An Overview on Wireless Body Area Networks

Rudy Berton, Vassilikí Menarin
Department of Mathematics "Tullio Levi-Civita"
University of Padua
Padua, Italy
rudy.berton@studenti.unipd.it, vassiliki.menarin@studenti.unipd.it

***Abstract*—Wireless Body Area Networks (WBAN) is a recent wireless technology that presents its main application in medical field with the use of sensors that work in close vicinity to, on or inside a human body. Through the years, two main standards have been established by a task group to define this technology: IEEE 802.15.4 and IEEE 802.15.6. The purpose of this paper is to give a general overview of the technology employed in WBANs, describing the standards with their differences between Physical and Mac layers, to talk about the different fields in which WBANs can be applied and the issues and challenges that may arise when working with these networks.**

I. Introduction

The interest in developing wireless networks built around humans, mainly for an easy and quick way to help monitor health and physiology, has significantly grown in recent years: there is now a higher demand for these kind of communications, that have recently become possible thanks to technological advances.

In particular, the minimization of components and the creation of very-low-power wireless technologies have opened new possibilities for the development of small, personal wireless networks. Furthermore, non-invasive technologies as well as technologies compatible with human physiology are very sought after.

Wireless Body Area Networks (WBANs) have been developed as a new wireless technology with promising applications in many fields, mainly healthcare, but also athletic training, secure authentication and safety.

A WBAN is a network that connects tiny nodes, usually sensors and/or actuators to the human body. The wireless sensors are usually placed in, on or around a persons body. From there, they connect to router nodes that receive and elaborate the data transmitted. Since these router nodes are intended to be placed around the wearer, the sensor nodes dont need to cover wide ranges, averaging around 2m. From there, the data may ultimately be sent to centralized centers and databases. Figure 1 shows the general architecture of a WBAN.

Since they are based on sensors that gather and elaborate data, WBANs may be considered similar to sensor networks but, due to their unique characteristics, they pose some new technical challenges [1]. Some of the main differences between WBANs and conventional sensor networks are listed in Table I.

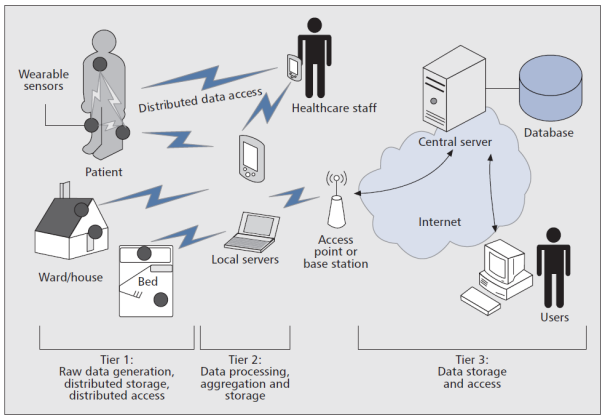

Fig. 1. The general architecture of WBANs

TABLE I
Main differences between WSNs and WBANs

	WSN	**WBAN**
Architecture	Every node is both a sensor and a router	Two categories of nodes: sensor/actuators placed in or on the human body and router nodes around them
Density	May present high redundancy for a better fault tolerance	Usually low
Data rate	Usually used for monitoring irregular events	Human physiological activities may vary in a periodic manner, this may lead to stable data rates
Latency	It may be necessary to maximize battery life in a WSN at the expense of higher latency	Reduce latency even if it impacts battery savings (replacements of batteries may be easy)
Mobility	Stationary nodes	Wearers move around

We will now discuss some of WBANs' most promising applications. Then we will discuss the different standards that have already been set for this kind of networks and their main differences. Finally, well give an overview of the challenges these network pose.

II. WBAN Applications and Devices

The employment of Wireless Body Area Networks was initially mainly focused on the medical field, nevertheless in the last years, starting from these initial discoveries, they have been used to introduce some innovations in non-medical fields too.

Still, the most common application of this technology remains healthcare, where WBAN is used to collect biomedical signals monitoring patients with health problems remotely and continually. Knowing the patient's history and coupling this knowledge with this type of applications can reduce medical accidents and increase public safety alerting medical personnel in time. Some parameters monitored are heartbeat, body temperature and blood pressure. This is possible thanks to wearable applications (e.g. ECG) while implanted applications are used to monitor more particular diseases (e.g. diabetes, cancer) and can be implanted directly under the skin or in the bloodstream.

Some non-medical fields in which WBAN is recently being employed are the sports, entertainment and military environment. Both in the first and last case this technology can improve performances of athletes and soldiers keeping a log of physiological data, as well as detect life threatening situations in military context. In the entertainment environment WBANs can be used for different purposes, for example to register body motions of actors during the making of a film.

There are three classes of devices that constitute WBANs and allow its applications: wireless sensor nodes, actuators and wireless personal devices. The first type concerns components, wearable or implantable, that provide wireless monitoring of people or environment, communicating physiological parameters to other devices. Indeed, the work of actuators depends on the data received: if sensors detect an abnormal parameter, actuator administer medicine to the patient. Finally, a Personal Device (PD) is the device responsible for the communication between sensors, actuators and cellular phone through wireless connection [2].

III. WBAN Standards

Two are the most known standards created as solution for Wireless Body Area Networks. The first one is IEEE 802.15.4, developed in 2003 and mainly thought for low-rate and low-power Wireless Personal Area Networks (WPAN), later adapted to operate around the human body with a WBAN. The second one is IEEE 802.15.6 and it was born in 2007 abd developed to be a good solution for the WBAN right from the beginning. Its final version was published in 2012 and nowadays is the most widely used standard in WBAN technologies.

These solutions have a different structure in Physical layer (PHY) and Medium Access Control layer (MAC) as we will see below.

A. IEEE 802.15.4

The topology thought for the IEEE 802.15.4 standard considers devices that consume minimal power in a WPAN and can cover an area of 10 meters using unlicensed radio bands (ISM). Each device represents a node in the network and can have two possible roles during the communications: a coordinator node, with specific tasks to fulfill, or a simple node that only sends/receives information.

The PHY layer presents 27 channels divided in three different frequency bands and interacts with the MAC layer after the selection of the right channel. Moreover, the PHY level controls the activation/deactivation of radio transceivers, the quality of the links, the transmission and reception of packets over the medium and the estimation of the inbound signal power.

The standard's structure allows MAC layer to operate in two different modes, beacon-enabled or beacon-less, using three different access schemes in the exchange of packets: unslotted carrier sensing multiple access with collision avoidance (CSMA-CA), a slotted version of the same one and the contention free period scheme (CFP).

Beacon-enabled mode: There is a coordinator node that periodically transmits a beacon, defining a superframe that starts with a beacon and ends with the next one. Each beacon contains information about the identification and the synchronization of the PAN in addition to the structure of the superframe. The remaining part is called Contention Access Period (CAP) and is used for data transmission made by nodes through the channel using the slotted CSMA/CA for a correct synchronization. Moreover, the coordinator could reserve up to seven slots after CAP in the superframe, called Guaranteed Time Slots (GTS). These slots can be assigned to devices that have to run their applications without the contention with other devices. The GTS form the CFP that works in Time Division Multiple Access (TDMA) [fig. 2].

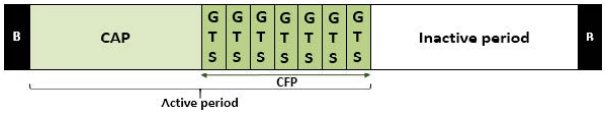

Fig. 2. Superframe in Beacon-enabled mode of standard IEEE 802.15.4

Beacon-less mode: No superframe is defined because there isn't any transmission of beacons for the synchronization; only random access is available and for this reason the transmission can not be guarantee and no GTS slot can be reserved. It implies the use of an unslotted version of CSMA-CA before the transmission of data. Devices that want to send data have to pick a random backoff delay and, when it expires, they have to perform a clear channel assessment (CCA): listen if the channel is idle and transmit or pick a new backoff delay to try again in the next transaction.

Both the slottend and unslotted CSMA-CA algorithms are only used for data transaction and not for beacon frames, acknowledgment or CFP transmissions and definition of the maximum number of backoffs that can fail before the channel is declared inaccessible. Indeed, in beacon-enabled mode, when the device performs a CCA, after the random backoff delay, if the channel is idle the device decides to repeat the CCA for a number of backoff units in accordance to the value

of the contention window (CW) before it transmits. During all the backoff units of CW, if channel is idle, the device can transmit the data, otherwise it has to restart with a new backoff delay.

In this type of networks two types of data transactions are possible: from coordinator to devices or vice versa. In the former, when the coordinator informs the target device of the data through beacon, the receiver replies that it is ready by sending a request back to the coordinator (using slotted CSMA-CA). The coordinator can now select a free slot to start the transmission. In the latter case, when the coordinator receives data from the device, in a similar way as explained above, it could confirm the successful reception by sending back an acknowledgment [3].

B. IEEE 802.15.6

Several years after IEEE 802.15.4,the definition of a new standardization of WBAN to optimize the low-power nodes that handle the applications started.

The new 802.15.6 standard defines a MAC layer that supports not one but three operational PHYs layers, each one with an hub (or coordinator) and a total number of at most 64 nodes that are organized into one-or-two-hop star topology. A brief description of the physical layers follows:

Narrowband PHY. It is responsible for the activation/deactivation of the radio transceiver, clear channel assessment and data reception/transmission; it defines the Physical Protocol Data Unit (PPDU) frame that includes three components:

- Physical Layer Convergence Procedure (PLCP) preamble is composed of two sequences: the first one is used for coarse time synchronization, carrier-offset recovery and packet detection, the second instead is used for fine time synchronization.
- PLCP header contains a PHY header, with several fields used to convey information to the receiver for a successful decoding and some parity check bits used for error detection and error correction of PHY header.
- Physical-layer Service Data Unit (PSDU), transmitted for last, contains a MAC header, a MAC frame body and a Frame Check Sequence (FCS).

Ultra Wideband PHY. It supports 11 channels in low and high band with different frequencies and has two modes of operation: default mode and high Quality of Service mode, thought for high priority medical applications. The aim of UWB is to achieve high performance, low complexity and low power consumption. The PPDU frame for this PHY layer consists of the Synchronization Header (SHR) with the same task of PLCP plus the start-of-frame delimiter (SFD) used for frame synchronization; a PHY Header (PHR) that conveys information (about the data rate of the PSDU and length of payload) used by the receiver to decode the PSDU and a third part that defines the frame, similar to the Narrowband one. However, the disposition of parity check bits for error correction of MAC frame body changes.

Human Body Communications PHY. Similar to NB PHY, the packet contains a PLCP preamble, SFD, PLCP header with control and error detection/correction bits and at last PSDU. In this PHY, the preamble sequence is transmitted four times to ensure packet synchronization, while SFD is transmitted once.

For the MAC layer, the standard defines a channel division into beacon periods (also called superframes) of equal length made by hubs. They transmit a beacon to define the superframe boundaries and allocate the slots that are used for data transmission. Generally a hub transmits a beacon in each active superframe and when beacons are not used the boundaries of superframe are defined by a polling action.

The frame in the MAC layer is formed by a header, a frame body with maximum length of 255 bytes and the Frame Check Sequence at last. The MAC Header includes a control field that controls information about the frame, the sender and recipient identification and the WBAN ID field with information about the network. In addition to the payload, in the MAC frame body there are bits with the aim of assessing the freshness, authenticity and integrity of the message.

IEEE 802.15.6 supports three different communication modes: *Beacon Mode with Superframe Boundaries, Nonbeacon Mode with and without Superframe Boundaries*. In the first mode (fig. 3), mostly used in medical applications, the superframe structure is divided into Exclusive Access Phases (EAPs), used to transfer high-priority or emergency traffic, Random Access Phases (RAPs), a Contention Access Phase (CAP), both used for regular traffic and Managed Access Phases (MAPs or TypeI/II phases) provided for reservation of transmission periods or for unplanned traffic. When superframe boundaries are defined in non beacon mode the hub operates during the MAP periods only, in the other case instead the hub provides only unscheduled Type II polled allocation because each node establishes its own time base independently.

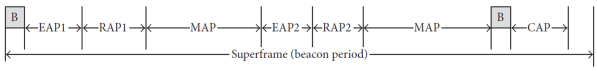

Fig. 3. Beacon mode with superframes of standard IEEE 802.15.6

The access mechanism used in each period of the superframe presents three categories. The *Random Access Mechanism*, used in EAP, RAP and CAP periods, define the use of slotted Aloha or CSMA/CA protocol by the coordinator for the resource allocation. *Improvised and Unscheduled Access Mechanism* is used when hub needs an improvised access to send poll or post commands without a notice in beacon or nonbeacon modes, outside the scheduled allocation interval. *Scheduled and Scheduled-Polling Access Mechanism* instead is used to schedule the allocation of slots in one or multiple upcoming superframes (also called 1-periodic or m-periodic allocations). [4] [5]

C. Comparison between WBAN standards

Table II [2] summarizes the main differences in the designs of standards IEEE 802.15.4 and IEEE 802.15.6.

TABLE II
A COMPARISON BETWEEN IEEE 802.15.4 AND IEEE 802.15.6

Criteria	**IEEE 802.15.4**	**IEEE 802.15.6**
Network type	WPAN	WBAN: NB, UWB and HBC
MAC modes	Beacon/Non beacon mode with/without superframe	Superframe with/without beacon mode
Access mechanism	Random access (with contention), scheduled access (without contention)	Contention based random access or connection oriented contention-free
Contention access resource allocation procedure	Slotted and unslotted CSMA/CA	CSMA/CA slotted Aloha
Specific Access for prioritised traffic	No	Yes (EAP)

There have been some tests and evaluations on the two standards described to better understand how to employ them in WBANs and which one is better fitted for real-life scenarios. Even though IEEE 802.15.6 was specifically designed for WBANS, tests done in a simulation environments (Castalia for both [6] and [7]) show how 802.15.4 outperforms 802.15.6 in terms of throughput and energy consumption. Indeed, the number of received packets in IEEE 802.15.4 is greater since it uses TDMA technology that mitigates the number of packet collision; in EAP and RAP periods instead, for standard 802.15.6, the use of CSMA/CA access procedure for resource allocation leads to a higher collision probability for nodes with same priority. More specifically, 802.15.4 seems overall more suited for communications in low traffic rates conditions. On the other hand, 802.16.6 shows better performances when it comes to packet delivery latency and seems to work better in high traffic rate scenarios.

One proposal [6] is to use IEEE 802.15.4 for non-time critical sensor requiring low data rates while favoring IEEE 802.15.6 for sensors with high data rates and in time critical applications.

IV. CHALLENGES AND OPEN RESEARCH ISSUES

To design efficient and usable WBANs, we have to overcome some important challenges. Since WBANs may be used in different applications, the issues we are facing may also vary a lot. Here we analyze the general challenges and research issues one has to consider when designing a WBAN [1], even though they may not all be pertinent at the same time.

A. Physical characteristics of nodes

Since the nodes are going to be implemented on, if not inside, human bodies, it is crucial to consider how they are built. One needs to carefully evaluate their size, material and compatibility with the human body. Furthermore, many people may find the implant of a sensor inside their body invasive, and refuse it. Thus, sensor placed on the skin may be preferable. Finally, one needs to answer concerns regarding the electronic and magnetic energy absorbed by human tissues.

B. WBAN specific issues

Overall, WBANs would benefit for more research and improved models to help predict their unique behavior in realistic environments. For example, how is the signal propagation being affected by the physical characteristics of the human body? Are there going to be issues when considering a moving wearer? Also, power management, sensor calibration, management of resources may be handled in new, different ways from the ones already in use in other kind of networks.

C. Power Supply

While batteries may be easy to replace in devices situated outside the human bodies, remote battery recharging becomes not-negotiable for devises implemented directly inside the human body.

D. Device Interoperability

Different devices, from different manufacturers and monitoring different phenomena may be implemented at the same time on a single wearer. All these devices need to be able to operate without interfering with each other. In same cases, they may need to exchange data between them. The setting of some common standards may greatly help with device compatibility.

E. Privacy and Security issues

Security may be the greatest challenge for WBAN and its strongly required due to the nature of the data exchanged, especially in medical applications. Since WBANs deal with very personal information, there is a strong need to ensure data privacy and a reliable authentication in the whole data transfer process.

Not only this, data also needs to be confidential, uncorrupted and dependable. Finding the right balance is a very delicate matter and security may conflict with many other aspects. Depending on the system we are building we may need to sacrifice efficiency or usability for an increased security.

Paper [8] gives an overview on all the different security issues involved when dealing with WLANs in healthcare, here we list some of the most common practical issues concerning security:

- Security and Efficiency: the devices involved in WBANs are very small and may lack the storage capabilities and power supplies needed for strong cryptographic computations required to ensure security. Efficiency may be sacrificed dedicating more power to the security operations
- Security and Safety: the devices may carry vital information on the wearers health which may become inaccessible in time of need if the wearer is unconscious or unresponsive. There needs to be a way to ensure strong security as well as privacy while, at the same time, allowing flexible access to qualified, legitimate, medical staff. There has been some research in this regard ([8]) but it's still a challenging requirement

- Security and Usability: the main aim of medical WBANs is to simplify health monitoring. That means that even non-qualified people should be able to manage their own devices, at least at a basic level. When configuration and setup of the devices becomes too technical, people may feel discouraged and prefer other solutions. On the other hand, if we try to increase usability by omitting some manual configuration steps, this may lead to looser security policies.

V. Conclusions

WBAN is an emerging and promising technology that may bring huge changes in peoples lives. In order to improve this technology a coordinated effort between different fields may be required: proposals may come not only from computer science, but also from biology and the design of new materials.

We gave an overview of WBANs' many applications and the steps that have already been taken to try and standardize this technology. While WBANs may be used in many different fields, arguably, their most interesting use is healthcare, through what is often termed e-healthcare. E-Healthcare is also the field that poses the biggest challenges, mainly in data security and privacy.

In conclusion, WBAN technology, while still requiring thorough research and studies before it can be widely applied, may lead to very important developments in our everyday lives.

References

[1] H. Cao, V. Leung, C. Chow, and H. Chan, "Enabling technologies for wireless body area networks: A survey and outlook," *IEEE Communications Magazine*, vol. 47, no. 12, pp. 84–93, 2009.

[2] M. Salayma, A. Al-Dubai, I. Romdhani, and Y. Nasser, "Wireless body area network (wban): a survey on reliability, fault tolerance, and technologies coexistence," *ACM Computing Surveys (CSUR)*, vol. 50, no. 1, p. 3, 2017.

[3] C. Li, H.-B. Li, and R. Kohno, "Performance evaluation of ieee 802.15. 4 for wireless body area network (wban)," in *2009 IEEE International conference on communications workshops*. IEEE, 2009, pp. 1–5.

[4] K. S. Kwak, S. Ullah, and N. Ullah, "An overview of ieee 802.15. 6 standard," in *2010 3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL 2010)*. IEEE, 2010, pp. 1–6.

[5] S. Ullah, M. Mohaisen, and M. A. Alnuem, "A review of ieee 802.15. 6 mac, phy, and security specifications," *International Journal of Distributed Sensor Networks*, vol. 9, no. 4, p. 950704, 2013.

[6] A. Nabila *et al.*, "A qos based comparative analysis of the ieee standards 802.15. 4 & 802.15. 6 in wban-based healthcare monitoring systems," in *2019 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS)*. IEEE, 2019, pp. 1–5.

[7] A. Toumanari, R. Latif *et al.*, "Performance analysis of ieee 802.15. 6 and ieee 802.15. 4 for wireless body sensor networks," in *2014 International Conference on Multimedia Computing and Systems (ICMCS)*. IEEE, 2014, pp. 910–915.

[8] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," *IEEE Wireless communications*, vol. 17, no. 1, pp. 51–58, 2010.