An Analysis of Bluetooth, Zigbee and Bluetooth Low Energy and Their Use in WBANs

Emmanouil Georgakakis, Stefanos A. Nikolidakis,
Dimitrios D. Vergados, and Christos Douligeris

Department of Informatics, University of Piraeus,
80, Karaoli & Dimitriou St., GR-185 34, Piraeus, Greece
{egeo,snikol,vergados,cdoulig}@unipi.gr

Abstract. A rapid development of services and technologies in the field of health care has been witnessed in the last few years. In this paper we present an analysis and an extensive comparison of radio communication technologies, namely Zigbee, Bluetooth and Bluetooth Low Energy, that have been proposed as likely candidates to provide wireless connectivity between body sensors and the health care system and consequently to lead the development and extended deployment of Wireless Body Area Networks. After the description of their characteristics, we concentrate on the security that these technologies offer since security is extremely important for the sensitive health care clinical information communicated and the protection of patients' clinical information privacy.

Keywords: WBAN, Bluetooth, Zigbee, Bluetooth Low energy, m-Health, security.

1 Introduction

The availability of efficient continuous monitoring of patients can help doctors and trained personnel to provide patients with a series of advanced and effective health care 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 typically enabled with the deployment of a Wireless Body Area Network (WBAN).

In this paper we describe the most common wireless technologies that can be used in WBANs. In particular we focus on Bluetooth and Zigbee, which are widely used, as well as on Bluetooth Low Energy (LE), which is an emerging technology. 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 advance rapidly and there is a need for continuous evaluation and comparison of the new features presented by the corresponding standard associations and research forums.

J. Lin and K.S. Nikita (Eds.): MobiHealth 2010, LNICST 55, pp. 168–175, 2011.

2 Wireless Body Area Network (WBAN)

2.1 Overview

A WBAN is a collection of several small devices that are close or attached to the human body. These devices integrate wearable health monitoring systems into a telemedicine system that is able to support the early detection of abnormal conditions and the prevention of its serious consequences. For example a WBAN can alert the hospital, even before a patient has a heart attack, through the measuring of changes in one's vital signs [1, 2].

2.2 Wireless Communications Technologies in WBANs

The most widely used technologies enabling WBANs are Bluetooth and ZigBee. Bluetooth LE is an emerging and very promising technology for WBANs. The use of these technologies is important for the exchange of information that the sensors collect, from the sensor to the monitoring application and vice versa. Thus, there are a lot of parameters and different characteristics that each technology may offer to the health care systems. These characteristics may include the offered applications, the cost, the communication range, the power consumption, the data rate, the frequency band and the security parameters.

3 Bluetooth, ZigBee and Bluetooth LE Functionality and Features

3.1 History and Applications

Bluetooth, which is specified in IEEE 802.15.1, is the widest used wireless technology [3]. It was invented by telecommunications vendor Ericsson in 1994 and was originally conceived as a wireless alternative to RS-232 data cables. It can be used in a variety of applications that include: 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 successfully address issues that wireless technologies could not manage to carry out successfully. The first guidelines were published in 2004 under the name "Bluetooth Low End Extension" [4]. Following these efforts in 2006 Nokia introduced the Wibree technology as an open industry standard. Bluetooth 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.

In 2004 the IEEE 802.15.4 also known as ZigBee 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 include home automation, commercial

building automation and smart energy which cut across industry segments 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 have already been utilised in healthcare systems that use WBANs in order to offer monitoring services for patients and elderly people that may live alone in their home. Some important of them are the following:

A WBAN System for Ambulatory Monitoring of Physical Activity and Health Status that utilises Zigbee was proposed in [6]. The Improved WBAN communication at mental healthcare system with personalized bio signal devices that uses Bluetooth is proposed in [7].

3.2 Topology

The choice of the appropriate network topology is an important part of the network design. A misconfigured network can result in waste of time, energy and a lot of troubleshooting methods are required to resolve disorders.

The Bluetooth Specification defines a uniform structure for a wide range of devices that connect and communicate with each other. Bluetooth operates primarily using ad hoc 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. Figure 1 summarises Bluetooth topology.

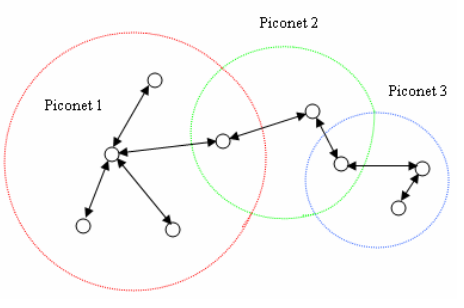

Fig. 1. Bluetooth topology

The topology of the Bluetooth LE is different to 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, The slaves 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). Figure 2 presents this topology.

A ZigBee network consists of one coordinator, one or more end devices and, optionally, one or more routers (Figure 3). 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 allowing

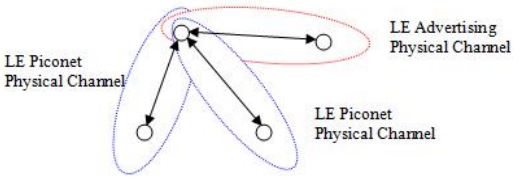

Fig. 2. Bluetooth Low Energy topology

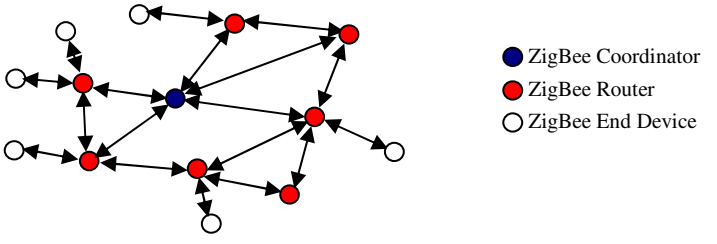

Fig. 3. Zigbee topology

the network to expand 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. Hence, a router is also an FFD device.

3.3 Power Consumption and Data Rate

ZigBee, was designed to be a low-power alternative to Bluetooth, and indeed offers a significantly improved performance of 30mW compared to the Bluetooth's 100mW. ZigBee can achieve a data rate of 250Kbps at 2.4GHz (16 Channels), 40 Kbps at 915 MHz (10 channels), and 20Kbps at 868Mhz (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 theoretical data transfer speeds of up to 24 Mbit/s.

The Bluetooth LE enables dual-mode implementations to reuse the Bluetooth RF part and to guarantee ultra low power consumption for devices with embedded stand-alone implementation of the Bluetooth LE specification. The Bluetooth LE has physical layer bit rate of 1 Mbps and may achieve link distance of around 10 meters. Bluetooth LE consumes only 10% of the power consumed by Bluetooth. It can save energy and extend battery life by sleeping and waking up when it needs to send data.

3.4 Error Correction

Bluetooth, ZigBee and Bluetooth LE implement CRCs (Cyclic Redundancy Checks) to protect against errors on communication channels. The error detection capability of a CRC depends on its length. Bluetooth and ZigBee utilise 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 10^6 bits (or 0,12 MB) transmitted. A 16 bit CRC can not handle easily very low BER, (smaller than 10^{-6} - 10^{-8}). Hence in the health care 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

Due to the open nature of Wireless communications 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 [8, 9].

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 [10, 11].

ZigBee is based on the security suite specified in the IEEE 802.15.4 standard [12]. 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 functionalities 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].

Bluetooth LE supports the ability to send authenticated data over an unencrypted channel between two devices with a trusted relationship. This is accomplished by signing the data with a 128-bit Connection Signature Resolving Key (CSRK).

It has to be noted that stream ciphers tend to be faster than block ciphers and the complexity of their implementation in hardware is not high. In addition to that they do not propagate errors, contrary to block ciphers.

However Zigbee and Bluetooth LE that employ variations of AES (block cipher) for encryption and authentication provide high level of assurance with regard to the strength and safety of the deployed algorithm. On the other hand, the encryption (stream cipher) and authentication mechanisms of Bluetooth have been proven to be susceptible to attacks that may undermine the overall security posture of the Bluetooth communication and put at risk the privacy of its users.

3.6 Modulation

Digital modulation techniques can be categorized in three groups: amplitude shift keying (ASK), frequency shift keying (FSK), and phase shift keying (PSK). The data rate and range supported by wireless technologies are directly affected by the modulation scheme adopted.

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 utilises GFSK.

In FSK a binary 0 is transmitted as a frequency f_0 and a binary 1 is transmitted as a frequency f_1. MSK (Minimum Shift Keying) is a form of FSK with a minimum frequency difference between f_0 and f_1 [13]. 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). In general the higher order forms of modulation allow higher data rates to be carried within a given bandwidth. Nevertheless, the higher data rates require a better signal-to-noise-ratio (SNR), otherwise the error rates will start to rise and any improvements in the data rate performance will be diminished [13].

4 Conclusions

In this paper, we analysed and compared Bluetooth, Bluetooth LE and ZigBee according to a series of criteria and performance features. Table 1 summarises the advantages and disadvantages of these technologies and Table 2 their similarities and differences.

Bluetooth LE appears to have adopted several key features from Bluetooth and some from Zigbee and it has also introduced several novel ideas. The Bluetooth LE specification improves on the weaknesses and addresses issues that were not resolved in Bluetooth and other wireless technologies. In particular Bluetooth LE appears to have superior features regarding power consumption, scalability, confidentiality, authentication mechanisms and error correction. The improvements in the aforementioned areas have a negative impact on Bluetooth LE data rate transfer and the

achievable range. Nevertheless with regards to WBANs a data rate of 1Mbps and a range of 10 meters are acceptable.

However there are several open issues regarding WBANs, the most important aspects that need to be addressed are: interoperability, system devices design, system and device-level security, invasion of privacy, sensor validation, data consistency, sensor resource constrains and the intermittent availability of uplink connectivity.

Table 1. Comparison of Zigbee, Bluetooth and Bluetooth Low Energy

	Bluetooth	ZigBee	Bluetooth LE
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.	It offers high spectral efficiency and low power consumption
Disadvantages	Open to interception and attack.	Low data rate.	Not supported by many devices

Table 2. WBAN technologies key features

	Bluetooth	ZigBee	Bluetooth LE
Applications	Computer and accessory devices, Computer to compute, Computer with other digital devices	Home control. Building automation, Industrial automation, Home security, Medical monitoring	Sports and fitness products, watches, smart energy home automation devices, remote controls and healthcare devices.
Frequency Band	2.4 - 2.48GHz	868MHz, 902-928MHz 2.4-2.48GHZ	2.4GHz
Topology	Ad-hoc piconets	Ad-hoc, star, mesh	Ad-hoc piconets
Scalability	Low	High	High
Range	~10 meters	~100 meters	~10 meters
Maximum Data transfer rate:	3 Mbps	20 Kbps 40 Kbps 250 Kbps	1 Mbps
Power Consumption	100 mW	30 mW	~10 mW
Access Method	TDMA	CSMA/CA	TDMA FDMA
Encryption	128-bit encryption E0 stream cipher	128-bit AES block cipher (CTR, counter mode)	128-bit AES block cipher (CCM mode)
Modulation	GFSK, 2PSK, DQSP, 8PSK	BPSK (868/928MHz) OPSK (2.4GHz)	GFSK
Authentication	Shared secret (PIN), SAFER+	AES CBC-MAC (CCM mode)	AES CBC-MAC (CCM mode)
Robustness	16-bit CRC	16-bit CRC	24-bit CRC

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 NeuroEngineering 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. Lu, Y., Vaudenay, S.: Cryptanalysis of an E0-like Combiner with Memory. Journal of Cryptology 21, 430–457 (2008)
9. Lu, Y., Vaudenay, S.: Cryptanalysis of Bluetooth Keystream Generator Two-Level E0. In: Lee, P.J. (ed.) ASIACRYPT 2004. LNCS, vol. 3329, pp. 147–158. Springer, Heidelberg (2004)
10. 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)
11. Shihui, Z., Licheng, W., Yixian, Y.: A New Impossible Differential Attack on SAFER Ciphers Computers and Electrical Engineering. Elsevier Computers & Electrical Engineering 36(1), 180–189 (2010)
12. 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)
13. Eren, H.: Wireless Sensors and Instruments: Networks, Design, and Applications. CRC Press, Boca Raton (2005)