A NOVEL APPROACH TO BLUETOOTH AND ZIGBEE WITH WBANS

S. M. Ghatole[1], P. B. Dahikar[2]
[1]Department of Electronics, Shivaji Science College, Nagpur (MS) India.
[2]Department of Electronics, Kamala Nehru College, Nagpur (MS) India.
smghatole@gmail.com

Abstract
Wireless technologies find its wide application in domestic and industrial sectors. Healthcare is one of the fastest emerging fields today. ZigBee is simple and inexpensive than other short range Wireless Personal Area Network while Bluetooth working with low data transfer rate, both operated on radio frequency. It assures reliability and security in data transfer. It is low-cost, low-power, secured communication wireless mesh networking standard and based on an IEEE 802 standards for networks. In this paper, we present an analysis and general evaluation of radio communication technologies, namely ZigBee and Bluetooth. It had been proposed to provide wireless connectivity between body sensors and the healthcare systems, thus that leads the growth and extensive use of Wireless Body Area Networks (WBANs). After the study of their characteristics, we concentrate on the security issue essential for the sensitive healthcare clinical information.
Keywords: WBANs, Bluetooth, ZigBee, Healthcare.

1 Introduction

The aging population and growing cost of healthcare has introduced the great challenges for government, health service providers and healthcare industry. The availability of competent constant monitoring of patients can help doctors and trained staff to provide patients with a series of advanced and effective healthcare services. These services may include diagnostic procedures, maintenance of chronic conditions or supervising recovery from an acute event or a surgical procedure. These services are normally enabled with the use of a Wireless Body Area Network (WBAN). In this paper we had described the most commonly used wireless technologies, Bluetooth and ZigBee that can be used with WBANs. These technologies are presented in detail and they are compared with a focus to their security features. It is important to note that the available technologies in this field advances rapidly and there is a need for continuous evaluation and comparison of the new features presented by the corresponding standard associations and research agencies.

2. Wireless Body Area Network (WBAN)

2.1 Overview:

WBAN is a type of biomedical sensor networks. The Biomedical sensor nodes in WBAN are placed on, near or within a human body. In a medical healthcare system, WBAN continuously provides monitoring healthcare of especially elderly or ill people wherever needed. The Biomedical nodes sense and process vital signs such as heart rate, blood pressure, body temperature, respiratory from the human body. Then, they send collected data to a medical center via a base station in order to monitor human health by medical professionals. In the medical center, doctors/caregivers need monitoring systems/interfaces to process, analyze and visualize the received data from WBAN based systems [1, 2].

2.2 Wireless Communications Technologies in WBANs:

The economical and most widely used technologies enabling WBANs are Bluetooth

and ZigBee. Bluetooth is an emerging and very capable technology for WBANs. The use of these technologies is important for the exchange of informations that the sensors bring together. It sends the informations from the sensor to the monitoring application and vice versa. There are number of parameters and different characteristics that each technology may offer to the health care systems. These parameters and characters may include the offered applications, the cost, the communication range, the power consumption, the data rate, the frequency band, privacy and the security parameters.

3 Bluetooth and ZigBee features

3.1 Evolution and Applications:

Bluetooth is the widely used wireless technology, which is specified by IEEE 802 standards as IEEE 802.15.1 [3]. It was invented in 1994 by telecommunications vendor Ericsson and was originally conceived as a wireless alternative to RS-232 data cables. It can be used in a variety of applications that includes wireless control and communication between a mobile phone and a hands-free headset, replacement of traditional wired serial communications in test equipment, GPS receivers, bar code scanners, traffic control devices and short range transmission of health sensor data from medical devices to medical computers.

Nokia's research centre, attempted to develop a technology that would address issues in wireless technologies successfully. The first guidelines were published in 2004 under the name "Bluetooth Low End Extension" [4]. In 2006 Nokia introduced the Wibree technology as an open industry standard. Bluetooth Low Energy (LE) has evolved from the Wibree standard. In July 2010, the Bluetooth SIG announced the formal adoption of Bluetooth Core Specification Version 4.0 with the feature of Bluetooth low energy technology. The Bluetooth LE can be used for the interconnection of small devices like watches and sports sensors as well as in smart energy, home automation and healthcare devices.

IEEE 802 standard has introduced IEEE 802.15.4 in 2004 also known as ZigBee. It was first defined as a vertically integrated protocol suite that provides a distributed object abstraction for devices on a new low-power wireless link. The broad utility of this link led to the definition of a wide variety of application profiles that includes home automation and medical monitoring. In December 2006, the ZigBee 2006 specification was released, which was followed in October 2007 by the ZigBee 2007/PRO specification [5].

Bluetooth and ZigBee had already utilized in healthcare systems that use WBANs in order to offer monitoring services for patients. The elderly person that may live alone in their home requires homecare monitoring. Some important of them are the following: A WBAN System for Ambulatory Monitoring of Physical Activity and Health Status utilizes ZigBee [6]. The Improved WBAN communication at mental healthcare system with personalized biosignal devices uses Bluetooth [7].

3.2 Topology:

The selection of the suitable network topology is an important part of the network design. Improper selection results in waste of time, energy and a lot of troubleshooting methods are required to resolve disorders. The Bluetooth provides a uniform structure for a wide range of devices that connect and communicate with each other. Bluetooth operates primarily using adhoc piconets, where a master device controls multiple slaves. The slave devices may only communicate with the master device and they do not communicate directly with another slave device. However, a slave device may participate in one or more piconets. Piconets are limited to 8 devices as shown in Figure 1.

Bluetooth LE topology is different from Bluetooth. A device is the master in a piconet (represented by the blue dotted area, and known as piconet) with the other devices to be the slaves, it do not share a common physical channel with the master. Each slave communicates on a separate physical channel with the master. Also there are devices that are advertisers and initiators (represented by the red dashed area) as shown in Figure 2.

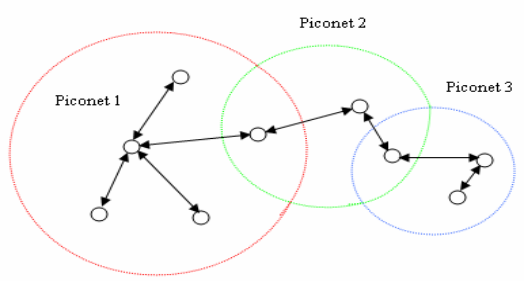

Fig. 1: Bluetooth topology

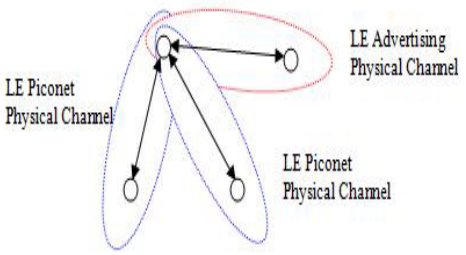

Fig. 2: Bluetooth Low Energy topology

ZigBee network consists of one coordinator, one or more end devices and optionally, one or more routers. The coordinator is a Full Function Device (FFD), responsible for the inner workings of the ZigBee network. A coordinator sets up a network with a given PAN identifier which end devices can join. End devices are typically Reduced Function Devices (RFDs) to allow for an inexpensive implementation. Routers can be used as mediators for the coordinator in the PAN, thus allows using Bluetooth, ZigBee and Bluetooth LE in WBANs. ZigBee topology network as shown in figure 3 works beyond the radio range of the coordinator. A router acts as a local coordinator for end devices joining the PAN, and must implement most of the coordinator capabilities and also acts as FFD device [12-20].

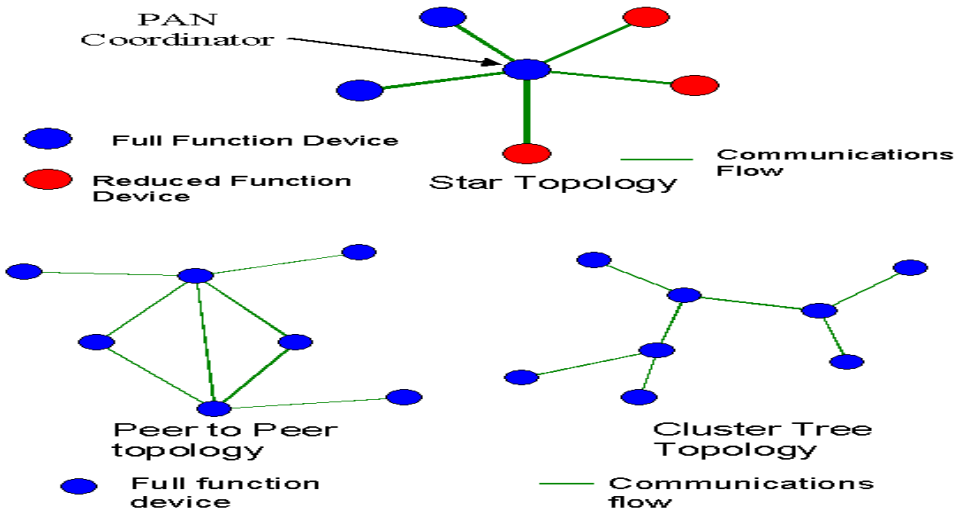

Figure 3: ZigBee Network Topology

3.3 Power deployment and Data Rate:

ZigBee is low-power alternative to Bluetooth and has extensively improved performance of 30mW compared to the Bluetooth's 100mW. ZigBee can attain a data rate of 250Kbps at 2.4 GHz (16 Channels), 40 Kbps at 915 MHz (10 channels), and 20Kbps at 868 MHz (1 channel). Bluetooth 1.2 achieves a maximum data rate of 1.2 Mbps and Bluetooth 2.0+EDR (Enhanced Data Rate) achieves up to 3 Mbps. Bluetooth 3.0 supports data transfer speeds of up to 24 Mbps.

3.4 Error rectification:

Bluetooth, ZigBee and Bluetooth LE execute Cyclic Redundancy Checks (CRCs) to protect against errors on communication channels. The error detection capability of a CRC depends on its length. Bluetooth and ZigBee utilize a 16-bit CRC for error control at the link layer. Bluetooth LE implements a 24-bit CRC that provides a higher level of assurance regarding error detection. The Bit Error Ratio (BER) is defined as the percentage of bits that have errors relative to the total number of bits received in a transmission. A BER of 10-6 in a transmission means that one bit is in error out of 106 bits (or 0,12 MB) transmitted. A 16 bit CRC cannot handle easily very low BER, (smaller than 10-6 - 10-8). Hence in the healthcare applications which are the focus of this paper a 16-bit CRC offers efficient error detection and the difference would be trivial compared to a 24-bit CRC.

3.5 Data Encryption and Authentication:

Wireless communications occurs in open atmosphere, it is trivial for an attacker to intercept and acquire data transmitted over the air, thus compromising the privacy of the involved parties at the same time. This inherent weakness is typically addressed with data encryption of the communication channel, ensuring that only authorized entities can decipher the information communicated. Bluetooth employs the E0 stream cipher for packet encryption and is based on a shared cryptographic secret, a previously generated link key or a master key. A 128-bit key is used in the E0 implementation of Bluetooth. These keys rely upon the Bluetooth PIN which has been entered into the end user devices. The E0 stream cipher has been proven to be susceptible to a number of attacks, degrading the strength of a 128-bit key to that of a 64-bit key. Bluetooth uses algorithms that are based on SAFER+ for key derivation, namely E21 and E22, and authentication as Message Authentication Codes (MACs), called E1. Again attacks against SAFER+ have been demonstrated. ZigBee is based on the security suite specified in the IEEE 802.15.4 standard. The 802.15.4 standard requires the use of the AES (Advanced Encryption Standard) algorithm with 128-bit keys and 128-bit block lengths. AES may be used in several modes, each of which offers either data privacy (encryption), data integrity, authentication or a combination of these functions. The standard requires that the CCM-64 (Counter with Cipher Block Chaining (CBC)-MAC) mode (encryption plus data integrity, with an 8-byte message integrity code MIC) is supported by the devices. ZigBee supports AES in CCM mode with a 128-bit key, a small variation of the CCM mode. The functions of encryption/decryption, authentication and verification / integrity are provided. Similarly to the ZigBee specification, session confidentiality in Bluetooth LE is provided by the AES encryption, which is used in CCM counter mode. In LE a 128-bit Long Term Key (LTK) is used to generate session keys for encrypted connections. Every time a new LTK is distributed a 64-bit random number (Rand) and a 16-bit encrypted diversifier (EDIV) are generated. Rand and EDIV are used to identify the LTK and establish a previously shared LTK in order to start an encrypted connection among two previously paired devices. Another 128-bit key, called Identity Resolving Key is used to generate and resolve random addresses, a feature that provides privacy to the communicating parties [4, 8].

3.6 Modulation:

Amplitude shift keying (ASK), frequency shift keying (FSK) and phase shift keying (PSK) are three types of Digital modulation. The Wireless technologies use the modulation process and supports data rate and range. ZigBee uses PSK modulation and in particular the BPSK (or 2PSK) and OPSK (or 8PSK). Bluetooth uses both PSK (BPSK and OPSK) and FSK (GFSK) while Bluetooth LE utilizes GFSK. In FSK a binary 0 is transmitted as a frequency f0 and a binary 1 is transmitted as a frequency f1. MSK (Minimum Shift Keying) is a form of FSK with a minimum frequency difference between f0 and f1. In Phase Shift Keying the digital information is transmitted by shifting the phase of the carrier among several discrete values. The performance of PSK and FSK is similar, however the bandwidth required by a signal transmitted in PSK is significantly less than in FSK. On the other hand FSK based schemes are considered simpler to implement. There are many variations of PSK. Some of the more widely used include: binary phase shift keying (BPSK), differential phase shift keying (DPSK), quaternary phase shift keying (QPSK), differential QPSK (DQPSK) and octonary phase shift keying (OPSK). The higher order modulation allows higher data transfer within a given bandwidth. Thus it requires a better signal to noise (S/N) ratio, otherwise the error rates will start to grow and affect the improvements in the data rate performance [9-11].

4. Comparison between Bluetooth & ZigBee

Key Points	Bluetooth	ZigBee
Range	10m to 100 m	5m to 500m
Networking Topologies	Ad-hoc, very small networks	peer to peer, star, Tree, or mesh
Operating Frequency	2.4 GHz	868 MHz (Europe) 900-928 MHz (NA), 2.4 GHz (worldwide)
Maximum Data transfer rate	3 Mbps	20 Kbps, 40 Kbps, 250 Kbps
Power Consumption	Medium -100 mW	Very Low- 30 mW
Access Method	TDMA	CSMA/CA
Complexity	High	Low
Authentication	Shared secret (PIN), SAFER+	AES CBC-MAC (CCM mode)
Robustness	16-bit CRC	16-bit CRC
Advantages	A widely used technology that is supported by most devices. It is ideal for applications that are requiring high bit rates over short distances.	A low-power alternative to Bluetooth, that offers significantly improved performance of 30mW compared to Bluetooth 100mW.
Disadvantages	Open to interception and attack.	Low data rate.
Applications	Wireless connectivity between devices such as phones, PDA, laptops, headsets, Computer and accessory devices, Computer to compute, Computer with other digital devices.	Industrial control and monitoring, sensor networks, building automation, healthcare, home control and automation, toys.

Table 1: comparison between Bluetooth & ZigBee

4 Conclusions

According to a succession of standard norms and performance features, analysis is performed and compared Bluetooth and ZigBee. Table 1 summarizes the advantages and disadvantages of these technologies, similarities and differences based on certain key points. Several key features of Bluetooth and ZigBee had introduced numerous novel ideas. With regards to WBANs, ZigBee is a low-power alternative to Bluetooth that offers significantly improved performance of 30mW compared to Bluetooth 100mW for healthcare applications. However, there are several open issues regarding WBANs, the most important aspects are: interoperability, system devices design, system and device-level security, invasion of privacy, sensor validation, data consistency, sensors resource constrains and the intermittent availability of uplink connectivity.

References:

1. Istepanian, R.S.H., Jovanov, E., Zhang, Y.T.: M-Health: Beyond Seamless Mobility and Global Wireless Health-Care Connectivity. The Proceedings of the IEEE Transactions on Information Technology in Biomedicine, 405–414 (2004).

2. Jovanov, E., Milenkovic, A., Otto, C., de Groen, P.C.: A Wireless Body Area Network of Intelligent Motion Sensors for Computer Assisted Physical Rehabilitation. Journal of Neuro Engineering and Rehabilitation, 6–16 (2005).

3.http://www.bluetooth.com/English/Technology/Building/Pages/Specifcation.aspx.

4.http://www.bluetooth.com/English/Products/Pages/low_energy.aspx.
5.http://www.zigbee.org/Markets/ZigBeeSmartEnergy/Version20Documents.aspx.
6. Jovanov, E., Milenkovic, A., Otto, C., De Groen, P., Johnson, B., Warren, S., Taibi, G.: A WBAN System for Ambulatory Monitoring of Physical Activity and Health Status: Applications and Challenges. In: The Proceedings of 27th Annual International Conference of the Engineering in Medicine and Biology Society, Shanghai, pp. 3810–3813 (2005).
7. Jung, J.Y., Lee, J.W.: Improved WBAN Communication at Mental Healthcare System with the Personalized Bio Signal Devices. In: The Proceedings of 8th International Conference Advanced Communication Technology, Korea, pp. 812–816 (2006).
8. Vaudenay, S.: On the need for Multipermutations: Cryptanalysis of MD4 and SAFER. In: Preneel, B. (ed.) FSE 1994. LNCS, vol. 1008, pp. 286–297. Springer, Heidelberg (1995).
9. IEEE Std. 802.15.4-2003, IEEE Standard for Information Technology Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks Specific Requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (WPANs). IEEE Press, New York (2003).
10. Eren, H.: Wireless Sensors and Instruments: Networks, Design, and Applications. CRC Press, Boca Raton (2005).
11.http://www.zigbee.org/About/AboutAlliance/TheAlliance.aspx.
12. S. M. Ghatole, K.Y. Rokde, S. S. Shende, P.B. Dahikar, "Role of Wireless Body Area Network in Remote Healthcare Monitoring" published in International Journal of Researches in Biosciences, Agriculture and Technology (IJRBAT), ISSN: 2347-517X, Volume II, issue (7), Nov 2015, pp 154-157.
13. K. Y. Rokde, P. B. Dahikar, M. J. Hedau, S. M. Ghatole, S. S. Shende "Study of Biosensors using nanotechnology" published in International Journal of Advances in Science, Engineering and Technology (IJASEAT), ISSN: 2321-9009, Special Issue-1, June- 2015, pp 155-157.
14. K. Y. Rokde, S. M. Ghatole, A. G Kshirsagar, N. D. Meshram, S. S. Shende "Design and Implementation of Speed Control Motor Using Fuzzy Logic Technique" International Journal of Industrial Electronics and Electrical Engineering (IJIEEE), Volume 4, Special Issue 2, June 2015, ISSN: 2347-6982, pp 120-124.
15. S. M. Ghatole, K. Y. Rokde, S. S. Shende, P.B. Dahikar "Healthcare System with Interactive Biosensors" published in International Journal of Electronics, Communication & Soft Computing Science and Engineering (IJECSCSE), ISSN: 2277-9477, Volume 4, Issue 4, July 2015, pp 1-4.
16. K. Y. Rokde, S. M. Ghatole, S. S. Shende, P. B. Dahikar, "An Embedded System for Patient Heartbeat Monitoring" International Journal of Electronics, Communication & Soft Computing Science and Engineering (IJECSCSE), ISSN: 2277-9477, Volume 4, Issue 4, July 2015, pp 288-292.
17. S. M. Ghatole, P. B. Dahikar, "Survey on Wireless Body Area Network for Healthcare Applications", International Journal of Researches in Biosciences, Agriculture and Technology (IJRBAT), Vol. IV, Issue (3), Sept. 2016: ISSN 2347 – 517X, pp 14-17.
18. S. M. Ghatole, K. Y. Rokde, P. B. Dahikar, "ZigBee: A Wireless Communication Network" Kamla Nehru Journal of Science & Technology (KNJST) Vol. - 1 ISBN: 978-93-81432-97-6, pp 62-66.
19. S. M. Ghatole, P. B. Dahikar, "Use of Innovative ZigBee Technology in Homecare Monitoring System", International Journal of Researches in Biosciences, Agriculture and Technology (IJRBAT), Vol. V, Special Issue 2, July 2017: ISSN 2347 – 517X, pp 101-104.
20. K. Y. Rokde, P. B. Dahikar, S. M. Ghatole, S. S. Shende, M. J. Hedau, "A Non-Invasive Blood Pressure Measurement Using Embedded Technology" International Journal of Scientific Research in Science and Technology (IJSRST), Volume 4, Issue 1, IJSRST 4132/ NCRDAMDS/January-February-2018, pp 137-141.

.