An Overview of Wireless Body Area Network (WBAN) using Zigbee Technology

[1]Anupam Jain, [2]Minakshi Halder

[1]M.E. Pursuing, [2]Assistant Professor
Electronics and Communication Engineering (ECE)
Acropolis Institute of Technology and Research, Indore, India

***Abstract*—Wireless Body Area Networks (WBANs) is one of the latest approaches in medical identification, management and also key building block for future intentional networks and Internet. Patient monitoring in a hospital environment is becoming more and more complex with multiple parameters (ECG, EEG, temperature & pressure etc.) to be measured and the need of network that gathered data from many patients for observation at a central monitoring station. Wireless BAN has a capability to process and communicate data of heart beat, respiration, body temperature and blood pressure. Non-invasive sensors can be used to mechanically monitor physiological reading, which can be forward to nearest devices, as cell phone as a gateway. Among different multiplexing approaches like TDMA, FDMA, CDMA, SDMA best one is taken and the work will also involve selection and acquisition of biomedical sensors. The IEEE 802.15.4 (zigbee) is used to provide a low-power, low data rate protocol offering a high reliability. In this paper, we present an overview of wireless body area network (WBANs) & its applications.**

***Keywords*— WBAN, Zigbee, Sensors, Health Monitor, Routing Protocols.**

I. INTRODUCTION

Over the past few years, there is a rapid growth in the wireless body area network (WBAN) for patient monitoring system in information processing and wireless data transmission. WBAN provides low cost wireless sensor network technology that creates a system to monitor patient, remotely using an Internet, and it could be seen as a special-purpose wireless sensor node network that provide the health monitoring to anyone, anytime and anywhere [1].

Figure: 1.1 shows the overall architecture of a WBAN system model for remote patient monitoring environment. In WBAN networks, wireless sensors are placed very close to the body for collection of specific physiological data from it. Those sensors forward data to Zigbee router and then it transfers to a Zigbee coordinator who allows the medical specialist to continuously monitor the patient situation by comparison with an original database of the patient [2].

In patient monitoring system, data transmission is very important and that is why IEEE formed a specialist study group IEEE 802.15.4 (Zigbee), working on the development of body area network [3, 4].

The main function of such devices is to collect patient physiological data and forward to medical center in the efficient way. Therefore, routing is a very important task in WBAN. Nowadays, lots of routing algorithms are available, but it is difficult to select the suitable algorithm for desired network.

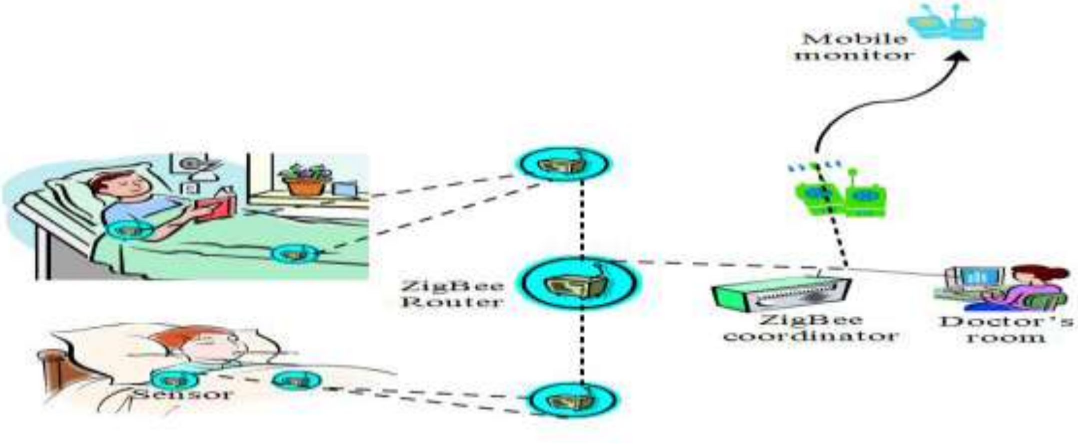


Figure 1.1: Architecture of WBAN

2. CLASSIFICATION OF ROUTING PROTOCOLS FOR WBAN

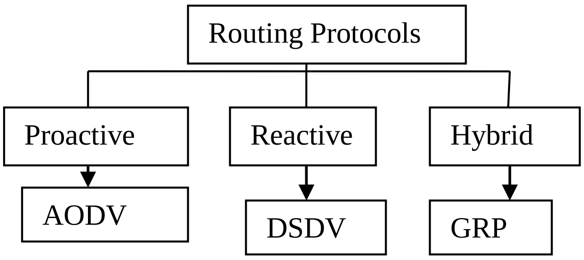


Figure 2.1: Classification of Routing Protocols

A routing protocol specifies how the routers communicate with each other.

Proactive Routing Protocol

This type of routing protocol continuously modifies its routing table by sending request update to neighbor node and share its routing table with all nodes, so the route will available, when any node wants to send a packet of information to a destination node. Here, latency delay is low as the route is established before communication requirement.

AODV (Ad Hoc- on Demand Distance Vector):

The AODV routing protocol is on demand and destination based routing protocol. In AODV, RREQ carries the destination address, this implies that AODV has potentially less routing overhead. In AODV, RREP carries the destination IP address and sequence number, so AODV resolves the problem of potential overhead [5]. When a node wants to send a packet of information to destination node subsequently it broadcasts a RREQ on the network. When the intermediate node receives the RREQ message, it creates a reverse route back to the destination node and then checks for a valid route to the destination in the routing table, if it does not have a valid route, it will broadcast the RREQ message in the network.

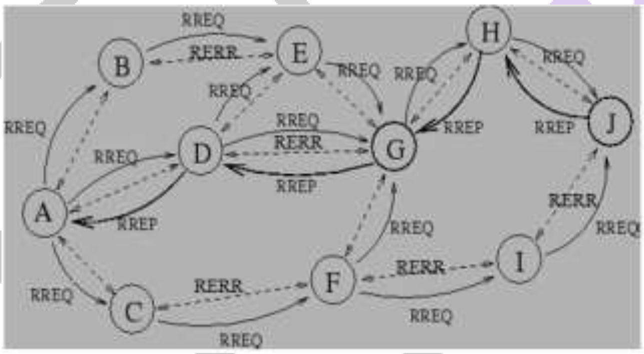


Figure 2.2**:** AODV Routing Protocol

Node lifetime is related to the entry in routing table if a route is not used for a long time, then that route is deleted from routing table .When the destination node receives the RREQ, it generates Route Reply (RREP). If the number of route reply is received at the source, then the route with the shortest hop count is chosen. In this case when the intermediate node fails to forward the packet to next hop or destination due to any reason, it generates the Route Error (RERR) message [5].

When a link breakage in an active route is detected, a RERR message is used to notify other nodes for the loss of the link. In order to enable this reporting mechanism, each node keeps a "precursor list", containing the IP address for each neighbor that are likely to use it as a next hop towards each destination. When the source node receives the RERR, it will again start the route discovery process for destination.

The advantage in AODV routing is that it provides an easy way to get change in link situation, but the node may experience the large delays during route construction and consume more bandwidth as the network size increases [6].

Reactive Routing Protocol

In this type of Routing protocol when any node wants to send a packet of information to a destination node, it will first check whether the route is available in the routing table or not, if the route is available, the source node sends through that route otherwise it sends a request for a route from source node to destination.

Destination Sequenced Distance Vector (DSDV):

DSDV has one routing table, each entry in the table contains: destination address, number of hops towards destination, next hop address. Routing table contains all the destinations that one node can communicate. When a source A communicates with a destination B, it looks up routing table for the entry which contains destination address as B. Next hop address C was taken from that entry. A then sends its packets to C and asks C to forward to B. C and other intermediate nodes will work in a similar way until the packets reach B. DSDV marks each entry by sequence number to distinguish between old and new route for preventing loop.

DSDV use two types of packet to transfer routing information: full dump and incremental packet. The first time two DSDV nodes meet, they exchange all of their available routing information in full dump packet. From that time, they only use incremental packets to notice about change in the routing table to reduce the packet size. Every node in DSDV has to send update routing information periodically. When two routes are discovered, route with larger sequence number will be chosen. If two routes have the same sequence number, route with smaller hop count to destination will be chosen.

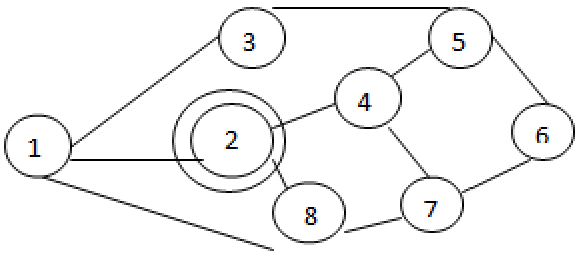


Figure 2.3**:** DSDV Routing Protocol

Advantages

(1) Simple routing table format

(2) Simple routing operation and guarantee loop-freedom.

Disadvantages

Large overhead caused by periodical update. Waste resource for finding all possible routes between each pair, but only one route is used.

Table 1: DSDV Routing Protocol Table for 2 Nodes

Destination	Next Hop	Metric	Dest. Seq. No.
1	1	1	123
2	0	0	516
3	3	1	212
4	4	1	168
5	4	2	372
8	1	INF	432

Hybrid Routing Protocol

This protocol combines reactive and proactive routing protocols along with a location assisted routing protocol.

Geographic routing:

Also-called geo-routing or position-based routing is a routing principle that relies on geographic position information. It is mainly proposed for wireless networks and based on the idea that the source sends a message to the geographic location of the destination instead of using the network address [7]. Geographic routing requires that each node can determine its own location

and that the source is aware of the location of the destination [8]. With this information a message can be routed to the destination without knowledge of the network topology or a prior route discovery.
There are various approaches, such as single-path, multi-path and flooding-based strategies [9]. Most single-path strategies rely on two techniques: greedy forwarding and face routing. Greedy forwarding tries to bring the message closer to the destination in each step using only local information. Thus, each node forwards the message to the neighbor that is most suitable from a local point of view. The most suitable neighbor can be the one who minimizes the distance to the destination in each step (Greedy).
Alternatively, one can consider another notion of progress, namely the projected distance on the source-destination-line (MFR, NFP), or the minimum angle between neighbor and destination (Compass Routing). Not all of these strategies are loop-free, i.e. a message can circulate among nodes in a certain constellation. It is known that the basic greedy strategy and MFR are loop free, while NFP and Compass Routing are not [10].

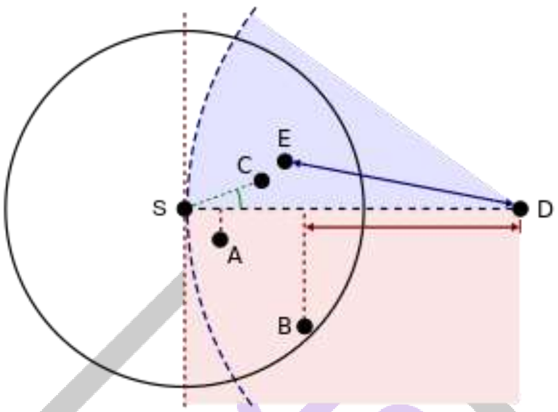


Figure 2.4**:** Geographic Routing Protocol

Greedy forwarding variants: The source node (S) has different choices to find a relay node for further forwarding a message to the destination (D). A = nearest with Forwarding Progress (NFP), B = Most Forwarding progress within Radius.

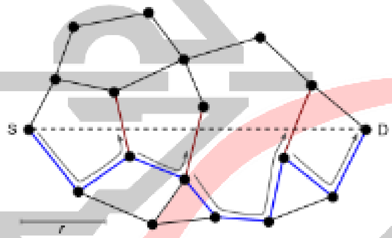


Figure 2.5**:** Geographic Routing Protocol

Face routing: A message is routed along the interior of the faces of the communication graph, with face changes at the edges crossing the S-D-line (red). The final routing path is shown in blue.
Greedy forwarding can lead into a dead end, where there is no neighbor closer to the destination [11]. Then, face routing helps to recover from that situation and find a path to another node, where greedy forwarding can be resumed. A recovery strategy such as face routing is necessary to assure that a message can be delivered to the destination [12]. It guarantees delivery in the so-called unit disk graph network model [13].
Although originally developed as a routing scheme that uses the physical positions of each node, geographic routing algorithms have also been applied to networks in which each node is associated with a point in a virtual space, unrelated to its physical position [14]. The process of finding a set of virtual positions for the nodes of a network such that geographic routing using these positions is guaranteed to succeed is called greedy-embedding.

3. ZIGBEE

Zigbee is a short distance wireless transmission technology that has been rapidly developed in the past years .It is established by the Zigbee Alliance and the IEEE802.15.4 Team along with several companies, and it stresses low costs and low power consumption. The rapid development zigbee has led to the inclusion of functions not restricted to general home networks, and it has also been introduced into industry and medicine. Zigbee with low transmission rate (250 Kbps), short distances (generally 50m-100m), and low power consumption is easily installed and equipped and it supports a large number of network nodes and several network topologies. Moreover it is fast, reliable, and safe with lower costs. The amount of transmission of zigbee is comparatively less as is often used for simple wireless control, including the simple applications for home industries and medicines, toxic gas like (carbon-monoxide) detection, medical sensors and patient emergency alarm calls. It can facilitate medical treatment procedures by transmitting the measured signals any times in comparison with traditional wired equipment. The positioning function of wireless networks can be used to monitor the movements of patients and monitor the human body temperature or pulse anytime.

Among the different wireless technologies, the Zigbee wireless transmission module is often selected for healthcare systems that require frequent measurements and text based data transmission that the low power consumption. Besides, in consideration of the simplicity in operation and user acceptance, Zigbee can be easily installed has lower costs and supports various networks. When a node is out of order, other nodes could be selected as the path for signal transmission to ensure the continuous operation of the entire system, which is critical for the life safety of the elderly. The advantages of Zigbee are further summarized as follows:

(1) Low cost: The simple protocol and small storage account for the low costs of Zigbee, so that it costs merely low.

(2) Low power consumption: Zigbee uses sleep mode when not working, and the startup time is merely 15ms, which is faster than Bluetooth which takes 8 seconds to add a node. Zigbee can rapidly recover and connect when

nodes are required and go into sleep mode again after transmitting data. Such a transformation allows Zigbee to prolong battery life. Various types of batteries could support Zigbee service for periods ranging from six months up to two years.

(3) High reliability: With collision avoidance of talk when ready, a confirmation reply would be sent after receiving each control instruction or transmitted data envelope feature.

Without such reply, the transmission would proceed again to ensure the transmission of physiological information. Zigbee thus presents high reliability information transmission.

(4) High expandability: Zigbee can cover up to 65,536 nodes in the network. Such network nodes would automatically construct a mesh network for rapidly allocating nodes. In other words, each Zigbee node could be connected with many nodes to show the larger capacity.

(5) Support for various network structures: Zigbee supports star, tree and web structures. A web structure could provide higher reliability so that other nodes could be used as a path for transmitting signals when one node is broken.

(6) Security: Zigbee offers three levels of security mode, including non-security setting, utilizing Access control list (ACL) for preventing illegal data acquisition, and applying 128 bit Advanced Encryption Standard (AES) with complete data transmission checking function. Such measures ensure the security of Zigbee and prevent the data from being changed or accessed by attackers.

3.1 Zigbee devices:

(1) Zigbee Coordinator (ZC): The most capable device, the coordinator forms the root of the network tree and might bridge to other networks. There is exactly one Zigbee coordinator in each network since it is the device that started the network originally. It stores information about the network, including acting as the Trust Center & repository for security keys.

(2) Zigbee Router (ZR): As well as running an application function, a router can act as an intermediate router, passing on data from other devices

(3) Zigbee End Device (ZED): Contains just enough functionality to talk to the parent node (Either the coordinator or a router); it cannot relay data from other devices. This relationship allows the node to be asleep a significant amount of the time thereby giving long battery life. A ZED requires the least amount of memory, and therefore can be less expensive to manufacture than a ZR or ZC.

3.2 Applications of Zigbee:

Zigbee protocols are intended for use in embedded applications requiring low data rates and low power consumption. Zigbee's current focus is to define a general-purpose, inexpensive, self-organizing mesh network that can be used for industrial control, embedded sensing, medical data collection, smoke and intruder warning, building automation, home automation, etc.

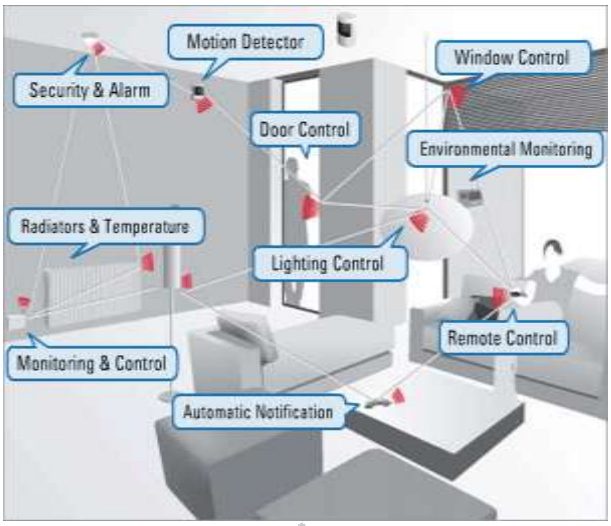
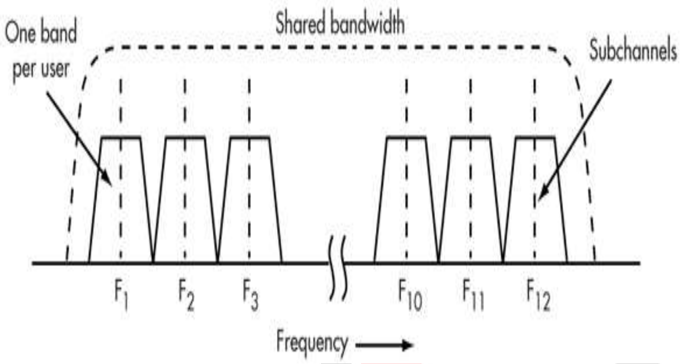


Figure 3.1**:** Zigbee and its applications

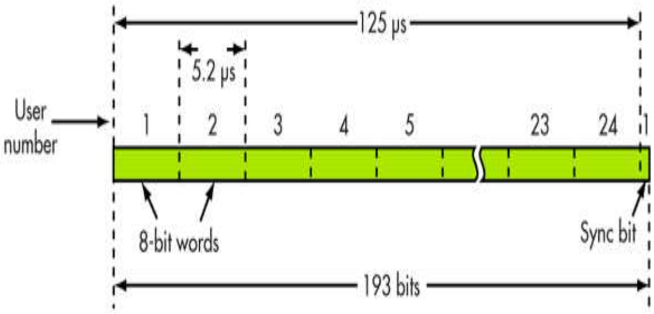
Frequency Division Multiple Access (FDMA)

The frequency-division multiple access (FDMA) channel-access scheme is based on the frequency-division multiplexing (FDM) scheme, which provides different frequency bands to different data-streams. In the FDMA, the data streams are allocated to different nodes or devices. Each message signal (each phone call) is modulated on a specific carrier frequency.



Time division multiple access (TDMA)

The time division multiple access (TDMA) channel access scheme is based on the time-division multiplexing (TDM) scheme, which provides different time-slots to different data-streams in a cyclically repetitive frame structure. An advanced form is Dynamic TDMA (DTDMA), where a scheduling may give different time slots but some time node 1 may use time slot 1 in first frame and use another time slot in next frame.

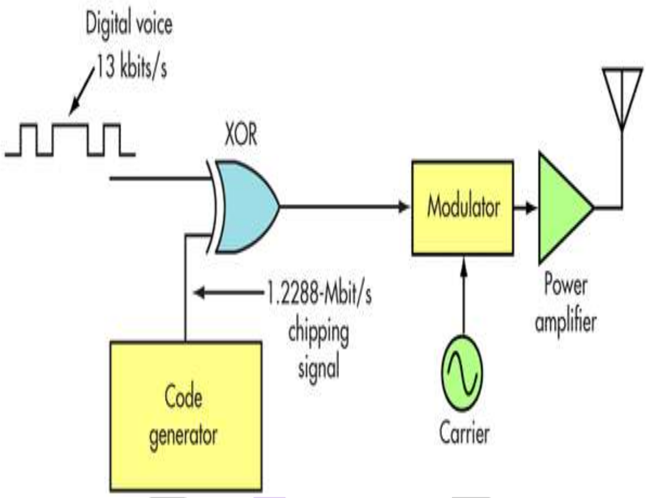


Statistical time division multiplexing multiple-access is typically also based on time-domain multiplexing, but not in a cyclically repetitive frame structure. Due to its random character it can be categorized as statistical multiplexing methods, making it possible to provide dynamic bandwidth allocation. This requires a media access control (MAC) protocol, i.e. a principle for the nodes to take turns on the channel and to avoid collisions.

Code division multiple access (CDMA)/Spread spectrum multiple access (SSMA)

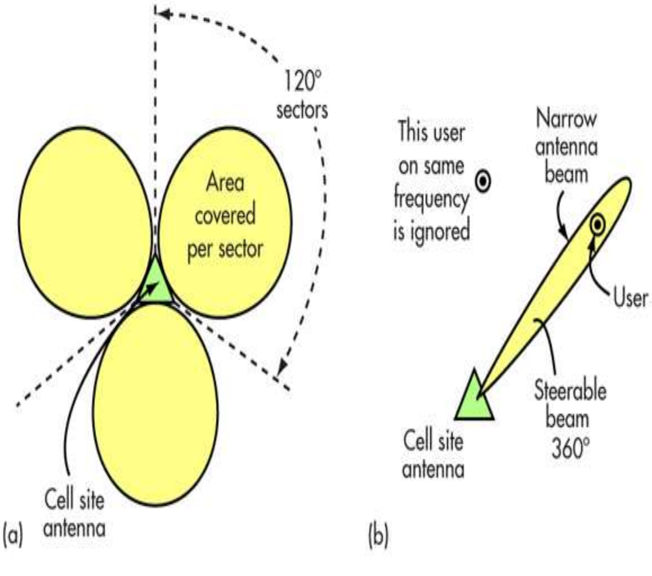
The code division multiple access (CDMA) scheme is based on spread spectrum, meaning that a wider radio spectrum in Hertz is used than the data rate of each of the transferred bit streams, and several message signals are transferred simultaneously over the same carrier frequency, utilizing different spreading codes. The wide bandwidth makes it possible to send with a very poor signal-

to-noise ratio of much less than 1 (less than 0 dB) , meaning that the transmission power can be reduced to a level below the level of the noise and co-channel interference (cross talk) from other message signals sharing the same frequency.
One form is direct sequence spread spectrum (DS-CDMA). Each information bit (or each symbol) is represented by a long code sequence of several pulses, called chips. The sequence is the spreading code, and each message signal (for example each phone call) use different spreading code.



Another form is frequency-hopping (FH-CDMA), where the channel frequency is changing very rapidly according to a sequence that constitutes the spreading code. As an example, the Bluetooth communication system is based on a combination of frequency-hopping and either CSMA/CA statistical time division multiplexing communication (for data communication applications) or TDMA (for audio transmission). All nodes belonging to the same user (to the same virtual private area network) use the same frequency hopping sequence synchronously, meaning that they send on the same frequency channel, but CDMA/CA or TDMA is used to avoid collisions within the VPAN. Frequency-hopping is used to reduce the cross-talk and collision probability between nodes in different VPAN's.

Space division multiple access (SDMA)
Space-division multiple access (SDMA) transmits different information in different physical areas. Examples include simple cellular radio systems and more advanced cellular systems which use directional antennas and power modulation to refine spatial transmission patterns.



A sensor is a device that measures a physical quantity and converts it into a 'signal' which can be read by an observer or by an instrument.
EEG:-These are bio potential generate neural activity of the brain known as electroencephalogram. EEG signal repeated application of stimulus, awake, sleep is evoked response.

ECG:-Electrocardiography (ECG) is the process of displaying the electrical activity of the heart over a period of time using electrodes placed on a human body. These electrodes detect the electrical changes on the membrane that arise from heart muscle depolarizing during heartbeat.
EMG:-Electromyography is an electro diagnostic medicine technique for estimating and footage the electrical activity produced by skeletal muscles. Electromyography is performed using an instrument called an electromyograph, produce record called as electromyogram.

A pressure sensor is a device which senses pressure and converts it into an analog electric signal whose magnitude depends upon the pressure applied. Since they convert pressure into an electrical signal, they are also termed as pressure transducers.

Limitations of WBAN using zigbee:

1. Scalability: As large as human body parts.(mm/cm)
2. Node number: Few or more perfect sensor node essential.
3. Node size: Invasive monitoring and they require for minimization.
4. Event recognition: Early adverse events detection fundamental human tissue failure irrevocable.
5. Data defense: High level wireless data transfer security necessary to protect patient's information.
6. Contact: Implantable sensor substitute difficult and requires biodegrability.
7. Bio Compatibility: A must for implantable and some external sensors, likely to increase cost.
8. Context consciousness: Very important because body composition is very sensitive to context change.
9. Wireless tools: low power wireless required, with signal detection more demanding.

CONCLUSION:

BAN is a network which support all environmental conditions whether hospital, communication network etc. In WBAN, patient doesn't need to stay longer time at hospital. All the important medical information's will be transferred to doctor with the help of zigbee devices. Routing Protocols plays an important role in transferring information from patient to doctor. Three Routing Protocols i.e. AODV, DSDV and GRP are used using zigbee technology.
In this paper we gave overview of wban, challenges and applications with open research issues that gives necessary information for future research directions.

FUTURE WORK: Some of the future applications of wban includes patient home care, a pre hospital mobile data base for emergency medical services, security system and other different types of real time routing protocols.

REFERENCES:

[1]. Jami Y. Khan, Mehmet R. Yuce and Farbood Karami, "Performance evaluation of wireless body area sensor network for remote patient monitoring" 30th annual international IEEE EMBS conference Vancouver, British Columbia, Canada, August 2008.
[2]. Muhannad Quwaider and SuberBiswas,"On body packet routing algorithms for body sensor networks" first international conference on network and communication, 2009.
[3]. Ting, Kok Seng, et al. "The performance evaluation of IEEE 802.11 against IEEE 802.15. 4 with low transmission power"Communications(APCC),17thAsia-Pacific Conference on. IEEE, 2011.
[4]. N. F. Timmons and W. G. Scanlon, "Improving the ultra-low power performance of IEE 802.15.6 by adaptive synchronisation" publisher in IET wireless sensor systems doi: 10.1049/iet-wss-2011.0036
[5]. Qutaiba Razoui, Ahmed Boushehri, Mohamed Goballah, and Lina Alsaleh, "Extensive simulation performance analysis for DSDV, DSR and AODV MANET routing protocols"27th international conference on advanced information networking and application workshops, 2013.
[6]. Zahian Ismail and Rosilah Hassan,"Effect of packet size on AODV routing protocol implementation in homogeneous MANET" Third international conference on computational intelligence, modelling and simulation, 2011.
[7]. Takagi, H.; kleinrock, L. (March 1984). "Optimal transmission ranges for randomly distributed packet radio terminals". IEEE Transactions on Communications 32 (3): 246–257.
[8]. Finn, Gregory G. (March 1987). "Routing & Addressing Problems in Large Metropolitan-Scale Internetworks" (PDF) University of Southern California, ISI/RR-87-180.
[9]. Stojmenovic, Ivan (2002). "Position based routing in ad hoc networks". IEEE Communications Magazine 40 (7): 128–134.
[10]. Stojmenovic, Ivan; Lin, Xu (2001)."Loop free hybrid single-path/flooding routing algorithms with guaranteed delivery for wireless networks."IEEE Transactions on Parallel and Distributed Systems 12 (10): 1023–1032.
[11]. Bose, P. Morin, P. Stojmenovic, I. Urrutia, J. (1999). "Routing with guaranteed delivery in ad hoc wireless networks". Proc. of the 3rd international workshop on discrete algorithms and methods for mobile computing and communications (DIALM '99).
[12]. Djenouri, Djamel; Balasingham, Ilangko (2011). "Traffic-Differentiation-Based Modular QoS Localized Routing for Wireless Sensor Networks". IEEE Transactions on Mobile Computing 10 (06): 797–809.
[13]. Ruehrup, Stefan (2009). "Theory and Practice of Geographic Routing". In Liu, Chu, Leung. Ad Hoc and Sensor Wireless Networks: Architectures, Algorithms and Protocols. Bentham Science.
[14]. Rao, Ananth; Ratnasamy, Sylvia; papadimitriou, christos h.; shenker, scott; stoica, ion (2003), "Geographic routing without location information", Proc. 9th ACM Mobile Computing and Networking (MobiCom).