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—Da fare
Index Terms—Da mettere???

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 of these kind of communications, that have 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 (WBAN) 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 date. Since these router nodes are intended to be placed around the wearer, the sensor nodes dont need to cover wide ranges, averaging around 2 m. 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. Some of the main differences between WBANs and conventional sensor networks are listed in Table I:

In this paper we will discuss some of WBAN most promising applications. Then we will discuss the different standards that have already been set for this kind of networks and finally well give an overview of the challenges these network pose. (AGGIUNGI RIFEWRIMENTI ALLE SEZIONI).

II. WBAN APPLICATIONS AND DEVICES

The employment of Wireless Body Area Network was mainly focused on medical field, nevertheless in the last years, from these discoveries, have been introduced some innovations in non-medical fields too.

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

The most common application of this technology is for healthcare, where WBAN is used to collect biomedical signals monitoring patients with health problems remotely and continually. Knowing the patient's history 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 thanks to wearable applications (e.g. ECG); instead implanted applications are used to monitor more particular diseases (e.g. diabetes, cancer) implanting them under the skin or in the stream of blood.
The non-medical fields in which WBAN is recently taking place are 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, and detect life threatening situations in military context. Entertainment environment use WBAN for different purposes compared to the other, for example to register body motions of actors during the making of a film.
There are three classes of devices that constitute WBAN and allow its applications: wireless sensor node, actuators and wireless personal device. 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, Personal
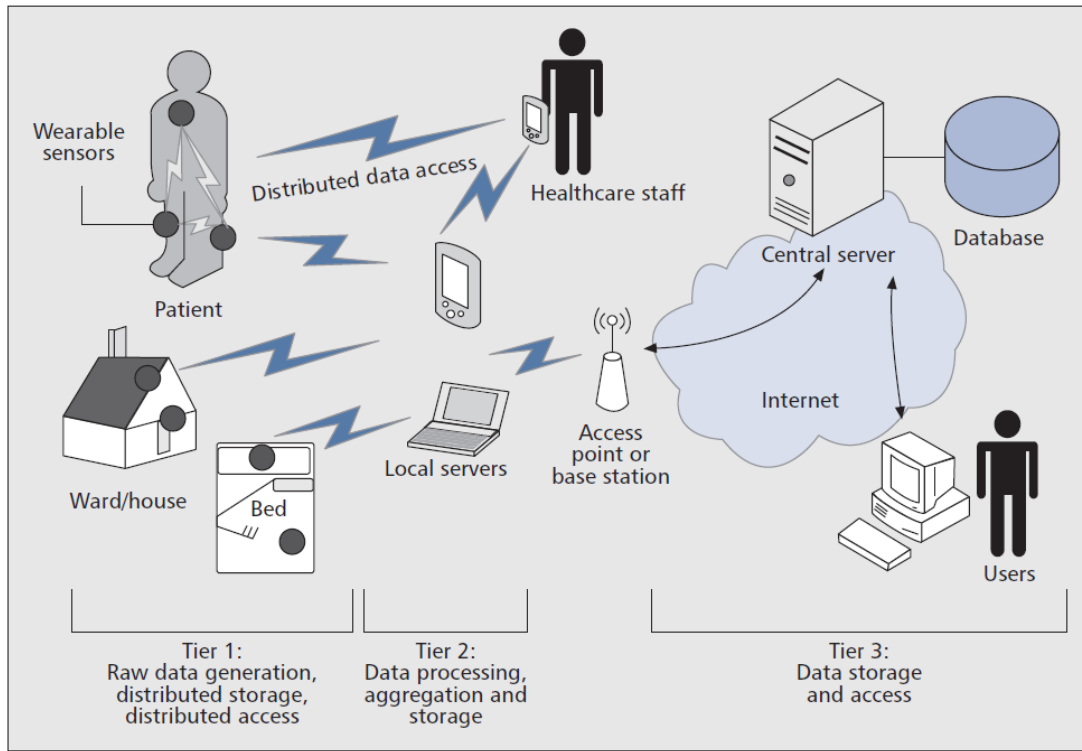
Fig. 1. A general architecture of the WBAN

Device (PD) is the device responsible for the communication between sensors, actuators and cellular phone through wireless connection. [1]

III. WBAN STANDARDS

Two are the most known standards created as solution for Wireless Body Area Networks. The former standard 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 latter, instead, is IEEE 802.15.6 and was born in 2007 with the purpose of to be a good solution for the WBAN from the beginning. Its final version was published in 2012 and nowadays is the most widely standard used 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 considered devices that consume minimal power in a WPAN and can cover an area of 10 meters. Each device represents a node in the network that could have two possible roles during the communications: be a coordinator node, with specific tasks to fulfill, or a simple node that receive information. This structure allowed MAC layer to operate in two different mode, 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). In the beacon-enabled mode there is a coordinator node that periodically transmits a beacon, so 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 superframe. The remaining part of superframe is called Contention Access Period (CAP) and is used for data transmission. Moreover, coordinator could reserve some slots after CAP in the superframe, called Guaranteed Time Slots (GTS), assigned to devices that have to run their applications without the contention with other devices.These slots form the CFP. [fig. ?]. In beacon-less mode instead no one superframe is defined because there is not any transmission of beacon for the synchronization; only random access is available and for this reason no one GTS slot could be reserved. It implies the use of an unslotted version of CSMA-CA before the transmission of data. Device that want to send data has to pick a random backoff delay and when it expires device has to perform a clear channel assessment (CCA): listen if the channel is idle and transmit or pick a new backoff delay to try again the transaction later.
A slotted CSMA-CA version is instead used in beacon-enabled networks for a correct synchronization. In this case when the device performs a CCA, after the random backoff delay, if channel is idle, device decides to repeat the CCA for a number of backoff units in according to the value of the contention

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

Both slottend and unslotted CSMA-CA algorithms are used only for data transaction, not for beacon frames, acknowledgment or CFP transmissions and define a maximum number of backoffs that could fail before to declare the channel inaccessible.

In beacon-enabled mode exists two type of data transactions: from coordinator to devices or vice versa. In the former, when the coordinator inform the device target of the data through beacon, the receiver reply that is ready sending a request to coordinator (using slotted CSMA-CA); coordinator can now select a free slot to start the transmission. In the latter case, when the coordinator receive data from device, in a similar way explained above, it could confirm the successful reception sending back an acknowledgment [PAPER 3].

B. IEEE 802.15.6

Several years later started the definition of this new standardization of WBAN to optimize the low-power nodes that handle the applications.

This standard defines a MAC layer that supports three operational PHYs layers responsible for the activation/deactivation of the radio transceiver, clear channel assessment and data reception/transmission. Ultra Wideband (UWB) and Human Body Commmunications (HBC) are mandatory PHY, instead Narrowband (NB) is an optional one. Describe each one briefly.

Narrowband PHY. It defines the Physical Protocol Data Unit (PPDU) frame that includes three components (fig. ?):

- Physical Layer Convergence Procedure (PLCP) preamble is composed of two sequences; the former used for coarse time synchronization, carrier-offset recovery and packet detection, the latter instead used for fine time synchronization.
- PLCP header contains a PHY header, with several fields useful to convey information for a successful decoding made by receiver, and some parity check bits used for error detection and error correction of PHY header.
- Physical-layer Service Data Unit (PSDU) transmitted 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 convey information (about the data rate of the PSDU and length of payload) useful to receiver to decode the PSDU, third part that define the frame, similar to Narrowband one. However about the operation mode used changes the disposition of

parity check bits for error correction of MAC frame body.
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, preamble sequence is transmitted four times to ensure packet synchronization, while SFD is transmitted once.

As the previous standard, this works with nodes organized into one-or-two-hop star WBANs and an hub (or coordinator) that controls the entire operation. For MAC layer, standard define a channel division into beacon periods (also called superframes) of equal length. Hub transmits beacon to define its boundaries and allocate the slots that are used for data transmission. Generally hub transmits beacon in each superframe that are active, but 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. MAC Header include a control field that controls information about the frame, 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 to assess the freshness, authenticity and integrity of the message [fig. ???].

IEEE 802.15.6 supports three different communication mode: Beacon Mode with Superframe Boundaries, Nonbeacon Mode with and without Superframe Boundaries. In the first mode 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 a Managed Access Phase (MAP or TypeI/II phase) used for scheduled/unscheduled bilink allocations, scheduled uplink and downlink allocations using polling. When superframe boundaries are defined in non beacon mode the hub operates during the MAP period only, in the other case instead hub provides only unscheduled Type II polled allocation.

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 obtain scheduled uplink, downlink and bilink allocations, useful to send management and data frames to and from hub respectively.

C. Comparison between WBAN standards

DA FARE

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, 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 easier to replace in devices situated outside the human bodies, remote battery recharging becomes not-negotiable for devises implemented directly into 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, it may need to exchange data between them. The setting of common standards may greatly help with device compatibility.

E. Privacy and Security issues

Security may be the greatest challenge for WBAN and its required by the data exchanged. Since WBANs deal with very personal information, there is the strong need to ensure data privacy and a reliable authentication in the whole data transfer process. Not only this, data 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 NUMERO UNO gives an overview on all the different security issues involved when dealing with WLANs, 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. 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 allowing flexible access to qualified , legitimate, medical staff. There has been some research in this regards VEDI NOTA PAPER 01 CODE BLUE.
- 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 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 through 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 in 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, 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] 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.