Ad Hoc Networks 42 (2016) 1–18

Contents lists available at ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

A Priority based Cross Layer Routing Protocol for healthcare applications

Hadda Ben Elhadj [a,*], Jocelyne Elias [b], Lamia Chaari [a], Lotfi Kamoun [a]

[a] LETI Laboratory, Sfax University, Tunisia
[b] LIPADE Laboratory, Université Paris Descartes – Sorbonne Paris Cité, 75006 Paris, France

ARTICLE INFO

Article history:
Received 28 February 2015
Revised 9 October 2015
Accepted 20 October 2015
Available online 2 November 2015

Keywords:
Wireless Body Area Networks
Healthcare
QoS
MAC
Cross layer
Routing

ABSTRACT

Wireless body area networks (WBANs) represent one of the most promising approaches for improving the quality of life, allowing remote patient monitoring and other healthcare applications. Data dissemination and medium access in a WBAN are critical issues that impact the network reliability, the efficiency and the total energy consumed by the network. In this paper, we propose a Priority-based Cross Layer Routing Protocol (PCLRP) along with a Priority Cross Layer Medium Access Channel protocol (PCLMAC) for healthcare applications.

PCLRP combined with PCLMAC ensures reliable traffic dissemination and customized channel access for intra- and inter-body communications. Simulation results show that the proposed protocol achieves customized quality of services and outperforms state of the art existing protocols in terms of power consumption, packet delivery ratio and delay.

1. Introduction

The increase in average lifespan and health costs along with the advances in miniaturization of electronic devices, sensing, battery and wireless communication technologies have led to the development of wireless body area networks (WBANs). In the health field, a WBAN consists of a set of medical sensors (i.e., ECG, EEG) and a coordinator (personal digital assistant (PDA) or a smart phone) implanted in or on the user's body [1–4]. These devices aim to collect, store and process patient's physiological parameters and provide him ubiquitous healthcare services. Due to their specific properties such as small size, data rate, reliability, security, mobility, power constraint, QoS requirements, and heterogeneous traffic, WBANs require special protocols design to meet their particular needs. In other words, although WBANs derive somehow from WSNs, there are intrinsic differences between these two networks (which are summarized in Table 1).

Ever since WBANs have emerged, different optimization schemes have been proposed to overcome the above challenging issues.

Cross-layer approaches have proven to provide better WBAN optimization results than their layered counterparts [7]. Indeed, layer cooperation in cross-layer based schemes well enhances the overall WBAN performance. For instance, in a cross-layer scheme, the QoS requirements at the application layer can be communicated to the MAC layer in order to achieve better resource allocation for the running healthcare application. Furthermore, the channel state information and battery level can be fed to the network layer to avoid paths including channels in a bad state or depleted nodes.

The great number of proposed WBAN cross-layer approaches (reviewed in Section 2) proves that there is still a need for further optimization of such networks, and that cross-layering is efficient to accomplish that. From this point of view, this paper presents a Priority based Cross Layer Routing Protocol for healthcare applications, named PCLRP. PCLRP is an adaptive protocol in the sense of slot assignment

* Corresponding author. Tel.: +21625369105.
E-mail addresses: Hadda.lbnelhadj@esti.rnu.tn (H. Ben Elhadj), jocelyne.elias@parisdescartes.fr (J. Elias), lamia.chaari@enis.rnu.tn (L. Chaari), Lotif.kamoun@isecs.rnu.tn (L. Kamoun).

http://dx.doi.org/10.1016/j.adhoc.2015.10.007
1570-8705/

Table 1
Comparison between WSNs and WBANs [5,6].

Challenges	WSN	WBAN
Scale	Monitored environment (m/km)	Human body (cm/m)
Node number	Many redundant nodes for wide area coverage	Fewer, limited in space
Node tasks	A node performs a dedicated task	A node performs multiple tasks
Node size	Preferred small, but not important	To be small is essential
Network topology	Very likely to be fixed and static	More variable due to body movement
Data rates	Homogeneous	Heterogeneous
Node replacement	Performed easily, nodes may be even disposable	Difficult (implanted nodes)
Node lifetime	Several months/years	Several months/years
Path loss	medium (free space)	important
Energy scavenging source	Most likely solar and wind power	Most likely motion (vibration) and thermal (body heat)
Biocompatibility	Not a consideration in most applications	A must for implants and on-body sensors
Security level	Lower	Higher, to protect data of patient
Impact of data loss	May be compensated by redundant nodes	More significant, may require additional measures to ensure QoS and real-time data delivery
Wireless technology	Bluetooth, Zigbee, GPRS, WLAN, ...	Low power technology (i.e., Bluetooth low energy)

techniques, sleep and wakeup mechanisms in face of topology changes. Moreover, it combines TDMA and priority guaranteed CSMA/CA approaches to access the channel and well defines a synchronization scheme to avoid collisions, data loss and idle listening. Furthermore, PCLRP handles WBAN traffic heterogeneity by defining three traffic classes:

- General Monitoring packets for ordinary Medical data;
- Delay Sensitive packets for High-priority medical data;
- Emergency packets for critical medical data.

PCLRP further ensures resource allocation and route selection in compliance with the heterogeneous QoS requirements of such traffic classes. In fact, as a key innovative feature, in this work we investigate the channel access issue both for intra and inter body communications with a clear differentiation between multiple traffic types with respect to their QoS requirements. This paper is a significant extension of existing WBAN MAC protocols in which the TDMA slots allocation is restricted to intra body nodes. More specifically, to ensure more reliability and collision avoidance, the PCLMAC superframe contains a Contention Free Period (CFP) customized for inter WBAN cooperation.

In summary, our paper makes the following key contributions:

- We define a set of healthcare monitoring applications (or traffic categories) to represent general monitoring traffic data, high priority and emergency data.
- To give meaning to the traffic classification, we propose a Priority Cross Layer Medium Access Channel protocol, PCLMAC, which operates in compliance with the defined traffic categories.
- We further propose an intra-body and extra-body routing protocols that operate in cooperation with the defined PCLMAC protocol.
- We perform a thorough performance comparison between our proposed approach and the Wireless Autonomous Spanning tree Protocol (WASP) for multi-hop wireless body area networks [8] and Data centric Multi objective QoS-aware routing protocol (DMQoS) for body sensor networks [9]. Numerical results show that PCLRP is indeed effective, since it significantly saves energy and ensures high reliability.

The paper is structured as follows: Section 2 discusses related work. Section 3 introduces our WBAN network model and traffic categories. In Section 4 we present our PCLRP approach, while we illustrate and discuss numerical results that show the efficiency of our proposal in Section 5. Finally, Section 6 concludes this paper and presents some future works.

2. Related work

Several works have appeared in the literature with the purpose of ensuring efficient routing and enhancing the QoS of WSNs [10,11]. Nevertheless, as mentioned in Table 1 the specificity of the operating environment and treated data make WBANs unique and require specific protocol design. In brief, WSNs protocols will not work as efficiently as the protocols specifically designed for WBANs. In this section, we survey some relevant ones that are tightly related to our work.

WBAN cross-layer protocol design is an emergent research area that aims to deliver greater efficiencies than single layer adaptation schemes [7]. We highlight the proposed cross-layer routing protocols for integration in WBAN systems.

Generally, cross-layer schemes may be either loosely coupled or tightly coupled designed. Loosely coupled protocol designs focus on communicating the lower layers available parameters to upper layers and/or coupling the functionalities of some adjacent layers in order to ensure overall network performance. Accordingly, in the loosely coupled approach the individual layers within the protocol

stack remain, but parameters exchange is not limited to adjacent layers. In the tightly coupled approach, different layers are optimized together to form one complete optimized solution. This latter approach may better get rid of stack communication overhead than the loosely coupled one, but this may be at the expense of protocol transparency and maintenance. Consequently, the most commonly proposed WBAN cross-layer protocols are loosely coupled schemes [12]. Authors in [13] have proposed a cross-layer solution for critical data delivery applications that combines APTEEN [14] and GinMAC [15] protocols with new features, such as multi-hops and mobility modules. Hence, the cluster heads selection technique used in [13] is that of APTEEN.

APTEEN operates in two phases, cluster setup phase and data transfer phase. In the cluster set up phase, cluster heads election and cluster member formation are done using the same algorithm used in LEACH [17]. Then, each cluster head broadcasts an advertisement message to the entire network including a Hard Threshold (HT) and a Soft Threshold (ST) attributes. That is, data transmissions take place only when actual sensed data is greater or equal to HT or changes by an amount greater or equal to ST compared to the previous sent value. Most operations that need to be made in [13] are taken from APTEEN, such as selecting forwarding routes and connection, and mobility management. Therewith, GinMAC follows the information given by APTEEN and then just confirms that data is forwarded to a next hop over a single hop communication. It uses the TDMA protocol to ensure that data is delivered to the sink in a timely and reliable manner. In fact, a TDMA schedule for each cluster is determined. Moreover, clusters, formed by APTEEN, operate on different transmission frequencies to accommodate a large number of nodes.

Although the protocol ensures mobility awareness, it suffers from complexity of cluster construction at different levels and overlooking traffic differentiation.

Ruzzelli et al. [16] and Latre et al. [18] incorporate a closely coupled interaction between the MAC and the network layers. It is a mechanism wherein the MAC slot allocation is customized for the underlying routing tree, thereby providing routing-specific energy economy at the MAC layer. Also, these proposals handle body mobility by adaptively reconstructing and maintaining the tree topology used for packet routing. However, traffic differentiation and scheduling are overlooked.

WASP [8] is a slotted spanning tree based cross-layer protocol. WASP time axis is divided into contention free and contention based slots, grouped in cycles, which are assigned to nodes in a distributed way. In a WASP-cycle, each node is allowed to send its data and/or to forward data received in the previous cycle to the next node. At the beginning of each cycle, the sink broadcasts a scheme message called WASP-scheme to inform its children when they can send their data. These children respond by sending out their own WASP-scheme in their designated time slots [8]. Whereas, WASP overlooks traffic heterogeneity, node mobility and node synchronization.

Although, authors in [19,20] have treated WBAN heterogeneity, these proposals, which are based on the IEEE 802.15.6 standard, suffer from high energy consumption due to idle listening.

DMQoS [9] is a modular QoS based protocol. It sets up a modular architecture wherein different modules coordinate with each other to provide QoS preferment services. DMQoS classifies data packets into four main categories: ordinary, critical, delay driven and reliability driven packets. The routings of delay critical and reliability critical packets are handled separately by employing independent modules for each, whereas for the most critical packets having both stringent delay and reliability constraints, the corresponding modules operate in coordination to guarantee the required service. While in [9] the delay control module chooses the next-hop router node offering higher velocity of data packets, the reliability control module injects minimal redundant information by exploiting high reliability links. To ensure reliability, DMQoS duplicates transmitted data packets, which leads to energy consumption and interference increase.

In order to mitigate packet losses, Gaudadri and Baheti [21] propose a cross-layer scheme based on application and MAC layer interactions. They focus on treating the issues of end-to-end packet losses due to link deterioration, interference, congestion and system load. The packet loss mitigation approach is based on the emerging signal processing concept, the compressed sensing, wherein significantly few sensor measurements can be used to recover signals with arbitrarily fine resolution. Lost packets are identified at the application layer via a sequence number field in the packet header of the lower layers. However, authors have not considered neither traffic heterogeneity nor node synchronization. The main characteristics of WBAN cross-layer protocols, previously reviewed, are summarized in Table 2.

Despite the fact that many of these proposed techniques look promising, there are still many challenges that need to be solved. From this point of view, we propose in the next section a cross-layer protocol that takes advantage of strengths and cope with weaknesses of previous cited proposals. In other terms, a protocol that ensures energy efficiency, traffic differentiation at the channel access and routing levels, reliability, node synchronization and mobility awareness. This may be achieved via different layer cooperation that limits idle listening, overhearing, collisions and interference.

3. Network model and traffic categories

This work focuses on remote healthcare monitoring systems, which are one of the most promising healthcare applications. In this section, we introduce our healthcare network model as well as the proposed traffic categorization in this latter domain.

3.1. Network model

In our network model, we consider a set of mobile personal WBANs (e-health users) denoted by $\mathcal{P}$ and a set of WiFi gateways ($\mathcal{G}$). Each personal WBAN ($p \in \mathcal{P}$) aims to ubiquitously disseminate its collected data to the e-health staff (doctor, nurse, emergency car, and so on.) via a gateway ($g \in \mathcal{G}$). Typically, each p is composed of a set of body implant and wearable sensors called *children*, and a central

Table 2
Characteristics of WBAN cross-layer protocol proposals.

Protocol	Energy efficiency	Traffic heterogeneity	Channel access scheme	Node synchronization	Mobility
[13]	Low	Yes	Yes	No	Yes
TICOSS [16]	Good	No	No	No	Yes
CICADA [18]	Medium	No	Yes	No	Yes
WASP [8]	Good	No	Yes	No	No
DMQoS [9]	Medium	Yes	No	No	Yes
[19]	Medium	Yes	No	No	Yes
NME and HME [20]	Medium	Yes	No	No	Yes
[21]	Good	No	No	No	No

device known as the *Coordinator* (C) ∗∗which may be a smart phone or a personal digital assistant (PDA). In *p*, children nodes send their collected data to C. In fact, C is computationally more powerful (in terms of energy, communication range, memory) than its sensors and behaves as a router in *p*. It is responsible for disseminating the data collected by its children to the medical staff, and precisely to the suitable *g* as a first destination.

C is equipped with multiple radio interfaces (e.g., ZigBee for communication with sensors, WiFi, 3G ...for Internet connection) to allow multiple overlapping transmissions [22]. In other words, as it supports multi-radio communications, *C* allows the WBAN to send and receive data simultaneously.

Hence, we may infer that each WBAN *p* may be considered as a cluster wherein C is by default its cluster head and its cluster members are the set of its children nodes. Conventionally, clustering protocols distinguish themselves by how they elect cluster heads. However, in a personal WBAN there is no election process and usually *C* is pre-designed as a cluster head. Note that in some cases the communication between C and gateway *g* cannot be one hop and needs to pass through another C of a neighbour *p*. Consequently, each C may be both a *relayed* and/or a *relaying* coordinator. We note by a relayed C, a coordinator that communicates with a *g* through another C, while a relaying C is a Coordinator through which another C communicates with a *g*. In view of this, the communication in our network model is classified in intra-body communication and extra-body communication. The extra-body communication involves the inter-WBAN communication as well as the communication between the coordinators and gateways. While, the intra-body one refers to the communication between *p*'s sensor nodes and C. Moreover, intra-body cooperation is required in some cases. Therefore, to communicate with their C, some sensors require the relaying service of their neighbouring sensors belonging to the same *p*. We note that a sensor node cannot communicate with any coordinator or sensor belonging to another *p*. To recapitulate, our network model is multi-hop cluster based. Fig. 1 represents an overview of our described network model.

3.2. Traffic categories and packet classification

Unlike conventional WSNs, each sensor node in a WBAN has its own requirements in terms of delay and data rate [23]. Table 3 shows the heterogeneous characteristics of some commonly used medical sensors.

Table 3
Delay and bit rate requirements of healthcare data [23].

Data source	Bit rate (bps)	Delay (s)	Sampling rate (Hz)
Electrocardiogram	10–100k	< 10	63–500
Blood pressure	10–30	> 120	63
Non-invasive cuff	0.05	30–120	0.025
Cardiac output	1k	< 10	63
CO_2 concentration	1k	30–120	63
Temperature (°C)	0.3	> 120	0.02

Furthermore, collected healthcare data are of different importance. To guarantee healthcare services efficiency, it is necessary to design a system that can handle such heterogeneity with different priorities. Consequently, in our solution we suggest the following traffic differentiation paradigm. We define three classes of data packets: EMergency (EM), Delay Sensitive (DS) and General Monitoring (GM). A detailed description of these packet types as well as their priority is given in Table 4.

Note that traffic priorities may vary depending upon the values generated by the sensors. For instance, body temperature readings may produce EM traffic flows if their values exceed the normal threshold. To give meaning to the classification made, an efficient channel access as well as accurate route selection are needed. Accordingly, in the next section we propose PCLRP that operates in compliance with the defined traffic categories as well as our multi-hop cluster based network model.

4. Priority based Cross Layer Routing Protocol (PCLRP)

PCLRP incorporates a loosely coupled interaction between the application, MAC, network and physical layers. It is a mechanism wherein the MAC slot allocation is customized for the underlying routing protocols taking into account the QoS requirements of the running healthcare application and physical parameters. In fact, PCLRP exploits the exchanged MAC frames to build the routing scheme for free and without a route discovery message exchange. Moreover, the routing algorithms exploit the node's battery level and the MAC frame structure (number of TDMA slots) in the relay selection process. On the other side, the MAC superframe duration depends on the network topology (number of nodes) and the QoS requirements of the running healthcare application (EM, DS, GM).

Section 4 details the PCLRP operations along with the MAC and routing protocols that it encompasses.

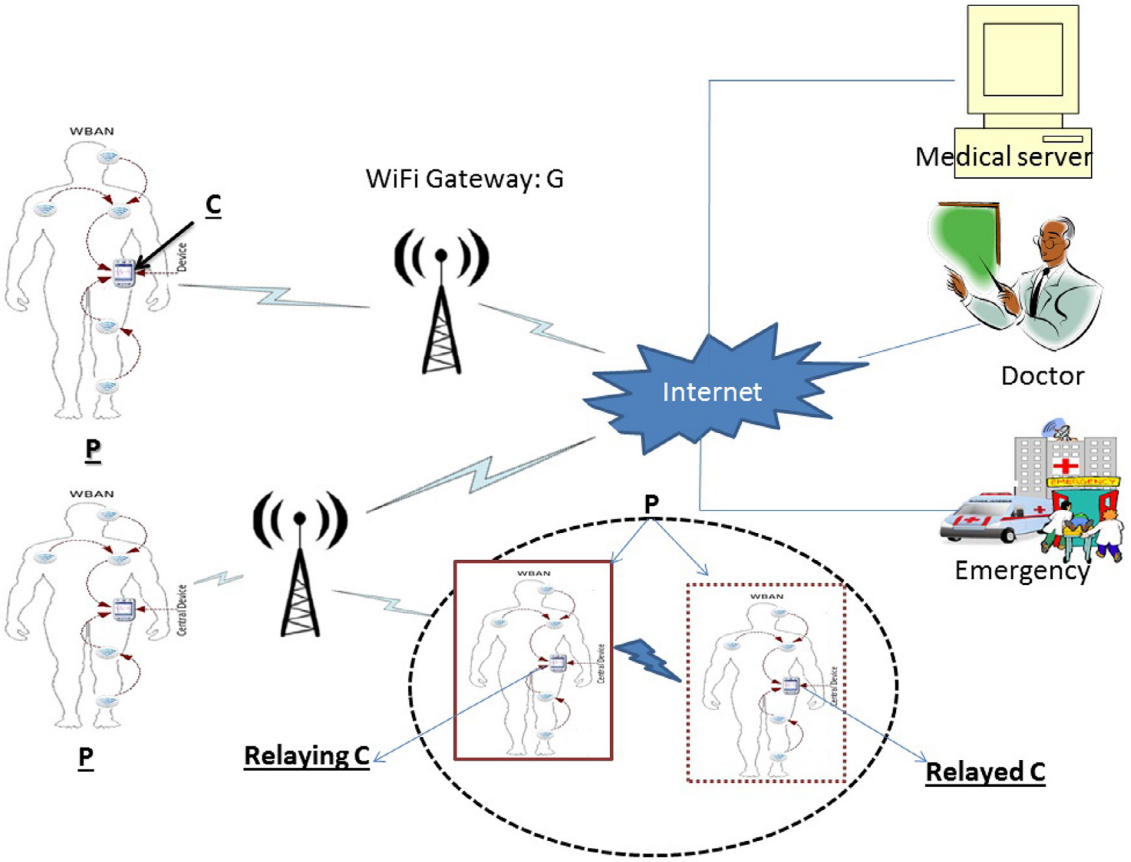


Fig. 1. Network model architecture.

Table 4
Data packets type classification and field encoding.

User priority	Packet subtype	Description
1	EM	They are the most critical data packets. They should be forwarded in a short time and reliable way. They are used to report alerts and warnings (e.g., packets reporting data values that exceed normal thresholds).
2	DS	The video traffic type defined by the standard is designed for nonmedical applications, e.g., video gaming. For this reason, we defined the DS type as the medical video type, e.g., video streaming of elderly monitoring and motion control. DS packets must be delivered in stringent deadline, while a reasonable packet loss is tolerated.
3	GM	The lowest priority is given to GM packets. They correspond to regular measurements of patient physiological parameters that typically indicate normal values.

4.1. Priority Cross Layered Medium Access Channel protocol

4.1.1. General description

The PCLMAC protocol operates in a beacon enabled mode, where beacons are transmitted at the beginning of each superframe followed by an active and an optional inactive period. All communications take place in the active period; in the inactive period, nodes are allowed to power down and conserve energy. As described above, in our network model, inter-WBAN cooperation is required in some cases. Consequently, our PCLMAC superframe structure may contain portions of time dedicated for inter-WBAN communication. Moreover, we have mentioned that C is the most powerful device in WBAN *p* and acts as a router. By analogy, C is the access channel scheduler and beacons generator in PCLMAC. Hence, as described in Fig. 2, the PCLMAC superframe consists of:

- Mandatory elements: a Beacon (B), a Children Contention Access Period (CCAP), a Children Contention Free Period (CCFP) and a DownLink period (DL).
- Optional elements: a Neighbour Contention Access period (NCAP), a Neighbour Contention-Free Period (NCFP) and an inactive period.

The active part of a superframe is divided into six main portions:

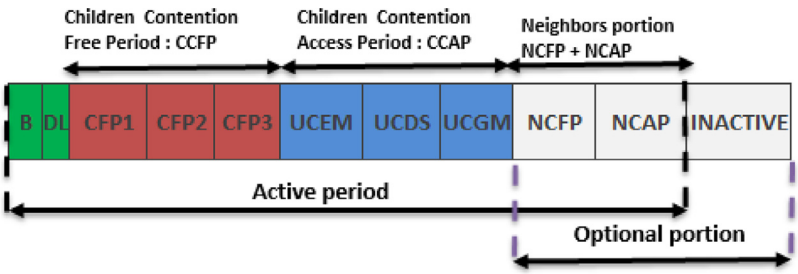


Fig. 2. Superframe structure.

- Beacon (B) is used for resource allocation information and synchronization. It also carries security codes in order to allocate resources to legitimate users.
- The Downlink (DL) is used by the C to transmit its queries and control frames to its associated cluster members.
- CCAP is used by children nodes for transmitting both control frames and pending data. In fact, new children send their join requests in the CCAP. Also, failed packets are retransmitted in this portion of time. Since traditional CSMA/CA schemes use a fixed contention window for all node types, and hence they are unsuitable for heterogeneous networks like WBANs, in CCAP we consider a priority-guaranteed CSMA/CA procedure. In fact, the CCAP is divided into three parts: Uplink Contention for EMergency traffic (UCEM), Uplink Contention for Delay Sensitive (UCDS) and Uplink Contention for General Monitoring (UCGM) traffic. During the CCAP period, nodes with emergency traffic contend for transmission throughout all the CCAP period, while multimedia nodes contend throughout both the UCDS and UCGM. Whereas, nodes with normal traffic contend for transmission only in the UCGM. Moreover, the priority-guaranteed CSMA/CA prioritizes all the nodes by using three different Inter-Fame Spaces (IFS): Emergency IFS (EMIFS), Delay Sensitive IFS (DSIFS) and the General Monitoring IFS (GMIFS) with $EMIFS < DSIFS < GMIFS$. Moreover, prioritized random back-off is applied during CCAP. Indeed, the back-off time depends on the traffic class and is randomly chosen as follows:

$$\text{backoff time} \in [0, 2^{BE+Traffic\_priority} - 1] \quad (1)$$

  where BE denotes the back-off exponent. Using the proposed Eq. (1), we guarantee that a high priority traffic has higher probability transmission opportunity.
- CCFP consists of multiple TDMA slots reserved by the coordinator's children nodes. It is composed of three sub contention free periods: CFP1: slots reserved by emergency nodes, CFP2: slots reserved by multimedia nodes, and CFP3: slots reserved by general monitoring nodes.
- NCFP is an optional period composed of TDMA slots reserved by relayed neighbour coordinators. This time is sufficient enough for sending data from relayed coordinators and receiving it by the relaying *C*.
- NCAP is used by the set of *C*'s relayed neighbours for transferring both control frames and pending data. In fact, neighbouring coordinators, aiming to relay data via the current coordinator, send their join requests in the NCAP. Failed packets are also retransmitted in this portion of time.

4.1.2. Priority guaranteed resource allocation and synchronization

As mentioned before, for resource allocation and synchronization, the coordinator continuously broadcasts beacons to all children and neighbours at the beginning of each superframe. Only active nodes are able to receive the beacons.

4.1.2.1. Synchronization. In practice, clocks in different sensor nodes suffer from random drifts, causing slot misalignment over time. They continuously keep drifting away from each other even if they initially start at the same time [24,25,27]. Consequently, if there is no synchronization among the nodes, the whole idea of time division multiplexing may not be productive. This may result in collisions and huge data loss in WBANs. One more challenge encountered is the decision about the start of the superframe and how to ensure sleep and wake up schedule accuracy to prevent messages being missed out. On the other side, when WSNs are used for critical applications, like healthcare, time stamping and a very accurate time information are an absolute requirement.

All that shows the need for clock synchronization in WBANs. In other words, for PCLMAC TDMA slot allocation to materialize, fairly good time synchronization needs to be present.

Thus, to ensure node synchronization, the PCLMAC beacon message is time stamped right before it is sent with T_0. Upon receipt of the beacon, concerned nodes timestamp the ACK message both with T_r (beacon reception time) and T_{ack} (Ack sending time). The three timestamps (T_0, T_r, T_{ack}) form a data point to compute the Guard time $\mathcal{GT}$ [27]. Hence, to ensure slot alignment, first the coordinator computes the maximum clock skew in its field [28]. Let $S = \{S_1, \ldots, S_n\}$ be both the set of all its children nodes and the list of its relayed coordinators C. The clock skew between S_i and C, denoted by δ_i is defined to be the difference between the clocks of C and S_i. Using the previous timestamps, a node S_i computes the δ_i as follows:

$$\delta_i = T_r - T_0 - T_b \quad (2)$$

While C computes the δ_i as below:

$$\delta_i = T_{ack} - T_0 - T_b \quad (3)$$

with

$$T_b = \frac{B_{data} + Ov}{D} \quad (4)$$

Table 5
Notations and definitions.

BI	Beacon interval
T_b	Beacon transmission time
T_0	Beacon message sending time
T_r	Beacon message reception time
S	C's cluster members (children and relayed C)
B_{data}	Beacon sampled bits
Ov	Overhead bits
D	Communication data rate
δ	Maximum clock skew
δ_i	Clock skew between node i and coordinator C
$slot_d$	Slot duration
$\mathcal{GT}$	Guard time
DLD	Down Link Duration
P_{data}	Sampled data bits
CFP	Contention Free Period intended for reservation
Ack	Acknowledgement bits
ASD	Active Superframe Duration
$CCAP$	Children Contention Access Period
$CCAP\_min$	Minimal CAP period (used by neighbour nodes)
$NCAP$	Neighbour Contention Access Period
A_NCFP	Number of slots intended for neighbour reservation
$NCAP\_min$	Minimal Neighbour Contention Access Period
NAS	Number of Slots that a node aims to book
TCF	Turned around Calibration Factor
Sec_i	Confidence level of gateway i ($Sec_i \in \{1, 0.75, 0.5, 0\}$)
RTT_i	RTT evaluation value of gateway i
Dir	Evaluation of the patient movement vs the gateway position
α	The security weighting coefficient
β	The RTT weighting coefficient
γ	The direction weighting coefficient
λ	The MF coefficient
σ	The RH coefficient
NB_needed_Slots	The number of slots needed by a relayed C
NB_free	Number of free slots that a relaying C may provide for its neighbour C
$AVG\_Walking\_speed$	The average walking speed of a patient (m/s)
WT	The walking period(s)
g_prob	Probability to encounter a g each walked meter

where B_{data} and Ov are the beacon sampled and overhead bits, and D is the data rate.

The basic notation used in this paper is summarized in Table 5.

We note here that each node measures only its own δ_i while the cluster head C computes the δ_i of each associated node to obtain δ, which is expressed as below:

$$\forall S_i \in S; \delta = \text{Max}|\delta_i| \tag{5}$$

In order to prevent possible TDMA slot overlap, the coordinator $\mathcal{C}$ uses the δ as the guard time to be inserted into each slot duration. In contrast, all $S_i, \forall i$, make use of δ_i to settle their wake up and sleep timers. The $\mathcal{GT}$ can be defined as the time duration in a slot, in which the packet transmission is not carried out to account for any collision due to clock errors [25]. To negate the possible interference effects of slowest and fastest clocked nodes having adjacent CFP slots, the $\mathcal{GT}$ is fairly two divided and inserted in the either sides of the transmission duration in each TDMA slot. The PCLMAC slot structure is as presented in Fig. 3.

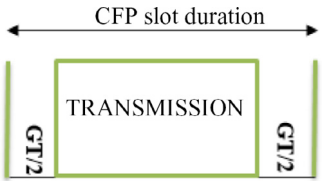


Fig. 3. PCLMAC slot structure.

The idea behind using δ as $\mathcal{GT}$ is to handle the maximum possible clock drifts between any two nodes. Moreover, even $\mathcal{GT}$ is chosen as the worst case, nodes are settling their clocks over time and may be converging towards a more uniform clock. In fact, nodes continuously settle their clocks according to the coordinator's clock using the beacon time stamping. Further, using a dynamic guard time tolerates node failures, adopts newly joint nodes to the network and accommodates clock drifts caused by environmental factors, which are time-varying [26]. The proposed synchronization scheme achieves synchronization and resynchronization for free, without any explicit synchronization message exchange.

The PCLMAC protocol allows low duty cycle children nodes to remain in sleep mode and save their energy (consumed by beacon overhearing).

4.1.2.2. Active superframe calculation. The Active Superframe Duration (ASD) is composed of five main portions: DL, CCFP, CCAP, NCFP, and NCAP. The duration of these different portions is flexible and may vary from one superframe to another. It depends on nodes traffic and events variation. Hereafter, we detail how the cluster head C performs the time assignment of each cited portion.

The ASD contains a fixed minimal CCAP duration denoted by CCAP_min. CCAP_min is used to guarantee that new and disconnected children nodes may contend to join their cluster heads. Moreover, if the coordinator is acting as a relay, it specifies also a fixed minimal NCAP for neighbour contention (NCAP_min). The existence of DL depends on the fact that the coordinator has data to transmit to its members or not. That is, the DL Duration (DLD) may be equal to zero.

For TDMA slots reservation:

- first, C computes CFP as follows:

$$CFP = ASD - CCAP\_min - NCAP\_min - DLD \tag{6}$$

- Second, it computes the maximum number of TDMA slots (NB_S) that may be reserved.

$$NB\_S = \frac{CFP}{slot\_d} \tag{7}$$

with

$$slot\_d = \delta + \frac{P\_data + Ov + Ack}{D} \tag{8}$$

Having determined the NB_S, C may manage the reservation requests of its children as well as of its relayed coordinators. In fact, aiming to limit network overhead and collisions,

unlike the state of the art existing protocols, CFP slot reservation is done without sending slot allocation queries in the CAP. Specifically, a node makes a request for CFP slots from the cluster head by setting a Number of Asked Slots (NAS) flag in its transmitted frame. Obviously, this flag is set to zero if the node is not intended to perform a reservation. The cluster head replies with an acknowledgement that contains the number of the granted slots. Consequently, the reservation for next data transmissions is performed within current data transmission and no additional signalling is required.

The coordinator assigns slots according to their availability and the order of requests arrival. What is evident is that, to sustain the health of patient, each coordinator serves its children first. This may be explained by the fact that, a small loss of collected information may be devastating for the patient's life. Moreover, most of healthcare applications are costly and it is mandatory that we manage our resources effectively. Another important point, there is a risk that the neighbour *C* is a malicious node that intends to deteriorate the relaying C's resources. Accordingly, *C* provides its children all the slots they ask, then if there remain slots, it serves its neighbours (relayed C).

Let A_NCFP denotes the number of slots intended for neighbour reservation. A_NCFP is obtained as follows:

$$A\_NCFP = NB\_S - CCFP \tag{9}$$

We mention that the number of total slots that are effectively reserved may be less than *NB_S*. Hence, the remained duration will be two divided and added to the CAP portions. In fact the CCAP and NCAP periods are computed, respectively, as follows:

$$CCAP = \frac{(A\_NCFP - NCFP) \times slot_d}{2} + CCAP_{min} \tag{10}$$

$$NCAP = \frac{(A\_NCFP - NCFP) \times slot_d}{2} + NCAP_{min} \tag{11}$$

For more details, we present, respectively, in Algorithm 1 and Algorithm 2 the pseudocodes of PLCMAC protocol at the coordinator and at the children sides (at each $node_i$ side).

Algorithm 1 Algorithm executed by coordinator C.

```
// Start of superframe
// synch_t: synchronization time
CFP = ASD − DLD − CCAP_min − NCAP_min
NB_S = CFP / slot_d
Next_frame_start = current_time + synch_t + T_b
∀ received_Ack_i;  δ_i = T_ack − T_0 − T_b
broadcast Beacon_new
for i = 1 to N
    δ = Max|δ_i|
end
if (DL_d > 0)
    send data to nodes
end if
if (receive (data_node_i , and data.NAS > 0)
    if (NB_S)
      if (NB_S >= data.NAS)
        NB_S− = data.NAS
      else
        NB_S = 0
      end if
      switch node_type:
        case EM: add CFF1 slots
        case DS: add CFF2 slots
        case GM: add CFF3 slots
        case Relayed C: add NCFP slots
      end
      send (ACK,node_i)
      end if
      else
        discard request
   end if
if (CAP and receive(sleep_request_node_i , NB_slots))
    if (node_i is allowed to sleep)
      send (ACK,node_i)
    else
      discard request
    end if
end if
if (CFP1 or CFP2 or CFP3 or NCFP)
    keep listening to receive data
if (inactive period starts)
    go to sleep and wake up at Next_frame_start
CCAP = CCAP_min + (NB_S/2) * slot_d
NCAP = NCAP_min + (NB_S/2) * slot_d
```

4.2. Routing establishment phase

Our network model is a distributed mobile public-BAN where intra and inter WBAN cooperations are required. In next subsections we detail the intra and extra routing paths establishment procedures.

4.2.1. Intra-body routing

Since in healthcare applications biosensors are deployed on the human body, which is a very lossy medium for propagated waves, the propagation loss around the human body is high. Consequently, using relay nodes becomes advantageous and sometimes even an absolute requirement to ensure connectivity of the network [29]. On the other hand, WBAN networks are small in size. Indeed, in the worst case intra-body communication will be two hops. Hence, we assume that the topology is a two-hop extended star BAN topology. As our approach is cross-layer, in our topology setup and routing paths establishment we make use of the described PLCMAC Beacon exchange. Therefore, when a coordinator C is switched on for the first time, it generates a PLCMAC beacon message and diffuses it to the whole network. As previously mentioned in the PLCMAC description, upon beacon receipt, children nodes respond by a time stamped ACK. Knowing that we mean by a *relay capable node* a child node that has a good battery level and is directly connected to C. More than time stamps, the ACK contains a boolean flag called R that indicates if the node is a relay capable or not. This flag is used in the topology extension procedure. In fact, upon their deployment, children nodes wait for beacon reception to join C. They keep listening for a beacon timeout period. Upon this period, children that have not received the beacon send join requests to their closer relay capable nodes. Relay nodes are chosen according to the Received Signal Strength Indicator (RSSI) and δ values. The use of δ helps a node to choose the relay with which is more synchronized. Algorithm 3 describes the pseudocode of our intra-body routing algorithm.

4.2.2. Extra-body routing

As described in our network model, the extra-body communication involves inter-WBAN communication as well as

Algorithm 2 Algorithm executed by a child node.

```
// Start of superframe
wake up to receive beacon
if (receive(Beacon))
    δ_i = T_r − T_0 − T_b
    Next_frame_start = current_time + δ_i
    if (DLD > 0 and there is data to me)
    // node will receive data from the coordinator
      keep listening
    else
      go to sleep
    end if
    if (its reserved_slot > 0)
      wake up when its reserved_slots starts
      set data.NAS = NAS
      send data
      go to sleep when its reserved_slots ends
    end if
    end if
    if ((CCAP starts || NCAP starts) & (∃ data or sleep_request to send
|| Not connected)
// nodes wake up to contend for slot reservation request, sleep request
and/or data transmission
      switch node_type:
        case EM: wake up
        case DS: keep sleeping and wake up when UCDS starts
        case GM: keep sleeping and wake up when UCGM starts
      end
    end if
    if (inactive period starts)
      go to sleep and wake up at Next_frame_start
    end if
else if(Beacon timeout)
    NB_lost_beacons++
    if(NB_lost_beacons > max)
// max is maximum authorized number of beacons that a node can loose
      Keep listening to find a relay node
    else
      go to sleep and wake up at Next_frame_start
    end if
end if
```

Algorithm 3 Intra-body routing algorithm.

```
if (Recv(Beacon_new, node_j))
// child node_j receives new beacon from C
    if (next_hop == NULL)
      next_hop = coordinator_id
    end if
  else if (beacon_timeout and next_hop == NULL)
    // node does not receive a beacon from the coordinator: not in its
communication range
      ∀ listened ACK_node_i−>coordinator
      if ((new ACKi.R == true) and RSSI (new ACK_i) > RSSI (last ACKi))
        Next_hop = sender of (new ACK_i)
      else if ((new ACKi.R == true) and RSSI (new ACK_i) == RSSI (last
ACKi))
        Node_j computes the clock skew δ VS node_i
        Chooses the node having the smallest δ
      end if
end if
```

the communication between the coordinators and WiFi gateways. Our extra-body routing algorithm consists of two distinct and cooperating parts:

- WiFi gateways selection
- WBAN relay selection (for inter WBAN communication)

4.2.2.1. WiFi gateways selection algorithm. The selection policy often used by mobile terminals for automatically selecting an access point, simply consists of scanning APs and then chooses the unencrypted one with the highest signal strength. This policy ignores important factors that impact on the obtained QoS, since it does not take into account the network load that nearby APs have, or security problems that may exist. This can result in unbalanced load on some APs, leading to low data throughput and an unsatisfactory network performance. Consequently, to cope with these shortcomings, we consider and describe in detail the following key parameters (Round Trip Time, Patient direction, Gateway confidence level):

Table 6
RTT evaluation values.

Obtained RTT	Corresponding value
$RTT \geq Max\_RTT$	0
$AVG\_RTT \leq RTT < Max\_RTT$	0.5
$Min\_RTT \leq RTT < AVG\_RTT$	0.75
$RTT < Min\_RTT$	1

- *Round Trip Time (RTT)*: It is the time between starting the transmission of a packet and receiving the corresponding immediate acknowledgement [30]. The use of RTT is advantageous and may be justified as follows:
  - Computing the RTT is an implicit estimation of the gateway distance and network density. Obviously, a distant gateway requires much time to respond to its associated clients than a near one. Moreover, according to Günther and Hoene [30], the distance separating a WBAN p from a gateway g may be obtained as follows:
    $$\text{Distance} = \frac{(\text{RTT} - \text{TCF}) \times \text{speed of light}}{2}, \qquad (12)$$
    where TCF is the Turned around Calibration Factor. It is an adjustment delay for errors that may occur during data transmissions [30].
  - In this case, we do not require strong assumptions to estimate the gateway distance, like each patient knows or may determine the position of each gateway.
  - Use of GPS is energy consuming.

  We define three thresholds (Max_RTT, AVG_RTT and Min_RTT) to evaluate the RTT parameter according to the procedure described in Table 6.
- *Patient direction (Dir)*: this parameter indicates if the gateway is in the same direction of the mobile patient or not. It helps us to avoid the so called ping-pong effect [31]. In fact, when a device is within the range of multiple WiFi Access Points (APs), the ping pong effect can be defined as the series of consecutive transitions from/to different access points. It is the result of the aggressive nature of 802.11 interfaces that try to connect to an access point with a better signal once the signal from the current access point drops below a given threshold [31,32]. This issue arises mainly when the device is mobile, and can be the source of extra energy consumption and data loss. *Dir* takes two possible values: 1, if gateway g is in the same direction of the patient, and 0, otherwise.

  We may estimate if a gateway is in the mobility direction of the patient or not, based on two successive captured RSSI values from such gateway. In fact, if the RSSI is

Table 7
confidence level description.

Confidence level (*Sec*)	Corresponding value	Description
High	1	The highest secure WiFi gateway is the one to which the patient is by default associated. For example, the gateway covering the room or healthcare department in which he resides.
Medium	0.75	A foreign *g* that the patient has access to before without meeting any security problem.
Unknown	0.5	A foreign *g* that the patient has not used before.
Not secured	0	A *g* that the patient used before and had security problems.

Table 8
Neighbour gateway routing table.

Gateway identifier (*G_ID*)	GCF_i	Last evaluation time	Timeout

improving, we may infer that the patient is moving in the same direction of *g*.

- *Gateway confidence level (Sec)*: in this work, we define four confidence levels which are **high, medium, unknown and not secured**. Table 7 details these different confidence levels.

We have to mention here that for gateways discovery procedure we make use of the active scanning technique [33]. This may be explained by the fact that passive scanning [34] can take a long time and is not suitable for time sensitive applications like healthcare ones. In fact, a WiFi gateway broadcasts a beacon packet every 100 ms, hence, to scan 11 channels (for 2.4 GHz) it takes well over a second. Scanning in the 5 GHz band, with 30 channels, it takes even longer. Moreover, we timestamp probe requests and responses used in active scanning to compute the RTT parameter. By this way, we limit the amount of overhead generated packets during the gateway selection process. The gateway selection process is based on a cost function. Thus, to ensure that each cluster head C selects the best candidate gateway *g*, for each available $g_i \in \mathcal{G}$, it computes a Gateway Cost Function (GCF_i) based on the three presented parameters: *RTT*, *Dir* and *Sec*. In fact, GCF_i is computed as below:

$$GCF_i = \alpha Sec_i + \beta RTT_i + \gamma Dir \quad (13)$$

with $\alpha + \beta + \gamma = 1$

We note that on the basis of α, β and γ weighting coefficients, we can promote one parameter versus another. Coordinator C selects g_i having the higher GCF_i value. Also it stores, $\forall i$, the obtained GCF_i values in a local sorted gateway routing table. Each table record includes the information given in Table 8.

Using this table naturally improves the selection process performance. It limits the process of repeatedly rescanning gateways that the patient frequently encounters. Therefore, coordinator C examines its data base and only tests gateways that do not already have a database record or are old-timer scanned. On the other hand, to cope with gateways performance variation, we force a periodic re-scans of gateways based on the last evaluation time and timeout fields. In fact, this forced re-scan timeout parameter value is set according to the study done in [35] and it depends on the patient's moving speed. Table 9 presents the used timeout values according to the patient moving speed (denoted as *MF*).

Table 9
Re-scan timeout vs patient mobility.

MF value	Re-scan timeout (in s)
1	1000
0.75	100
0.5	40
0	10

To recapitulate, coordinator *C* computes GCF_i of candidate gateways in the following cases:

- *C* newly joins the network.
- *C* reaches forced re-scan timeouts and discovers new gateways with high RSSI values (-35 (dbm) $< RSSI <$ -50 (dbm)).
- The received signal from the current gateway is low: (-65 (dbm) $< RSSI <$ -77 (dbm)).

We have to mention that each coordinator C maintains a gateway black list containing the set of unsecured gateways ($Sec_g = 0$). Obviously, C eliminates all black listed *g* from each set of candidate gateways.

4.2.2.2. Inter-WBAN communication algorithm. In some cases, direct communications between WBAN *p* and gateway *g* are impossible. In other terms, to communicate with *g*, the coordinator of WBAN *p* has to employ the relay mechanism. It has to find a secure relaying neighbour in its range. Hence, in this section we describe how a cluster head chooses its relay. As we work in a cross-layer context, our inter-BAN routing algorithm operates in compliance with the previously described PLCMAC and WiFi gateway selection algorithms. In fact, the coordinator C looks for a relaying neighbour in the following cases:

- Battery depletion: its remaining energy is less than a predefined battery threshold.
- Looses connection with its associated *g* or relaying coordinator C.
- It has no candidate gateway.
- Its current connection (with *g* or a relaying neighbour) is in continuous degradation.
- Its current relaying neighbour becomes overloaded (it cannot provide all the slots asked for reservation ($NAS >$ *NBS*)).

Similar to the gateway selection algorithm, the inter-BAN relay selection is cost-function based. But, since a gateway differs from a personal BAN coordinator regarding energy, mobility and transmission range characteristics, the selection parameters are not the same. Precisely, we make use of two

Table 10
Mobility evaluation.

$\widehat{MF}$	MF	Mobility description
$\widehat{MF} = 0$	1	Static: the patient is not able to move.
$0 < \widehat{MF} < 0.5$	0.75	Limited: the patient rarely moves.
$0.5 \leq \widehat{MF} < 1$	0.5	Medium: the patient is active.
$1 \leq \widehat{MF}$	0	High: the patient is very active.

parameters (mobility frequency and rate of helpfulness) described in the following.

- *Mobility frequency (MF)*: this parameter estimates the mobility degree of a candidate node. Each coordinator C records, in a local gateway routing table, the number of gateways (*NB_G*) it encounters in its pathway. In fact, to obtain MF:
  - First, C computes $\widehat{MF}$ as the ratio between *NB_G* and a threshold parameter, *NB_G_Thresh*:

$$\widehat{MF} = \frac{NB\_G}{NB\_G\_Thresh} \tag{14}$$

  - Second, according to the obtained $\widehat{MF}$, MF may take four different values. Table 10 represents the mapping done between the two parameters $\widehat{MF}$ and MF.

  NB_G_Thresh is an approximated value of the number of gateways that a patient may encounter along its pathway over a defined period of time, and it can be estimated as follows:

$$NB\_G\_Thresh = 1 + AVG\_Walking\_speed \times WT \times g\_prob \tag{15}$$

  Note that the value 1 represents the gateway to which the WBAN p is by default associated. *NB_G_Thresh* depends on the average walking speed of p, the walking period and the density of deployed gateways.
  Moreover, to ensure MF freshness, coordinator C resets the *NB_G* every one hour. Obviously, to guarantee service continuity, C selects nodes with limited mobility.
- *Rate of helpfulness (RH)*: the node examines the number of slots that the relay capable coordinator C may provide compared to the number of slots it requires. *RH* is computed as follows:

$$\mathrm{RH} = \begin{cases} 1, & \text{if } NB\_needed\_Slots \leq NB\_free \\ \frac{NB\_needed\_Slots}{NB\_free}, & \text{Otherwise} \end{cases} \tag{16}$$

  In fact, as mentioned before, nodes who look for finding relaying neighbours, have to keep listening to beacons exchanged in their range. A relay capable node must meets the two following requirements:
  - Has sufficient battery: its battery level is above a predefined threshold.
  - Is not an overloaded node: it can provide an $NCFP > 0$ for new nodes that aim to join it. This number is indicated in a dedicated beacon flag called *NB_free*. A node which broadcasts a beacon with $NB\_free > 0$ is a relay capable one (it both has sufficient battery and is not overloaded).

The coordinator computes the cost function (CFR) for each relay capable neighbour by summing the above parameters. Furthermore, it chooses the relay having the greatest CFR.

$$CFR_i = \lambda MF_i + \sigma RH_i \tag{17}$$

with $\lambda + \sigma = 1$

We note that node reliability, which may be estimated via the packet delivery ratio (PDR), is not considered in the CFR formula. This is due to the fact that:

- A node cannot measure the PDR of a node joining the network for the first time.
- Using a PDR measured by other neighbour nodes is not very effective for two main reasons: (1) communication links between nodes are quite different in terms of QoS, and (2) the PDR information exchange between neighbours may generate more overhead.

This issue is not overlooked in our algorithm. Indeed, the coordinator C keeps in memory all the relaying capable nodes that it has before. It puts those not providing it a sufficient PDR at the bottom of the list of its relay capable neighbours.

5. Performance evaluation

In the context of this work we focus on, but not limited to, elderly residential healthcare monitoring spaces. This application domain is very important and strategic, since it permits to leave patients more freedom and make them feel at home while still being monitored by the medical staff. Often, these healthcare smart spaces are WiFi covered to collect different types of data about patients. We consider a typical smart healthcare hospice scenario of area 1000 m × 1000 m in which 120 patients are being monitored through a WBAN. This area is covered by eight WiFi Access Points (APs) having a communication range of 120 m. Each WBAN p has a star topology, where a coordinator C is at the centre of the topology, and 6 sensor devices are placed around it. We note that, to communicate with their cluster head (the coordinator C), some sensors may require the relaying service of their one hop neighbouring sensors belonging to the same WBAN p. Fig. 4 presents an example of a WBAN topology.

Each WBAN p is by default associated to a gateway g. While they are doing their normal routine work, patients move and may be far away from their default gateway (i.e., go somewhere in the corridors, media room, or even in the playground). In this case, to keep connected, the WBAN will have to look for another relaying node C and communicate in a hop-by-hop fashion (inter-body communication) or connect to another g. In order to validate the proposed solution for such context, we have implemented our PCLRP protocol using the OMNeT++ simulator [36] and compared the QoS performance and energy consumption with those of WASP protocol [8,41].

We set the Beacon Interval (BI) of PCLRP the same as the BI of IEEE 802.15.4 [37] with superframe parameters BO = 6 and slot size = 7.68 ms. Simulation parameters are detailed in Table 11. We opted for the WASP protocol for comparison for two main reasons. First, WASP has several focal points: it is energy efficient, achieves a good packet delivery ratio, and reduces the coordination overhead [41,42]. Second, similar to our PCLMAC, this protocol incorporates a closely coupled interaction between the MAC and the network layers. Indeed, WASP schemes (beacons) are not only used to guarantee MAC

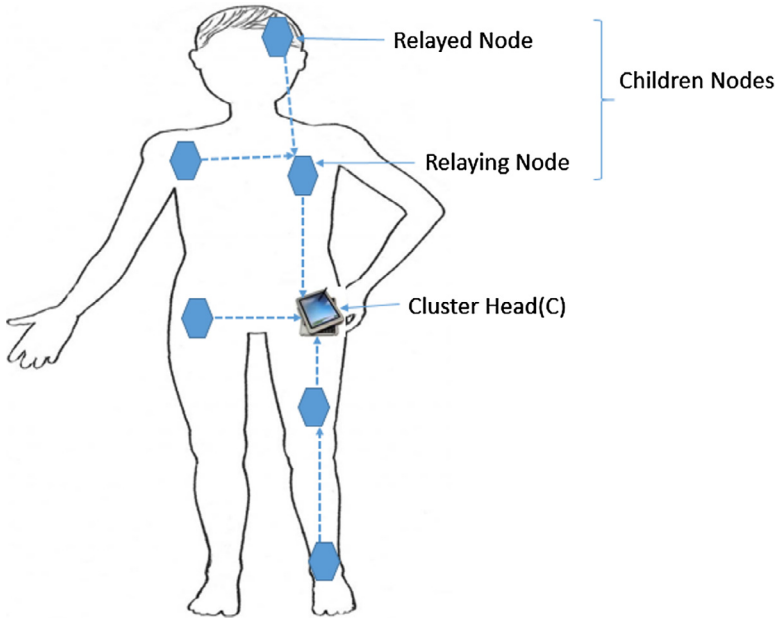


Fig. 4. Example of an intra-body WBAN topology.

Table 11
Simulation parameters.

Parameter	Value
ASD	967.68 ms
CCAP_min	61.44 ms
DLD	0
CFP	844.8 ms
NCAP_min	61.44 ms
Inactive period	15.36 ms
MaxFrameRetries	3
Backoff exponent	3
Number of backoffs	2
Channel model	Log Shadowing Wireless Model
Channel capacity	1024Kb/s
Initial energy of sensor	18,720 J
Sensor battery threshold	9360 J
Coordinator initial energy	20,000 J
Coordinator battery threshold	7000 J
Max_RTT	250 ms (max E2E specified in the WBAN standard IEEE 802.15.6 [39])
AVG_RTT	150 ms
min_RTT	50 ms
Mobility model	Random way point Bai and Helmy [40]
α	0.4
β	0.4
γ	0.2
λ	0.5
σ	0.5
EMIFS	60 μs
DSIFS	75 μs
GMIFS	85 μs
Path loss exponent	2.4
NBG_thresh	4
Maximum clock drift rate	40 μs
Clock accuracy	1 ms
AVG_Walking_speed	4.11 ft. [43]
WT	250 s
g_prob	1/120
Simulation time	250 s

slot allocation, but also to build the best routing paths. However, WASP does not consider the traffic heterogeneity in WBANs. For this reason, we have also considered the DMQoS protocol [9] in the evaluation process of PCLRP. In fact, similar to PCLRP, DMQoS considers each personal WBAN as a cluster wherein C is the head. Moreover, this cross-layer protocol ensures traffic differentiation by defining four classes of data packets: Ordinary data Packets (OP), Reliability driven data Packets (RP), Delay-driven data Packets (DP) and most Critical data Packets (CP).

In order to evaluate the effectiveness of PCLRP with respect to WASP and DMQoS, we run several simulation scenarios and use three main evaluation metrics: Energy consumption, Packet Delivery Ratio (PDR) and delay.

5.1. Scenario 1

As mentioned before, unlike coordinators, sensor nodes are energy constrained. Thus, in this scenario, we compute the average energy consumed by sensor nodes when each one generates 30 packets per second. Obtained results are presented in Fig. 5.

Fig. 5 shows that the PCLRP protocol outperforms WASP and DMQoS in terms of power consumption. This is because sensors in PCLRP wake up to receive beacons according to their traffic-patterns, thus reducing the extra power consumed in idle listening/overhearing. More specifically, low duty cycle nodes keep their radio receiver off and wake up only if there is data to report. However, regardless of their traffic-patterns, nodes in WASP have to wake up and receive the WASP-scheme at the beginning of each WASP-cycle. Also, as the DMQoS MAC is based on IEEE 802.15.4, it suffers from idle listening and overhearing [38]. Moreover, as described in Section 2, DMQoS is based on packet duplication to ensure reliability, which increases energy consumption.

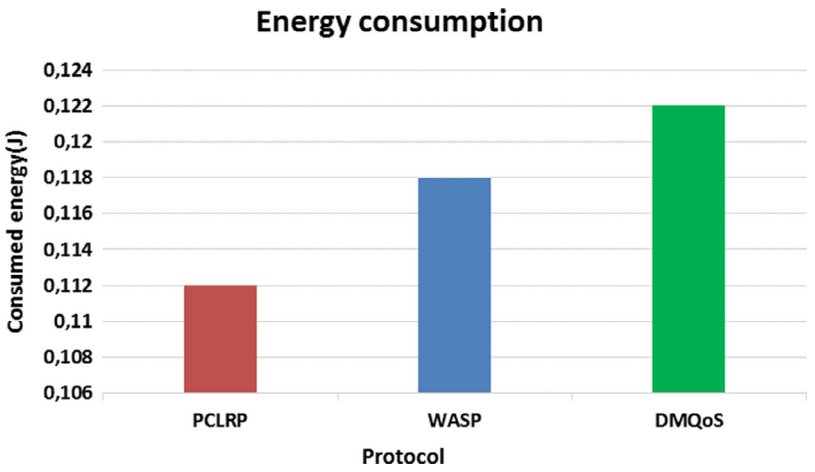


Fig. 5. Average energy consumed per node when each sensor generates 30 packets/sec.

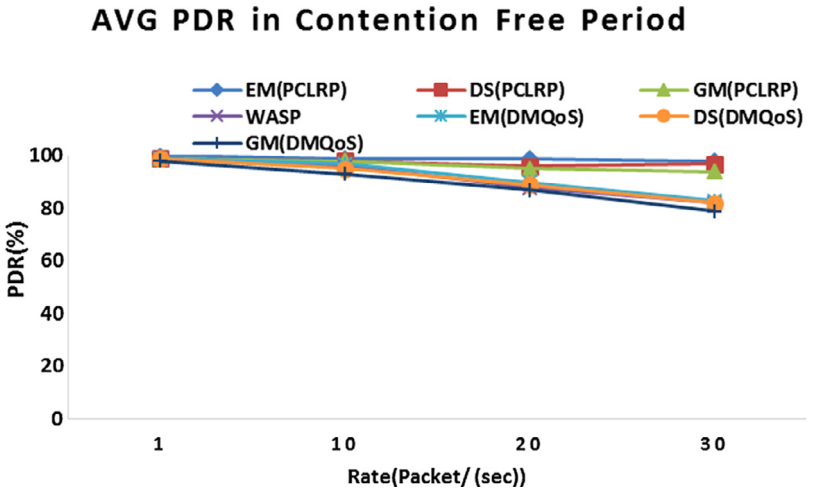


Fig. 6. PDR in CFP period according to traffic categories when increasing the data rate.

5.2. Scenario 2

In this scenario, we evaluate the protocols reliability versus the traffic increase. We vary the number of packets per second, generated by each node, and measure the packet delivery ratio. Figs. 6 and 7 show the PDR measured, respectively, in CFP and CAP periods.

It can be observed that best results are obtained in the CFP period for the PDR. This is due to the fact that communications in the CAP period suffer from high collision and interference probability, and this increases packet losses. As expected, we can see that in all cases the PDR decreases when we increase the packet rate and the rate of decrease is more evident for GM packets than for DS and EM packets, since packets are served according to their priority. We also note that PCLRP outperforms both DMQoS (for each traffic category) and WASP for all considered rates, since PCLRP ensures node synchronization and shorter transmission delays than DMQoS and WASP.

5.3. Scenario 3

In this scenario, we evaluate the effectiveness of PCLRP in terms of performed backoff and E2E delays. The backoff delay is measured only for PCLRP and WASP, since DMQoS does not tackle the channel access issue. Fig. 8 shows the average backoff delay (in ms) when EM, DS and GM traffics are co-generated, varying the number of nodes in each WBAN from 1 to 10.

Obtained results demonstrate that PCLRP outperforms DMQoS and ensures shorter backoff delays mainly for EM and DS traffics. This is due to the fact that in PCLRP the backoff time computation depends on the generated traffic's priority (see Eq. (1)). Precisely, a high priority sensor (a sensor with EM data to transmit) has a high probability to choose short backoff duration, resulting in low access delay. However, since WASP does not deal with the traffic classification issue, all nodes have the same probability to choose a short backoff delay. Moreover, in all cases, the backoff duration increases linearly by increasing the number of nodes.

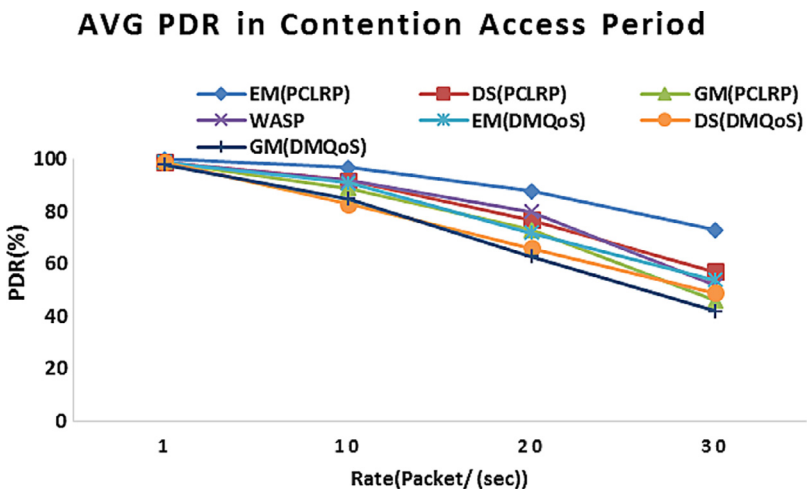


Fig. 7. PDR in CAP according to traffic categories when increasing the data rate.

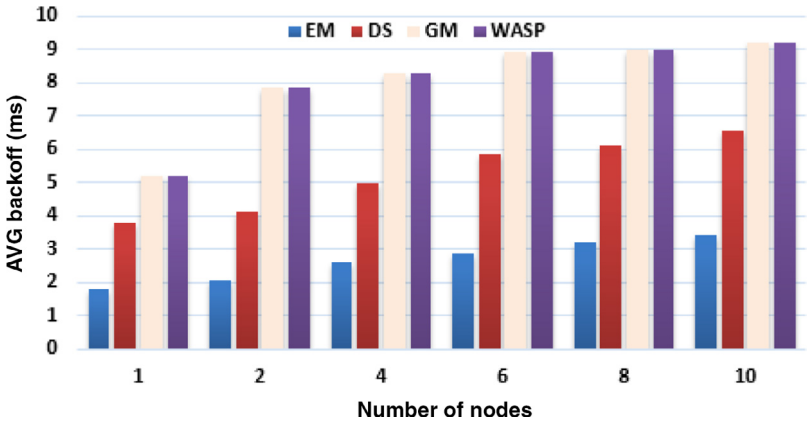


Fig. 8. Average backoff delay according to traffic classes vs number of nodes.

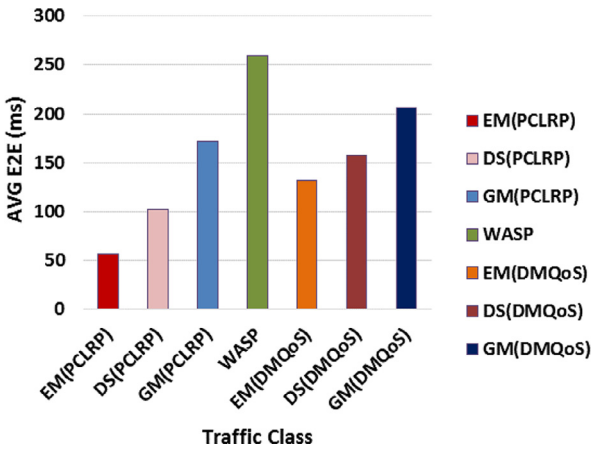


Fig. 9. Average E2E delay according to traffic classes.

It can be seen in Fig. 9 that the average End-to-End delay (E2E) in the PCLRP protocol is lower than in WASP and DMQoS. This is because, in WASP, packets of relayed nodes have to wait longer before they are served. As a consequence, the experienced delay depends on the number of hops in the network. Indeed, a node can send its data only one hop up during each WASP-cycle. For example, data generated by a node situated at a second hop requires two WASP-cycles to be served. Also, interference and network congestion caused by duplication of transmitted data increase the E2E delay experienced in DMQoS. However, in PCLRP, independently of the number of hops, all generated data are disseminated to the coordinator in the same beacon interval. Fig. 9 also shows that measured delays depend on the traffic priorities. Therefore, EM packets have the smallest delay while GM packets have the largest one. This result is expected, since PCLRP nodes with the highest priority have the shortest backoff and IFS delays, and guaranteed slots.

5.4. Scenario 4

In this scenario, we analyse the effects of varying the weighting coefficients of the security factor (α), the RTT factor (β), the direction factor (γ), the mobility factor (λ), and the Rate of Helpfulness (RH) factor (σ) of Eqs. (11) and (14). Specifically, we measure the effect of each weight on the obtained PDR and E2E delay according to patient mobility. Table 12 presents the three tested weighting coefficients assignment cases. In fact, we ignore the mobility parameters

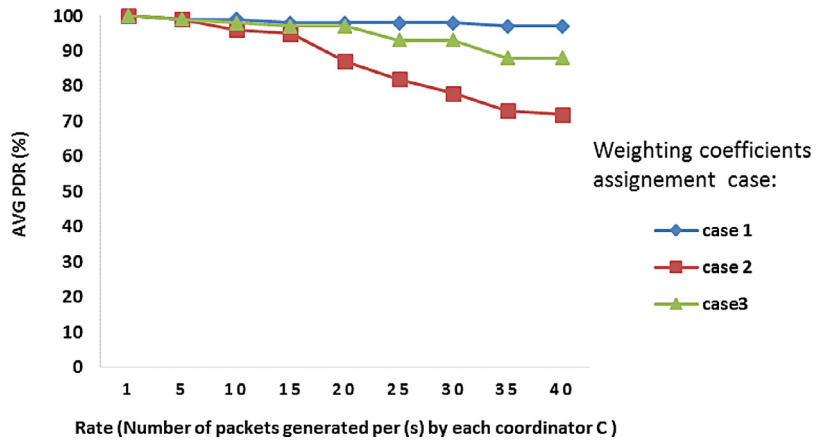


Fig. 10. Average PDR according to traffic rate and weighting coefficients variation in a static WBANs context.

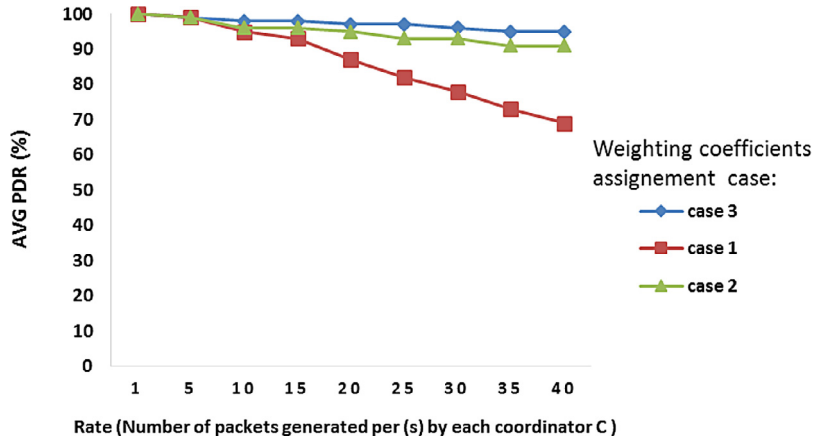


Fig. 11. Average PDR according to traffic rate and weighting coefficients variation in a mobile WBANs context.

Table 12
Weighting coefficients assignment.

	α	β	γ	λ	σ
Case 1	0	1	0	0	1
Case 2	0	0	1	1	0
Case 3	0.3	0.4	0.3	0.5	0.5

in case 1, while we neglect RH and RTT weights in the second case. Nonetheless, in case 3 we consider all the parameters. Fig. 10 shows the obtained PDR when we vary the packet rate from 1 to 40 packets/s and all WBANs are static. It can be seen that the best results are obtained when we set β and σ coefficients to their maximum values, i.e., 1. This means that, in a static context, the most important relay and gateway selection parameters are the *RTT* and *RH*. This is reasonable, since there is no much need to consider the mobility parameters in a static context. The same applies for the security parameter, since a static WBAN p does not encounter unsecured gateways in its pathway.

When comparing to Fig. 10, it can be seen in Fig. 11 that the obtained PDR slightly decreases in the mobile context. This is due to the additional time needed to the search for relays and connection/disconnection process during the WBAN's movement. Moreover, we observe that the worst PDR values are obtained when we ignore the mobility related parameters. One can also note that the best results are obtained when we consider all the parameters and not when the α, γ and λ coefficients are set to their maximum values. Here, we can infer that in a mobile context not only mobility parameters are important, but also the *RTT* and *RH*.

5.5. Scenario 5

Ensuring network scalability is a key issue in mobile WBANs. Indeed, in this scenario we focus on evaluating the robustness of PCLRP and DMQoS when the number of WBANs increases. We do not consider the WASP protocol since this latter focuses only on the intra-body communication level. Thus, we vary the number of associated WBANs per gateway and compute the consumed energy and the E2E delay when each WBAN generates 20 packets per second.

Figs. 12 and 13 show that, for both PCLRP and DMQoS, the higher the number of connected users per gateway, the higher the obtained E2E delay and consumed energy. Fig. 12 proves the scalability of PCLRP and DMQoS in terms of E2E delay. As shown in the figure, in all cases the measured E2E delay is much lower than the upper threshold of E2E delay defined by the WBAN standard IEEE 802.15.6 [39]. It can be

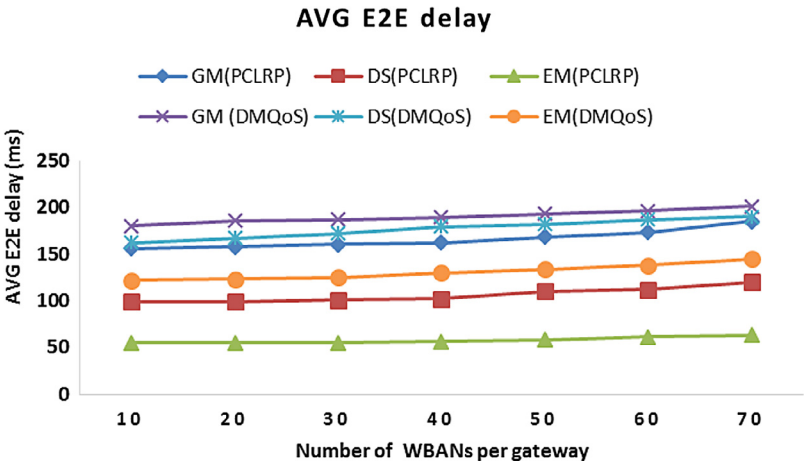


Fig. 12. Average E2E delay according to traffic classes vs the number of WBANs.

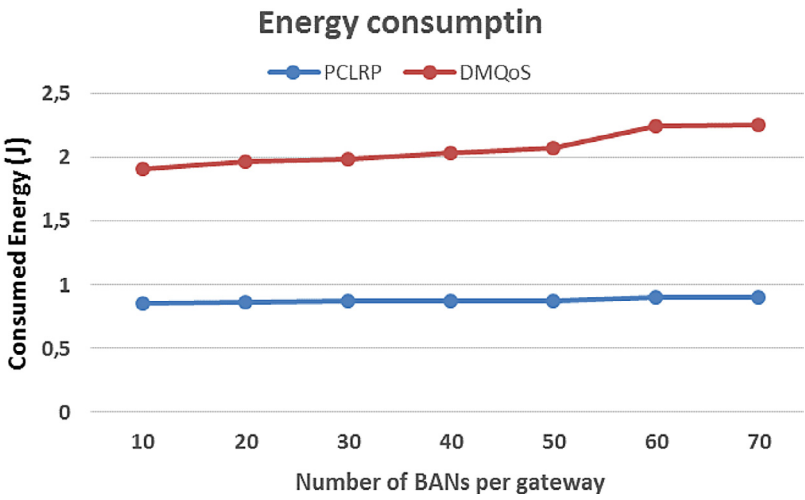


Fig. 13. Average consumed energy per mobile WBAN vs the number of WBANs.

seen that the highest E2E delays measured for the lowest prioritized packets (GM) are 185 ms for PCLRP and 201 ms for DMQoS, which is much lower than 250 ms. Likewise, we note that in all cases PCLRP outperforms DMQoS. This can be explained by the fact that layer-cooperation in PCLRP well enhances the QoS by limiting packet overheads and energy consumption caused by interference and idle listening. Contrariwise, in DMQoS, although traffics are classified, the MAC protocol operates without considering the classification made. Also, DMQoS suffers from huge interference due to duplication of transmitted data, especially when the number of WBANs is important.

Finally, Fig. 13 shows that unlike DMQoS, the energy consumed by the nodes forming each network is slightly influenced by the increase in the number of WBANs. This can be explained by the fact that PCLRP is TDMA-based. Furthermore, sensor nodes disseminate their collected data to their associated coordinator and go to sleep. In fact, transmission of data to the final destination, retransmissions on failure and due to interference and collisions are the responsibility of the coordinator, which is an energy powerful node.

6. Conclusion and future works

In this paper, we proposed a Priority based Cross Layer Routing Protocol for healthcare applications. PCLRP addressed the channel access and routing issues both for intra- and inter-body communication levels with a clear differentiation between multiple traffic types with respect to their QoS requirements. We evaluated PCLRP in terms of power consumption, PDR and delay. The results were compared with the well-known WASP and DMQoS protocols, and it was shown that the PCLRP protocol exhibits better performance (lower E2E delay and energy consumption, and higher PDR values) than WASP and DMQoS.

In the near future, we plan to implement our protocol in a real WBAN-based environment.

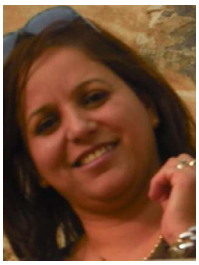
References

[1] H. Ben Elhadj, L. Chaari, L. Kamoun, A survey of routing protocols in wireless body area networks for healthcare applications, Int. J. E-Health Med. Commun. (IJEHMC) 3 (2) (2012) 1–18.

[2] N. Bradai, L. Chaari, L. Kammoun, A comprehensive overview of wireless body area networks (WBAN), Int. J. E-Health Med. Commun. 2 (3) (2011) 1–30, doi:10.4018/jehmc.2011070101.
[3] T. Hayajneh, G. Almashaqbeh, S. Ullah, A.V. Vasilakos, A survey of wireless technologies coexistence in WBAN: analysis and open research issues, Wireless Netw. 20 (8) (2014) 1–35.
[4] G.K. Ragesh, K. Baskaran, An overview of applications, standards and challenges in futuristic wireless body area networks, Int. J. Comput. Sci. Issues 9 (2012) 180–186.
[5] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao, V.C.M. Leung, Body area networks: a survey, Mobile Netw. Appl. 16 (2011) 171–193, doi:10.1007/s11036-010-0260-8.
[6] C.S. Jang, D.G. Lee, J.-W. Han, J.H. Park, Hybrid security protocol for wireless body area networks, Wireless Commun. Mobile Comput. 11 (2011) 277–288, doi:10.1002/wcm.884.
[7] L.D. Mendes, J. JPC Rodrigues, A survey on cross-layer solutions for wireless sensor networks, J. Netw. Comput. Appl. 34 (2) (2011) 523–534.
[8] B. Braem, B. Latre, I. Moerman, C. Blondia, P. Demeester, The wireless autonomous spanning tree protocol for multihop wireless body area networks, in: Proceedings of the First International Workshop on Personalized Networks, San Jose, California, USA, ICST, 2006.
[9] M.A. Razzaque, C.S. Hong, S. Lee, Data-centric multi-objective QoS-aware routing protocol for body sensor networks, Sensors 11 (1) (2011) 917–937.
[10] X. Liu, A survey on clustering routing protocols in wireless sensor networks, Sensors 12 (8) (2012) 11113–11153.
[11] S. Saleh, M. Ahmed, B.M. Ali, M.F.A. Rasid, A. Ismail, A survey on energy awareness mechanisms in routing protocols for wireless sensor networks using optimization methods, Trans. Emerg. Telecommun. Technol. 25 (12) (2014) 1184–1207.
[12] L. Hughes, X. Wang, T. Chang, A review of protocol implementations and energy efficient cross layer design for wireless body area networks, Sensors 12 (2012) 14730–14773, doi:10.3390/s121114730.
[13] M. Atto, C. Guy, A cross layer protocol for energy aware and critical data delivered applications using wireless sensor networks, J. Emerg. Trends Comput. Inf. Sci. 5 (4) (2014) 308–315.
[14] A. Manjeshwar, D.P. Agrawal, APTEEN: a hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks, in: IPDPS, IEEE, 2002, p. 0195b.
[15] T. O'Donovan, J. Brown, U. Roedig, C. Sreenan, J. doO, A. Dunkles, L. Wolf, GINSENG: Performance Control in Wireless Sensor Networks, 2010.
[16] A.G. Ruzzelli, R. Jurdak, G.M. OHare, P.V.D. Stok, Energy-efficient multihop medical sensor networking, in: Proceeding of 1st ACM SIGMOBILE International Workshop on Systems and Networking Support for Healthcare and Assisted Living Environments, ACM, New York, NY, USA, 2007, pp. 37–42.
[17] W.R. Heinzelman, A. Chandrakasan, H. Balakrishnan, Energy-efficient communication protocol for wireless microsensor networks, in: Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, IEEE, 2000, p. 10.
[18] B. Latre, B. Braem, I. Moerman, C. Blondia, E. Reusens, W. Joseph, P. Demeester, A low-delay protocol for multihop wireless body area networks, in: Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services, 2007 (MobiQuitous 2007), IEEE, 2007, pp. 1–8.
[19] H. Ben Elhadj, S. Boudjit, L. Chaari Fourati, A cross-layer based data dissemination algorithm for IEEE 802.15. 6 WBANs, in: 2013 International Conference on Smart Communications in Network Technologies (SaCoNeT), 1, IEEE, 2013, pp. 1–6.
[20] H. Ben Elhadj, S. Boudjit, L. Chaari, L. Kamoun, IEEE 802.15.6 based node and hub architectures for healthcare applications, in: Wireless Days (WD), 2014 IFIP, IEEE, 2014, pp. 1–3.
[21] H. Garudadri, P.K. Baheti, Packet loss mitigation for biomedical signals in healthcare telemetry, in: Proceedings of Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Buenos Aires, Argentina, 2009, pp. 2450–2453.
[22] M.T. Hassan, E. Ahmed, J. Qadir, A. Baig, Quantifying the multiple cognitive radio interfaces advantage, in: 2013 27th International Conference on Advanced Information Networking and Applications Workshops (WAINA), IEEE, 2013, pp. 511–516.
[23] IEEE Engineering in medicine and biology society ISO/IEEE standard 11073: health informatics—POC medical device communication—Part 00101: guidelines for the use of RF wireless technology.
[24] L. Dai, P. Basu, J. Redi, An energy efficient and accurate slot synchronization scheme for wireless sensor networks, in: 3rd International Conference on Broadband Communications, Networks and Systems, 2006 (BROADNETS 2006), IEEE, 2006, pp. 1–8.
[25] S. Watwe, A. Bhatia, R.C. Hansdah, A design for performance improvement of clock synchronization in WSNs using a TDMA-based MAC protocol, in: 2014 28th International Conference on Advanced Information Networking and Applications Workshops (WAINA), IEEE, 2014, pp. 366–371.
[26] B. Kusý, Spatio-temporal coordination in wireless sensor networks, (Doctoral dissertation), Vanderbilt University, 2007.
[27] F. Sivrikaya, B. Yener, Time synchronization in sensor networks: a survey, IEEE Netw. 18 (4) (2004) 45–50.
[28] B. Sundararaman, U. Buy, A.D. Kshemkalyani, Clock synchronization for wireless sensor networks: a survey, Ad Hoc Netw. 3 (3) (2005) 281–323.
[29] J. Elias, A. Mehaoua, Energy-aware topology design for wireless body area networks, in: 2012 IEEE International Conference on Communications (ICC), IEEE, 2012, pp. 3409–3410.
[30] A. Günther, C. Hoene, Measuring round trip times to determine the distance between WLAN nodes, in: Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications Systems (NETWORKING 2005), Springer, Berlin/Heidelberg, 2005, pp. 768–779.
[31] R. Sousa, R. Morla, A. Maio, J. Coelho, Analysis of the logical proximity between 802.11 access points, in: CRC 2012: Conferencia Sobre Redes de Computadores, 2013, pp. 47–55.
[32] M. Kim, D. Kotz, Modeling users' mobility among WiFi access points, in: Papers Presented at the 2005 workshop on Wireless Traffic Measurements and Modeling, USENIX Association, 2005, pp. 19–24.
[33] S. Shin, A.G. Forte, H. Schulzrinne, Seamless Layer-2 Handoff in IEEE 802.11 using Two Radios.
[34] M. Youssef, M. Mah, A. Agrawala, Challenges: device-free passive localization for wireless environments, in: Proceedings of the 13th Annual ACM International Conference on Mobile Computing and Networking, ACM, 2007, pp. 222–229.
[35] T. Li, Cutting WiFi Scan Tax for Smart Devices, Dartmouth College, 2014.
[36] http://www.omnetpp.org/.
[37] A. Koubâa, A. Cunha, M. Alves, E. Tovar, TDBS: a time division beacon scheduling mechanism for ZigBee cluster-tree wireless sensor networks, Real-Time Syst. 40 (3) (2008) 321–354.
[38] M. Khanafer, M. Guennoun, H.T. Mouftah, A survey of beacon-enabled IEEE 802.15. 4 MAC protocols in wireless sensor networks, IEEE Commun. Surv. Tutorials 16 (2) (2014) 856–876.
[39] 802.15.6–2012 IEEE Standards for Local and Metropolitan Area NetworksPart 15.6: Wireless Body Area Networks, http://standards.ieee.org/findstds/standard/802.15.6--2012.html.
[40] F. Bai, A. Helmy, A survey of mobility models, Wireless Adhoc Networks, University of Southern California, USA, 2004, p. 206.
[41] P.T. Sharavanan, R. Kumar, D. Sridharan, A comparative study of cross layer protocols in wban, Aust. J. Basic Appl. Sci. 9 (16) (2015) 294–300.
[42] K. Garg, D. Puccinelli, S. Giordano, Implementation of the wireless autonomous spanning tree protocol on mote-class devices, in: The 2nd International Conference on Emerging Network Intelligence (EMERGING 2010), 2010.
[43] http://www.usroads.com/journals/p/rej/9710/re971001.htm.

Hadda Ben Elhadj was born in Sfax, Tunisia, in 1985. She received her degree in Computer Engineering and her Master in Computer Engineering from Sfax University, Tunisia, in 2010. Actually, she is a Ph.D. student and a member of Sfax Laboratory of Electronics and Information Technology. Her current research interests are communications and networking specially related to wireless and body are networks.

Jocelyne Elias is an Associate Professor at Paris Descartes University since September 2010. She held a Post-doc position at the Department of Information and Mathematical Methods of University of Bergamo (2009–2010). She obtained her Ph.D. in Information and Communication Technology at the Department of Electronics and Information of Politecnico di Milano in 2009. Her main research interests include network optimization, and in particular modeling and performance evaluation of networks (Cognitive Radio, Wireless, Overlay and Wired Networks), as well as the application of Game Theory to resource allocation, spectrum access, and pricing problems.



Lamia Chaari was born in Sfax, Tunisia, in 1972. She received the engineering and Ph.D.degrees in electrical and electronic engineering from National Engineering School of Sfax (ENIS) in Tunisia. She obtained her HDR in Telecommunication in July 2011. Actually, she is an Associate Professor in multimedia and informatics higher institute in Sfax. She is a researcher in electronics and technology information laboratory (LETI). Her scopes of research are communications, networking and signal processing which are specially related to wireless and new generation networks.

Lotfi Kamoun was born in Sfax Tunisia, 25 January 1957. He received the electrical engineering degree from the Sciences and Techniques Faculty in Tunisia. Actually he is a Professor in National Engineering School of Sfax (ENIS) in TUNISIA, Director of SfaxHigher Institute of Electronics and Communications in Tunisia and director of Laboratory of Electronics and Technology Information (LETI). His scopes of research are communications, networking, and software radio and signal processing which are specially related to wireless and new generation networks.