensors are located on human body or could be embedded in the body for the monitor the basic signs such as body temperature, circulatory strain, glucose level, heart rate, and so on. The usage of WBAN innovation is for the monitoring of the parameters that lessens the patient consumption in health care. With the WBAN assistance, the patients are monitored at home for more time. The sensors regularly monitor the information and send it to the medicinal server [2].

1.1 WBAN (Wireless Body area network) Architecture

The fig.1 below shows a secure level 3 WBAN architecture for medical and non-medical applications. Level 1 contains body with on-body BAN nodes (BN) like electrocardiograms (ECG) for monitoring electrical activity of the heart, oxygen saturation sensor (SpO2) for measuring oxygen levels, and electromyography (EMG) activity.

Level 2 has BAN Network Coordinator (BNC) that collects important patient information from BN and communicates with the base station. Level 3 contains many remote base stations for storing patient medical / non-medical records and providing relevant (diagnostic) advice. Traffic is divided into on-demand, emergency and normal traffic. On-demand traffic is initiated by the BNC to get some information. Emergency flow starts when the national array exceeds a predefined threshold. Normal traffic is data traffic under normal conditions, with no time requirements and on-demand events [3].

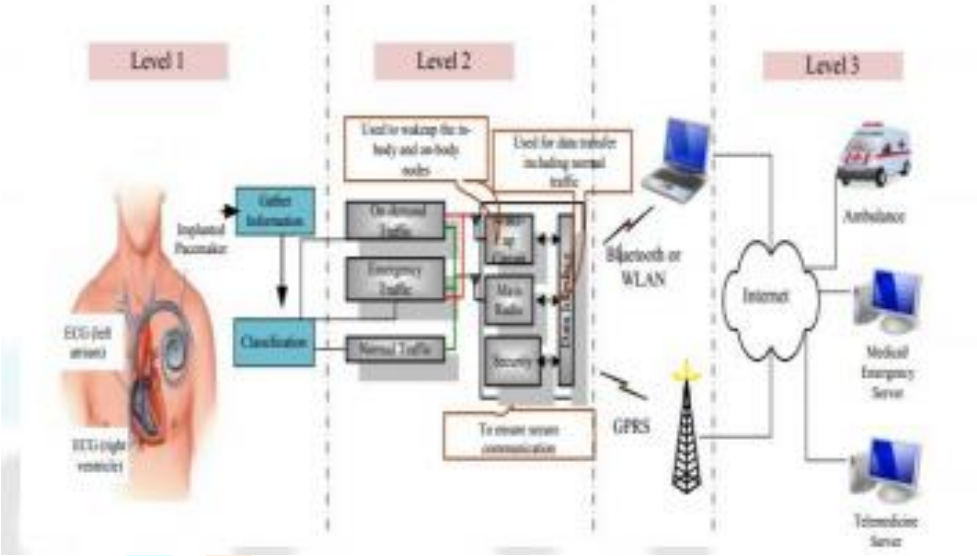

Figure 1 WBAN architecture

Normal data is integrated and executed by the BNC. The BNC has wake-up circuit, a main radio and a safety circuit, all of which is connected for data interface. Wake-up circuits are utilized to provide on-demand and emergency services. Security circuits are utilized for preventing malicious interaction with the WBAN [4].

1.2 WBAN Applications

The applications of WBAN have more prospective for different applications like for remote medical diagnosis, military and interactive gaming applications. Below table defines the few of in body and on body applications.

In-body applications have examining and program variations for pacemakers and implantable cardiac defibrillators, bladder function management, and limb movement restoration. It considers monitoring forgotten things, developing a social network, and examines soldier exhaustion and battle readiness [5].

Table 1 In- Body and On- Body Sensor Networks Applications

Type of application	Sensor node	Data rate	Duty cycle	Consumption of power	QoS	Privacy
In body application	Glucose sensor	Few kbps	<1%	Very les	Yes	High
	Pacemaker	Few kbps	<1%	Less	Yes	High
	Endoscope capsule	>2Mbps	<50%	Less	Yes	Medium
On body application	ECG	3 kbps	<10 %	Less	Yes	High
	Sp02	32bps	<1%	Less	Yes	High
	BP (Blood pressure)	<10bps	<1%	High	Yes	High
In body Non medical application	Music for headsets	1.4 Mbps	High	Comparatively High	Yes	Low
	Monitoring of forgotten things	256 kbps	Medium	Less	No	Low
	Social networking	<200 kbps	<1%	Less	No	High

II. WBAN REQUIREMENTS

The categorization of WBAN is in two categorizes, namely, system and security requirements. More detail has been defined in below sub sections [6]:

2.1 System Requirements

This section describes short system requirements being viewed in three dissimilar aspects like, data rate, device type and energy [7].

Table 2 System Requirements

Types of Devices	Data rates	Energy
Sensor Nodes • The device that collects the data on the process of physical stimuli if require and provides the report wirelessly. • It has number of components that contains power unit, processor, and transmitter/transreceiver and so on.	• The data transmission dependency has given interims of BER (bit error rate) which is considered as a live for packer lost amount. • The dependency of data rate is on medical device. • The addressing of high BER is on low rate devices and low BER acquires better rate • The mentioned BER is concerned about the information critical nature.	• Energy consumption is categorized in three domains: ➢ Sensing ➢ Processing ➢ Communication • More security requires general correspond for more energy consumption for operations of cryptographic discipline.
Gateway (Personal device) • It collects the information from the sensor node and informs the users. • The components considered are transreceiver, memory and power unit.		
Monitoring Server It has database for data storage, processing and examining the software for system planned services delivery.		

2.2 Security necessities

The privacy and security of patient connected knowledge square measure with two indispensable aspects for WBAN system security. The security of WBAN has been classified in Data storage, data access and other security requirements as described in below table [8]:

Table 3 Security requirements

Main Security Requirements	Narration
Data Storage Security Requirements	
Confidentially	Patient related data has to be remain confidential while storage periods. In particular, it has to robust for node compromise and client collusion. Access control and encryption list are the major techniques for giving data confidentiality.
Integrity assurance	The data of patient has to be amended while storing periods.
Dependability	The data of patient has to be instant retrievable when the failure of node with the data erasure occurs.
Data access security Requirements	
Access control (Privacy)	Fine grained access of data would be enforced for the prevention of unauthorized access towards patient data being.
Accountability	When the WBAN client mistreats the privileges for carrying the unauthorized actions than the client would be held and identified accountable.
Revocability	The WBAN node or user privilege has to be defined in time if the identification has been behaved or compromised maliciously.
Non-repudiation	The initialization of patient dependent data that cannot be deny by the source that produced it.
Other Security Requirements	

Authentication	The sender that has sent the data of patient should be authenticated and data injection from WBAN outside has to be prevented.
Availability	The data of patient has to be accessible in DoS (Denial of Service).attack

2.3 Existing Security Mechanisms

The security mechanisms are utilized for detecting, enduring an preventing the security attacks, even number of significant security mechanism are there from the ancient networks like Ad hoc and wired network for the resource unnatural wireless medical sensor network, so, below sub section defines the issues in the existing security mechanisms [9]:

2.3.1 Cryptography

a) For the development of safe attention application, strong cryptographic functions, physiological info an unit preponderating necessities are required. The mentioned functions provide security and privacy for the varied malicious attacks.
b) Selecting acceptable cryptography area unit is an issue for the resources of medical devices nods which may give security with the usage of lesser resources, therefore, it can be said that cryptographic functions provides security nd privacy to the patient.
c) The major factors for the selection of cryptography are communication and computation ability for sensor nodes.
d) While applying the protection method for resource forced medical sensors need to be selected with the support of consequent considerations like memory, energy and execution time etc.

2.3.2 Key management

The protocols of key management are the measure for general needs for development a safe application that can utilized for setting and distributing different cryptographic key forms to nodes in the network. Usually, some key management styles protocols, like, key pre-distribution, trusty server and self imposed [10].

Table 4 Key management Styles

Key management styles	**Description**
Trusted Server	The key management protocol has a trusty BS (Base station) accountable for the establishment of key agreement in the network while keeping more number of resource gateways. The trust server is a scheme that provides more security to hierarchical network in more atmosphere period.
Key pre-distribution	The key management protocols area unit carries symmetric key cryptography, when the secret key area carries itself in the network. The key pre-distribution protocol are easy for the execution and sends a smaller amount of complex process with the creation of more resource networks.
Self enforcing	It provides an infrastructure of public key that provides number of advantages, like more security, memory potency and quantifiably. Though, few researchers has depicted the elliptic curves cryptographic curves cryptographic method which is dependent on the schemes which are feasible for resource affected networks.

2.3.3 Secure Routing

In home care or disaster events, the sensor device may need to send data to other devices than its direct radio. Therefore, routing and message forwarding can be key services for end-to-end communication. To date, several routing protocols have been used for sensor networks; none of them are aimed at strong security. Karlof-Wagner mentions the fact that routing protocols suffer from multiple security holes. For example, an associate bachelor may launch a denial-of-service attack on a routing protocol. Attackers may jointly inject malicious routing information into the network, resulting in inconsistencies in the routing. In addition, most of the proposed regional units are currently designed for static wireless sensor networks, but the quality has not yet been taken into consideration and health care applications require quality-supported routing protocols. In addition, planning for secure routing protocols for mobile networks may be an advanced task, and current WMSNs healthcare security requirements can create additional advanced capabilities after they become time-bound applications [11].

2.3.4 Node capture resilience

Resilience captured for nodes is one of the most difficult issues in sensor networks. In real-time healthcare applications, the medical sensor is placed on the patient's body while the environmental sensor is placed inside the hospital (eg, ward, surgery area, etc.) which

can be easily accessed by an attacker. Therefore, attackers may be able to capture sensor nodes, obtain their cryptanalysis information, and thus alter sensor programming. Later, the user can place the compromised node in the network, which may jeopardize the success of the application. Current cryptographic functions, node authentication and identity, may find and defend against attacked nodes, but these attacks are threatened to not detect node attacks immediately, which may be the case for healthcare applications Huge problem For example, consider warnings. One possible solution to preventing such attacks is to use tamper resistant hardware; however, tamper resistant hardware is not an effective solution.

2.3.5 Trust management

Trust means that any two trusted nodes (ie, sensor nodes and aggregator nodes) are sharing their data with each other. Trust is generalized as the degree to which a node should be trusted, safe, or reliable in any interaction with a node. Wireless health care applications rely on distributed collaboration among network nodes. A key aspect of healthcare applications may be trust analysis of node behavior (i.e. data transfer and quality), so trust management system area units help to keep track of node trust.

2.3.6 Secure Localization

WBAN promotes patient comfort mobility so patient location estimation is necessary for the success of healthcare applications. Because medical sensors sense individual physiological information, they should also report the patient's location to a distant server. As a result, medical sensors need to remember the patient's location, which is called positioning.

2.3.7 Strength to Communication DoS (Denial-of-Services)

A criminal tried to disrupt network operations by broadcasting high-energy signals. If the broadcast is strong enough, the entire network communication may be blocked. Different attacks are potential, such as nurse adversaries may delay communication due to violation of media access management protocol. Moreover, the assistant in the care adversary will transmit the packet, while the neighbor node will transmit otherwise [12].

III. RELATED RESEARCH

Below table is defining the summary of the work existed in the field of wireless body area network. In the table, the proposed techniques with the simulator and outcomes have been described.

Table 5 A glance of existing techniques

Authors	Simulator	Proposed techniques	Outcomes
E. Jovanov et al. [2005]	Tiny Operating system	Zigbee- compliant radio interface and microcontroller with ultra low power were used.	Support messaging, wireless communication, Saved energy, Secure and provide privacy within the network.
Jamil Yusuf Khan et al. [2012]	MATLAB	MAC protocol, CSMA/CD architecture Based on Zigbee standard for Sports training activities.	Designed a low cost patient monitoring system .Different parameters like throughput, packet delivery ratio has been determined. It was concluded that the thepaynode size and packet transmission sequence was greatly influenced by the performance of WBAN.
S. H. Cheng and C. Y. Huang [2013]	NS-2	Random incomplete coloring with low time complexity and high spatial reuse for interference degradation.	The throughput of the WBAN for mobile network get increased
Chen, Haifeng et al. [2010]	MATLAB	ZIgbee method was sued to design a WBAn network.	Zigbee was used to transmit the collected information from the sensor nodes to the remote station. Method was used to analyze and monitor the EEG signal through internet.
S. Ivanov et al. [2012]	JAVA	Quality of health monitoring in WBAN.	QoHM will provide the feedback on the data received from the patient.
S. N. Ramli et	MATLAB	A boometric framework was	Proposed framework was mainly used for

al. [2013]		sued forrecognization within the WBAN.	EEG data collection and send that data tot eh remote station.
R. Kazemi et al. [2011]	MATLAB	Genetic algorithm and Fuzzy logic	Fuzzy logic was used to resuce the interference level of the input signal in WBAN.Genetic algorithm was used to optimize the Fuzzy output so that the power consumption was minimized in minimum time interval.
Thamilarasu, and Geethapriya [2016]	MATLAB	Genetic algorithm	The main aim of this paper wa to provide a network with higher security from the extremal attack in the network. Thus, a Genetic algorithm was used to detect the attack and hence decreasing the simulation complexity of the network.
D. B. Jourdan and O. L. de Weck [2004]	NS-2	Multiobjective Genetic algorithm (MOGA)	As the sensors consume more energy when they are in working condition. Thus to reduce their energy consumption GA was used.
C. Yi et al. [2017]	MATLAB	The model of system level energy having the transmission distance with the data rate intended for the WBAN has been presented.	By using optimization algorithm upto 59.77 % or even more energy has been saved as compared to the baseline scheme.
Sapna Singla et al (2016)	MATLAB	Medical and non-therapeutic applications have developed the interest of using WBAN.	Several protocols used for Wireless Body Area Network and its various techniques used in health care application have been discussed.
SavitaSindhu et al (2016)	MATLAB	Wireless network as most trending area of nowadays and it is being increasing gradually. ome of the applications of WBAN are medical and non-medical areas. In the area of medical, health monitoring is beneficial which cares about the health of the patient in real time.	Various aspects of wireless body area network, its implementation techniques and MAC protocols have been explained

IV. CONCLUSION

In this article, we have presented WBAN infrastructure that supports wake-up and master radio to support on-demand, emergency and normal traffic. This infrastructure has given sufficient for unobtrusive health monitoring. We further have provided technical discussions on in vivo antenna designs and patch antennas that support in vivo communication. We also discussed WBAN's low-power MAC protocol. In this survey, we have reviewed the current status of the wireless body area network and address the security issues facing the technology.

REFERENCES

[1] Sindhu, S., Vashiath, S., &Chakarvarti, S. K. (2016). A Review on Wireless Body Area Network (WBAN) for Health Monitoring System, Implementation Protocol. *Communication on Applied Electronics, Foundation of Computer Science, Newyork, USA*, *4*(7).

[2] Singla, S., & Sharma, K. (2016). A Review Paper on Wireless Body Area Network for Health Care Applications.

[3] Sun, F., Yi, C., & Li, Y. (2017). Battery-friendly scheduling policy in MAC layer for WBAN data packets transmission. *IET Communications*, *11*(9), 1423-1430.

[4] Jourdan, D. B., & de Weck, O. L. (2004). Layout optimization for a wireless sensor network using a multi-objective genetic algorithm. In *Vehicular technology conference, 2004. VTC 2004-Spring. 2004 IEEE 59th* (Vol. 5, pp. 2466-2470). IEEE.

[5] Thamilarasu, G. (2016). iDetect: an intelligent intrusion detection system for wireless body area networks. *International Journal of Security and Networks*, *11*(1-2), 82-93.

[6] Kazemi, R., Vesilo, R., &Dutkiewicz, E. (2011, May). A novel genetic-fuzzy power controller with feedback for interference mitigation in wireless body area networks. In *Vehicular Technology Conference (VTC Spring), 2011 IEEE 73rd* (pp. 1-5). IEEE.

[7] Ramli, S. N., Ahmad, R., Abdollah, M. F., &Dutkiewicz, E. (2013, January). A biometric-based security for data authentication in wireless body area network (wban). In *Advanced Communication Technology (ICACT), 2013 15th International Conference on* (pp. 998-1001). IEEE.

[8] Ivanov, S., Foley, C., Balasubramaniam, S., &Botvich, D. (2012). Virtual groups for patient WBAN monitoring in medical environments. *IEEE Transactions on Biomedical Engineering*, *59*(11), 3238-3246.

[9] Chen, H., Wu, W., & Lee, J. (2010). A WBAN-based real-time electroencephalogram monitoring system: design and implementation. *Journal of medical systems*, *34*(3), 303-311.

[10] Cheng, S. H., & Huang, C. Y. (2013). Coloring-based inter-WBAN scheduling for mobile wireless body area networks. *IEEE Transactions on parallel and distributed systems*, *24*(2), 250-259.

[11] Khan, J. Y., Yuce, M. R., Bulger, G., & Harding, B. (2012). Wireless body area network (WBAN) design techniques and performance evaluation. *Journal of medical systems*, *36*(3), 1441-1457.

[12] Jovanov, E., Milenkovic, A., Otto, C., De Groen, P., Johnson, B., Warren, S., &Taibi, G. (2006, January). A WBAN system for ambulatory monitoring of physical activity and health status: applications and challenges. In *Engineering in Medicine and Biology Society, 2005. IEEE-EMBS 2005. 27th Annual International Conference of the* (pp. 3810-3813). IEEE.