JOURNAL OF CURRENT RESEARCH IN SCIENCE
ISSN 2322-5009
CODEN (USA): JCRSDJ
Available at www.jcrs010.com

JCRS
4 (1), 2016: 7-16

The Zigbee Wireless Sensor Netwrok In Medical Applications: A Critical Analysis Study

Bader A Alyoubi[1], Ibrahiem M. M. El Emary [2]

1. Management Information Systems, College of Business, Jeddah University, Jeddah, Saudi Arabia
2. Information Science Department, King Abdulaziz University, Jeddah, Saudi Arabia

Received 8 September, 2015 **Accepted** 14 November, 2015 **Published** 20 February, 2016

K E Y W O R D S: IEEE 802.11b/g, IEEE 802.15.4, MEMS, Zigbee, Wireless Sensor Networks, Healthcare

ABSTRACT: Wireless sensor network is gaining popularity and its applications are being deployed in many sectors such as industrial, construction, healthcare etc. Zigbee standard provides the low cost, low rate data transmission wirelessly. The applications developed using Zigbee technology can transfer data to other devices within the network wirelessly. Zigbee based applications are being implemented in the healthcare sector and examples of such applications are wireless patient monitoring and wireless fitness monitoring. These applications use medical sensors to capture the vital indicators such as heart rate, blood sugar level, temperature etc. These data are securely transmitted to other devices; so that medical professionals can monitor the patient's health remotely and take further course of action. The main objective of this paper is to examine in detail the main characteristics, features and architecture of Zigbee standards; then the impact of interference on Zigbee applications were evaluated and finally concluded with analysing the impact of Zigbee WSN applications in the medical field.

Introduction

Wireless Sensor Networks (WSN) technology and the applications based on WSN are becoming popular among various sectors such as industrial, medical, telecom etc. Advancement in Micro Electrical Mechanical Systems (MEMS) has aided smart sensors development and hence WSN has grabbed the attention in the last few years (Srivastava, 2010). There are many applications based on WSN technology that are being used for industrial, construction, consumer electronics, healthcare, telecommunication, energy management purposes etc. Actually WSN is a collection of tiny sensors that act as nodes. These nodes have the ability to gather the information specifically configured to identify specific incidents and transmit that data using wireless technology. WSN produces an ad-hoc network and these needs minimal or no infrastructure set up. WSN comprises of broad range of technologies such as systems software, computer hardware, programming and networking technologies (Sharma, Chaba, and Singh, 2010). Zigbee is an IEEE standard set out for WSNs based on IEEE 802.15.4. Zigbee is a technological specification for high level communication protocols featuring low power and low cost Wireless personal Area Network (WPAN). Zigbee applications include wireless patient monitoring system, wireless fitness monitoring system, wireless electrical meter, wireless light control system etc. These applications require transfer of data wirelessly within a short range and with low rates (Khanna, Singh, and Kaushik, 2011).

WSN applications are being considered and implemented for various healthcare processes in order to improve the efficiency of healthcare service; where WSN applications used in medical purposes are considered highly sensitive as data of patients are being transmitted to a remote location where doctors can monitor the patients remotely. It is very vital that data related to patients' health condition is recorded and transmitted accurately without any loss of data during transmission. Patient monitoring primarily includes continuous observation of specific events that will be used by doctors to take next course of action (Ramasamy, 2012).

As WSN applications are becoming popular in medical field, this paper focuses on evaluating the WSN applications used in the medical field. A step by step approach is adopted to evaluate the WSN, WSN applications and the impact of WSN technology in the field of healthcare. The first step in the evaluation is to examine Zigbee in more detail which comprises of Zigbee characteristics, network topology, network components etc. The next step is to evaluate the working environment of Zigbee WSN applications used for medical purposes and study the interference effect caused by widely used wireless protocol Wireless LAN IEEE 802.11 spectrum. The last step comprises of evaluating the impact of WSN applications in the medical field.

Literature Review

WSN applications require network infrastructure that have standards-based protocols. Zigbee and IEEE 802.15.4 are the protocols that WSN applications use. The MAC and physical layers are defined by 802.15.4. The network and application layers are defined by Zigbee. Achieving long battery life, low cost and mesh networking are the core design requirements of WSN applications that can communicate with many devices in an interoperable environment. Zigbee WSN applications are being used in various fields and are illustrated in Fig.1 below (Daintree, 2010).

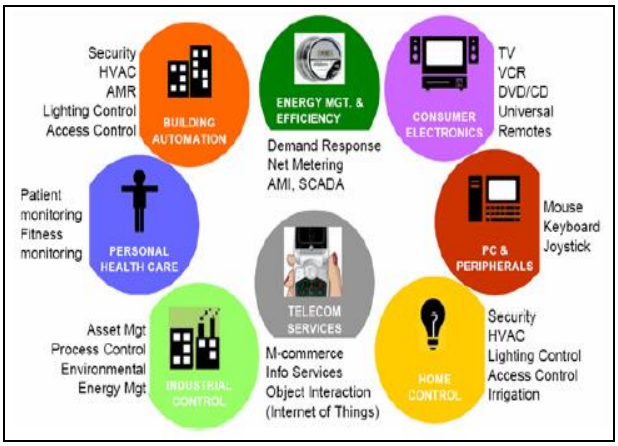

Figure1. Zigbee Wireless Sensor Network Various Applications

The Architecture of Protocol Stack of Zigbee and IEEE 802.15.4

In Fig.2 the structure of protocol stack of Zigbee and IEEE 802.15.4 was illustrated (Daintree, 2010). From this Fig; it is shown that each layer of the architecture provides a defined set of services to the layer above it through service access point (SAP). Below, a description of each layer of this structure is given as follows:-

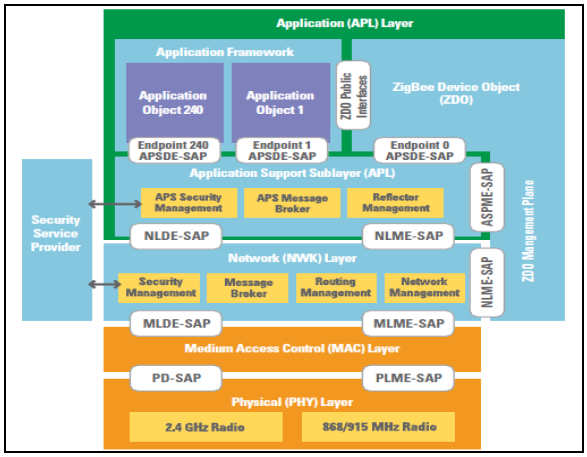

Figure 2. Zigbee Protocol Stack (Zigbee health)

Application Framework ensures that profiles are generated in a consistent manner by setting out the guidelines for building a profile on to the Zigbee stack. It specifies the range of data types that can be used for transmission of data, value pair construct, descriptors etc. to quickly develop profiles that are attribute-based. Application Objects supports endpoint numbered up to 240 with 0 reserved for Zigbee Device Object (ZDO) and each Zigbee node supports up to 240 application objects (IEEE 802.15.4 Specification, 2003).

Zigbee Device Object is responsible for establishing a secure connection between network devices. It initiates the binding, responds to discovery requests and defines the role of each device within the network. It provides the management commands defined in the Zigbee Device Profile.

ZDO Manage Plane aids the communication between Application Support and Network layers with the ZDO. It allows the ZDO to handle the network access and security requests from applications using Zigbee Device Profile (Lee 2006).

Application Support (APS) Sub layer is responsible for maintaining binding links, storing binding table and provide data service to device and Zigbee device profiles.

Security Service Provider (SSP), it provides security mechanisms for NWK and APS layers that uses encryption. The security mechanisms are initialised and configured through ZDO.

Network (NWK) Layer manages the network addresses and devices. It is also responsible for message routing, applying security, identifying and implementing route discovery. It communicates with MAC layer for routing.

Access Control (MAC) Layer facilitates the communications between nodes and helps in improving efficiency by preventing collisions. It is also responsible for managing data packets and frames.

Physical (PHY) Layer consists of two layers operating in different frequency ranges. The lower frequency layer takes care of both European band that use 868MHz and 915MHz that is used in USA and Australia. The higher frequency layer that operates at 2.4GHz is used across the globe (Chen et al., 2012).

The Zigbee Network Structure and Topologies

The structure of Zigbee comprises of three device types namely Coordinators, Routers and End Devices as shown in Fig.3 below. It can be observed that a Zigbee network can be a mixed mesh network and star network topology. Each of the devices has specific roles in the network.

Coordinators initialise and manage the network acting as the trust centre of the network. They act as repository for security keys and information about the network is stored in the coordinators.

Routers are the devices used to expand the network coverage area, identify network routes and store the information for backup during network congestion. Routers are able to connect to other routers, coordinators and can also maintain child devices.

End Devices are capable of transmitting and receiving messages but are not capable performing some operation such as routing, managing child devices etc. They are connected to either a router or the coordinator (Bijalwan and Singh, 2012).

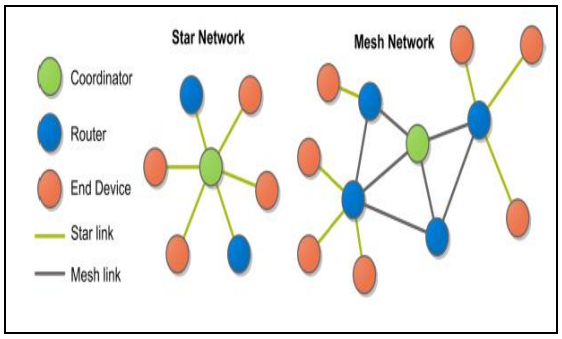

Figure 3. Zigbee Network Topologies (zigbee2)

Mesh Network Topology

Also referred as peer-to-peer network comprises of interconnected routers and end devices resembling a mesh. Each router in the mesh network is generally connected through two pathways or more which can transmit messages to its neighbours. As shown in Fig.3 above, there will be a single coordinator, multiple routers and multiple end devices in a mesh network. This topology is considered very robust and reliable (Stalling, 2004).

Star Network Topology

Comprises of single coordinator and multiple end devices as shown in Fig.3 above. The end devices act as nodes and can communicate only with the coordinator. This network topology is not supported by Zigbee, however, it is supported by IEEE 802.15.4 (Shuaib, 2007).

Zigbee Network Connection with Devices

Devices can join Zigbee network either through MAC association or NWK rejoin. MAC association is the default way to join and it is mandatory that every Zigbee device supports it as it is mandated by and implemented in the MAC layer. Zigbee router and coordinator wishing to allow other devices to join issue NLME_PERMIT_JOIINING request. After the joining device has identified the network to join makes a request by issuing NLME_JOIN request and the rejoin flag setting the rejoin flag to FALSE. The last request triggers the MAC protocol and the joining device receives the response from the

receiving device with a unique address for the device. This unique address is used while the joining device is associated with that particular network. The sequence is shown in Fig.4 below (Yang, 2009).

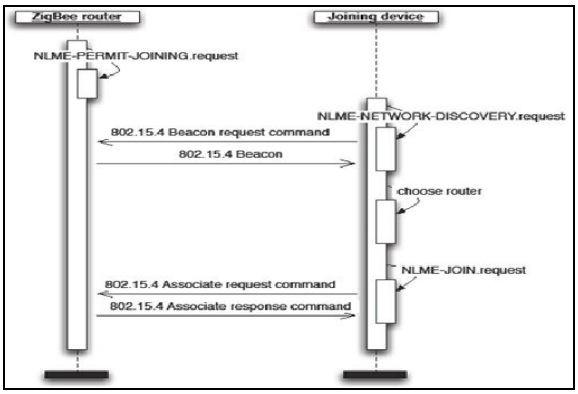

Figure 4. Joining to Zigbee Network through MAC association

In Fig.5, NWK rejoin may be used to join the Zigbee network for the first time. This type of joining is not subjected to MAC's mechanism of issuing the permission to join. The joining mechanism in NWK rejoin can be secured if the joining device has the NWK key if it is actually rejoining the network. The process involved in joining to Zigbee network through NWK rejoin is illustrated in Fig.5 below.

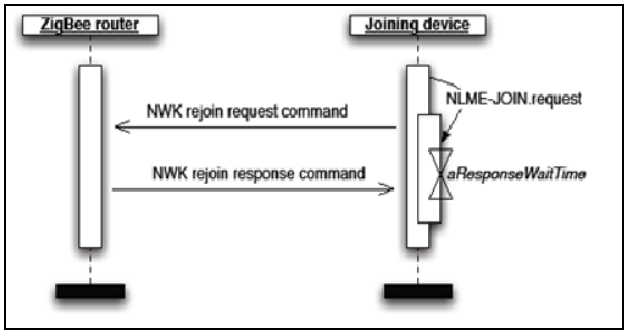

Figure 5. Joining to Zigbee Network through NWK Rejoin

The Zigbee Security Modes

Zigbee security is based on a security algorithm called 128-bit AES algorithm on top of the IEEE 802.15.4 security model. Application Profiles provide the security for applications and Zigbee specifies the security for MAC, NWK and APS layers. Three types of security keys are used in Zigbee and they are: Master Keys, Network Keys and Link Keys. Table 1 below shows the available security levels to NWK and APS layers (Pathan, Lee, and Seon, 2006).

Table 1. Available Security levels for NWK and APS layers

Security Level Identifier	Security Attributes	Data Encryption	Frame Integrity (length of MIC)
0x00	None	OFF	NO (M=0)
0x01	MIC-32	OFF	YES (M=4)
0x02	MIC-64	OFF	YES (M=8)
0x03	MIC-128	OFF	YES (M=16)
0x04	ENC	ON	NO (M=0)
0x05	ENC-MIC-32	ON	YES (M= 4)
0x06	ENC-MIC-64	ON	YES (M=8)
0x07	ENC-MIC-128	ON	YES (M=16)

Standard Security mode, in this case the devices list, all security keys can be managed by individual devices or by Trust Centre.

High Security mode, in this case the devices list, all security keys are managed by Trust Centre along with regular network key updates and managing policies on network admittance.

The Zigbee Commissioning Process

The device includes physical deployment, addressing and binding of several nodes to build a functional network. Commissioning the device is done by the installers and Fig.8 below shows the typical commissioning scenario. Commissioning tools are normally run on laptop or PDA and provides a user interface that is intuitive in nature hiding the complexity of the technology underlying.

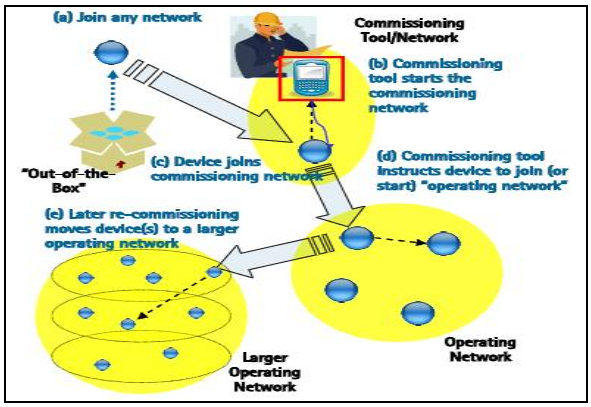

Figure 8. Commissioning Example of the Zigbee

Problem Statement

As we mentioned previously, this research work is intended to examine the characteristics, features and architecture of Zigbee standards; then evaluating the impact of interference on Zigbee applications, we should investigate the factors that affect the performance of Zigbee as well as examining the performance of Zigbee based on changing some network parameters.

Zigbee devices are used in many sectors including medical field. Hence it is necessary to examine the performance of Zigbee WSN which has to coexist with other wireless technologies mentioned above and sustain interference. The main factors that drive the performance of Zigbee WSN are power and timing. In order to transfer reliability, Zigbee uses dynamic device addressing and full handshake protocol. The duty cycle of Zigbee is <0.1% which is extremely low.

Both Zigbee and IEEE 802.11b uses CSMA/CA for media access control and Zigbee uses DSSS and listen before send mechanism to mitigate interference. A random backoff delay in [0, W] is generated which is known as contention window during idle mode for DIFS time interval. W is the size of the contention window which is initially set. The node transmits the data packet when the backoff counter reaches zero. The destination node waits for a short inter frame spacing (SIFS) after receiving the data packet and then transmits ACK signal to the sender.

Table 2. System and other parameters of IEEE 802.11b and IEEE 802.15.4

Parameters	IEEE 802.11b	IEEE 802.15.4
Transmit Power	20dBm	0dBm
Receiver Sensitivity	-76dBm	-85Dbm
Transmit Rate		
Bandwidth	11 Mbps	250 Kbps
Back off unit T_{bs}	20 µs	320 µs
SIFS	10 µs	192 µs
DIFS	50 µs	N/A
CCA	N/A	128 µs
CW_{min}	31	7
Center Frequency	2412 MHz	2410 MHz
Payload Size	1024 bytes	1 byte

Table 2 (Kang, 2007) shows the different parameter values such as receiver sensitivity, payload size, transmit power etc. In IEEE 802.15.4 channel is sensed only during clear channel assessment (CCA) period and not during backoff period. The contention window is doubled in IEEE 802.15.4 when the channel is busy during CCA. The contention window in IEEE 802.11b is same when the channel is busy but gets doubled when ACK is not received from the destination node. Fig.9 below shows the IEEE 802.11b and IEEE 802.15.4 spectrum.

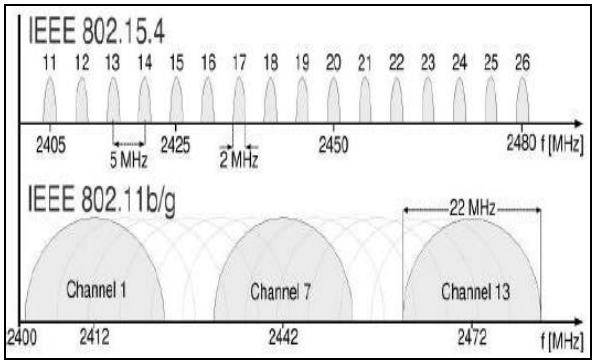

Figure 9. IEEE 802.11b and IEEE 802.15.4 spectrum usage

The transmission power of both 802.11b and 802.15.4 are different. This difference in transmit power and receiver sensitivity leads to different ranges R1, R2 and R3. They quantified these ranges as:

R1:Both 802.11b and 802.15.4 nodes were able to sense each other in this range.

R2: In this range; 802.15.4 was able to sense 802.11b but not vice versa.

R3: In this range; both nodes were not able to sense each other but IEEE 802.15.4 node still suffers interference.

The path loss follows free space propagation up to 8m and then eases rapidly with 3.3 coefficients which are considered a value of 4 in accordance with 32m indoor transmission distance of IEEE 802.15.4 nodes. The path loss is calculated according to the following steps:-:

$PL(d) = 20\ log_{10(4\pi d/\lambda)}$ $\quad if\ d \leq do$

$20\ log_{10(4\pi do/\lambda)} + 40\ log_{10(d/do)}$ $\quad if\ d > do$

D = distance between transmitter and receiver

Do = length of line of sight which is 8m

It is evident from the experiment that interference is caused to Zigbee WSN and using adaptive interface-aware multi-channel clustering algorithm helps avoiding interference. This algorithm comprises of two procedures namely interference detection procedure and interference avoidance procedure. The flow chart of the interference detection procedure is shown in Fig.11 (Kang, 2007).

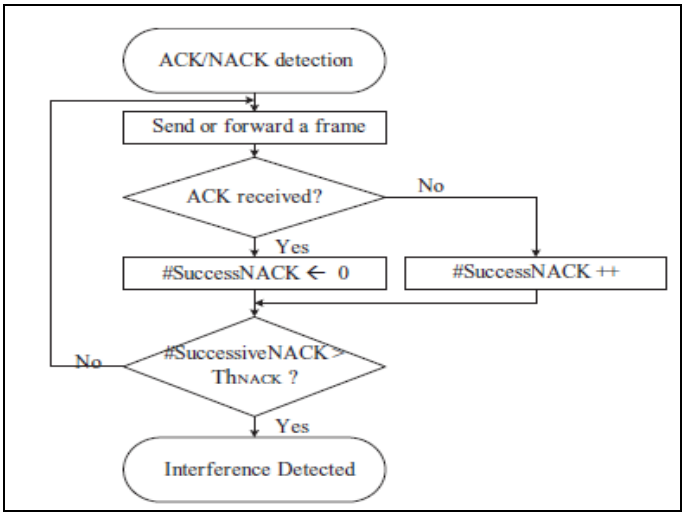

Figure 10. Interference detection procedure

Interference detection can be done using energy detection scan which uses Received Signal Strength Indicator (RSSI) value obtained from IEEE 802.15.4 PHY. Since ACK/NACK based interference detection scheme does not need redundant procedures for interference detection, it is more suitable for cluster tree networks. Once the detection is identified by the device, it starts to change its channel using pseudorandom-based interference avoidance scheme.

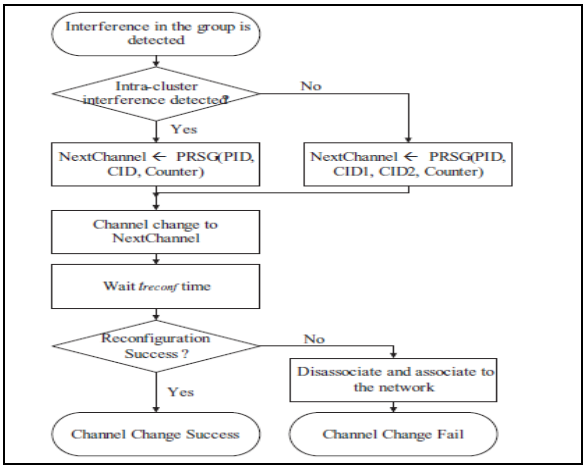

Figure 11. Interference Avoidance scheme flow chart

Each device in the network will have the same channel sequence, so that all devices can move to the same channel after avoiding interference. However there is no need for the devices to share the next channel information. All the Zigbee devices in a group have unique identification key which is a combination of their PAN identification (PID) and cluster identification (CID). With this unique key, all the devices in the group can get their shared next channel sequence generated from the pseudorandom sequence generator.

Major Applications Of The Zigbee Health Monitoring

Health monitoring systems are getting a lot of attention currently and have become an important research area. The applications make use of WSN to transmit critical data such as body temperature, sugar level, heartbeat rate, blood pressure etc. Zigbee has been the technology that caters to the need of low cost, low power and short range data transmission within the network that have large number of devices. Zigbee uses 2.4GHz frequency band that is available globally and is licence-free. Zigbee Alliance has been the pioneer in developing robust WSN healthcare systems (Ramsamy 2012). A typical block diagram of wireless patient monitoring system's data transmission through Zigbee can be seen in Fig.12.

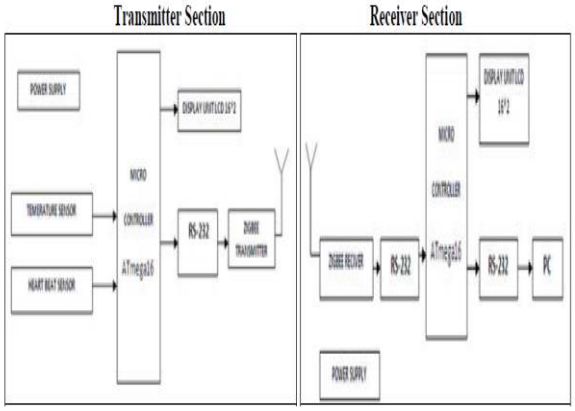

Figure 12. Wireless Patient Monitoring System's Block Diagram

Some of the major WSN healthcare systems developed using Zigbee are Chronic Disease Monitoring system, Personal Wellness Monitoring system, Personal Fitness monitoring system.

Chronic Disease Monitoring system can be used to monitor specific indicators remotely. Episodic patient monitoring system can be used to monitor specific indicators such as heart rate, body temperature etc. of non-critical patients. Some of the disease related indicators such as blood pressure, blood sugar level; EKG etc. can be monitored periodically to identify any anomalies. All the data pertaining to patient gathered by the medical sensors are time-stamped and forwarded to patient monitoring system securely. Fig.13 shows the chronic disease monitoring devices that can be used to monitor the patients' health.

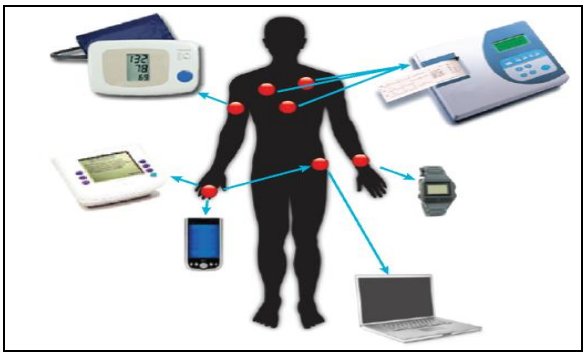

Figure 13. Chronic disease monitoring devices (Zigbee health)

Personal Wellness Monitoring system can be used to monitor and manage the safety, care and activity of the people in an assisted living facility. Senior Activity Monitoring scenario involves not just the medical sensors used to monitor body's vital signs but also uses non-medical sensors like motion sensors, smoke sensors, environmental sensors etc. The data captured is sent for recording and processing. Fig.14 shows the typical setup of monitoring devices for people in assisted living facility

Figure 14. Monitoring devices in assisted living facility

Zigbee applications can also be used in safety monitoring scenarios such as in a home environment to monitor safety hazards including water toxic gases and fire. The vital indicators of the body can also be recorded and the data can be transmitted to the server for processing and monitoring.

Personal Fitness Monitoring system can be used in home and health fitness centres. This monitoring system can track the fitness level of individuals. The medical sensors can be used to monitor various parameters such as heart rate, blood oxygen level and temperature while running on a treadmill. The information gathered by the medical sensors is securely updated in the server's database that can be displayed to the individual in real time.

(Jain, Gupta and Malviya, 2014) developed a Zigbee technology based wearable medical sensor that captures physiological parameters like heart rate and temperature of a human body. Fig.15 shows the high intensity LED and photodiode that senses the heartbeat. Illuminating the light from an LED using photodiode on the fingertip detects the change in volume caused by the pressure.

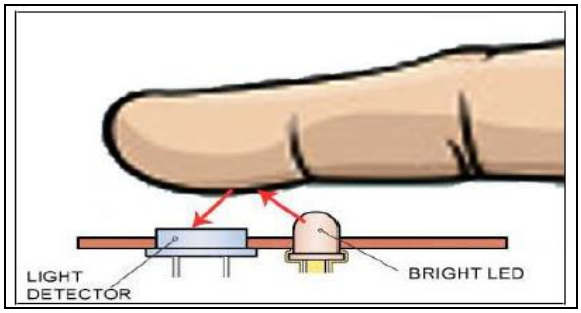

Figure 15. Heart Rate Measurement

Technological advancements in the area of telecommunication and information systems are creating an environment for the innovators to come up with new healthcare devices. Increased acceptance of communication and connectivity technologies has enabled remote health and wellness products to serve for a much wider community.

Conclusion

Zigbee IEEE 802.15.4 technology has been widely deployed in various sectors. It has to coexist with other systems like Bluetooth and WLAN. As the Zigbee network coverage is large, it is expected to experience interference from WLAN. However, using adaptive interference-aware multi-channel cluster algorithm, the interference can be detected and avoided. This paper started with examining the features, characteristics and architecture of Zigbee technology. Then Zigbee technology was evaluated for the coexistence with widely used technology IEEE 802.11b. It was clear that WLAN causes interference to Zigbee. As this paper primarily focussed on Zigbee applications in medical field, it was relevant to understand the impact of interference on Zigbee applications. Zigbee healthcare products are mainly used to record critical data of patients and transmit that data to another device, so that medical professionals can monitor the patients remotely and decide on next course of action. Timely arrival and accuracy of data is critical especially in the healthcare products as medical professionals will be relying heavily on the data they receive about their patients. If the data is lost during transmission, it may have a huge impact on critically ill patients who need continuous monitoring of their vital indicators. From the above paragraphs, it can be inferred that Zigbee applications can solve many healthcare problems by preserving mobility.

References

Al-Sakib K Pathan, Hyung-Woo L, Choong S. 2006. “Security in Wireless sensor Networks: Issues and Challenges”. ICACT

Balambigai SA. Ramasamy. 2012. “Efficient Zigbee Based Health Care System for Arrhythmia Detection in Electrocardiogram”. EJSR. 69 (2):180-187

Daintree. 2010. “Getting Started with ZigBee and IEEE 802.15.4”. Sep 17. http://www.daintree.net/wp-content/uploads/2014/07/zigbee_primer.pdf

Guang Y. 2009. “Zigbee network performance under WLAN 802.11b/g interference”. IEEE conference on Wireless pervasive computing. 11 (13).

IEEE 802.15.4 Specification. 2003. “Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (LR-WPANs)”.

Khaled Sh. 2007. “performance Evaluation of IEEE 802.15.4 Experimental and Simulation results”. Journal of communication. 2 (4).

Lee JS. 2006. “Performance evaluation of IEEE 802.15.4 for low-rate wireless personal area networks”. IEEE Trans Consumer Electron. 52 (3).

Meenu B, Vishwanath B, Banit N. 2010. “Zigbee & IEEE 802.11b(WLAN)coexistence in ubiquitous network environment”. Sep 16. http://arxiv.org/abs/1407.0462

Min S. Kang. 2007. “Adaptive Interference-Aware Multi-Channel Clustering Algorithm in a zigbee Network in the Presence of WLAN Interference”. IEEE conference on wireless pervasive computing. 5 (7).

Neelam S. 2010. “Challenges of Next-Generation Wireless Sensor Networks and its impact on Society” Journal of Telecommunications. 1 (1).

Ritu Sh, Yogesh Ch, Singh Y. 2010. “Ánalysis of Security Protocols in Wireless Sensor Network” International Journal Advanced Networking and Applications. 2 (3): 707- 713.

Satvika Kh, Priyanka S, Akhil K. 2011. “Wireless Sensor Network: Issues & Challenges”. IJMA 2 (11).

Shyr-Kuen Ch, Tsair k, Chai- Tai Ch, Chih-Ning H, Chih-Yen Ch, Chin-Yu L. 2012. “A Reliable Transmission Protocol for ZigBee Based Wireless Patient Monitoring”. IEEE Trans Information Technology Biomed. 16 (1).

Soo Y.Sin. 2007. “Packet error rate analysis of zigbee under WLAN and Bluetooth interferences”. IEEE transaction on wireless communication. 6 (8).

Surbhit J, Anshu G, Praveen K.Malviya. 2014. “A Zigbee Based Wireless Patient’s Monitoring System”. The International Journal of Science and Technoledge. 2 (4).

Vishwanath B, Sanjay S. 2013. “Analysis and Design of Joint PHY-MAC Model of IEEE 802.15.4” IJSETR. 2 (9).

Wei Y. 2007. “A Coexistence model of IEEE 802.15.4 and IEEE 802.11b/g”. 14th symposium on communication and vehicular technology in Benelux.

William S. 2004. “Wireless Communication and Networks”. Pearson Publication Limited