CIT. Journal of Computing and Information Technology, Vol. 26, No. 2, June 2018, 69–83
doi: 10.20532/cit.2018.1003832

Adaptive Parameters Adjustment in WBAN based IEEE 802.15.4 Protocol to Mitigate Wi-Fi Interferences

Sarra Essafi and Tahar Ezzedine

Communication System Laboratory Sys'Com, National Engineering School of Tunis, University Tunis El Manar, Tunis, Tunisia

Wireless Body Area Network (WBAN), called also Wireless Body Sensor Network (WBSN), is composed of a set of tiny wireless devices (sensors) attached, implanted or ingested into the body. It offers real time and ubiquitous applications thanks to the small form, the lightness, and the wireless interface of sensors. WBAN performance is expected to be considerably degraded in the presence of Wi-Fi networks. Their operating channels overlap in the 2.4 GHz Industrial Scientific and Medical (ISM) band which produces interference when they transmit data, accompanied by data losses and quick battery exhaustion. Therefore, it is crucial to mitigate the interference between WBAN and Wi-Fi networks in order to maintain the efficiency and the reliability of the WBAN system. Proposals in the literature use an added complex hardware in WBAN system, or perform the exchange of additional information, or establish expensive communications, or affect the quality of service of the WBAN. Unlike previous researches, we proposed simple, low cost and dynamic method that adaptively adjusts specific parameters in the Medium Access Control (MAC) layer. We have proved the effectiveness of our approach based on theoretical analysis and simulation using MiXiM framework of OMNet++ simulator.

ACM CCS (2012) Classification: Networks → Network types → Mobile networks

Keywords: IEEE 802.15.4, Wi-Fi, coexistence, interference, body, wireless sensors, WBAN, WBSN

1. Introduction

WBAN (Wireless Body Area Network) or WBSN (Wireless Body Sensors Network) offers plenty of innovative applications and mobile services in different domains. For instance, the medical WBAN is composed of a set of tiny wireless devices (sensors) attached, implanted or ingested into the body. WBAN sensors continuously monitor biomedical data and critical vital signs, such as temperature, heart activity, glucose level, blood pressure, etc. It continuously monitors the health state of the patient or deliver emergency drug to the body in order to save his life. WBAN improves the patient's quality of life and reduces laboratory, nursing and hospital costs. It should continuously function well to reliably deliver the collected data to the concerned medical entity.

WBAN provides continuous mobile services and is susceptible to meet other wireless networks that operate in the same unlicensed 2.4 GHz industrial, scientific and medical (ISM) band. The 2.4 GHz band is used by numerous wireless technologies like ZigBee, Bluetooth, Wi-Fi, etc. They take advantage from its worldwide availability and its large bandwidth. However, this leads to the band congestion and data collision.

We were interested, in this work, in the effect of the interfering Wi-Fi network, since it is omnipresent and with a large interference coverage range, to provide internet connection to nearby Wi-Fi devices.

The user carrying WBAN is more likely to be inside the range of Wi-Fi network, and they will interfere with each other causing data loss and a severe degradation of the WBAN performance.

In this paper, we described the coexistence problem between the WBAN based IEEE 802.15.4

protocol and Wi-Fi networks; and we proposed a simple and low cost method to mitigate interference, based on parameters adjustment in the Medium Access Control (MAC) layer. This method tries to reduce the packet size, the Clear Channel Assessment (CCA) and time slot of backoff process even when WBAN starts losing its data. Theoretical and simulation results have showed that this improves the reliability of WBAN transmissions under Wi-Fi interferences.

The rest of the paper is organized as follows: The second section reviews main related works; the third section describes the coexistence problem between WBAN and Wi-Fi and details their channel access mechanism; the fourth describes our proposed approach to improve the WBAN reliability under interference; the fifth section defines theoretical analysis and related results; and, finally, in the sixth section, a simulation example was conducted to investigate the potential interference effect of Wi-Fi on WBAN and to show the effectiveness of our proposal.

2. Related Work

Researchers were interested in studying the WBAN communication quality under interferences. Many works [1], [2], [3] showed that interferences decreased the reliability of packet reception, increased transmission delay and consumed more energy. Data losses caused by interferences disrupt the correct operation of time-constrained WBAN applications; especially, in medical applications, it disrupts the delivery of critical data (like heart beat measurements) to the concerned server and provokes delayed reception. Moreover, the overdone interference will severely exhaust the WBAN's power quickly, due to the attempt of retransmissions of lost data.

Thus, the interferences must be properly mitigated to improve the performance of the WBAN system. Essafi *et al*. [4] and Thaier *et al*. [5] provided reviews and critics of existing solutions.

Sensors in WBAN are constrained in terms of processor, memory and battery. This makes it unable to support complex algorithms and additional exchanges of extra information to improve its performance under interferences.

The IEEE 802.15 working group specifies wireless personal area network (WPAN) standards. The IEEE 802.15.4 and the IEEE 802.15.6 are the most widely used for WBAN. They define the characteristics of physical and MAC layer for data communications. They are conceived for short range communication and low energy consumption.

Theoretical analysis of Thaier *et al*. [5] show that Low Power Wi-Fi (lp-wifi) technology used for WBAN mitigates Wi-Fi interferences better than IEEE 802.15.4 and IEEE 802.15.6. Although it conserves more energy than the Wi-Fi standard, it consumes much more, compared to the other technologies used by WBAN. Jose [6] showed that lp-wifi consumes 350 mW in transmission while IEEE 802.15.4 standard consumes only 25 mW.

Jasleen [7] elucidated that IEEE 802.15.4 performs better than IEEE 802.15.6 in terms of energy consumption, throughput and latency. We mainly focus on WBAN based IEEE 802.15.4 standard, because it consumes less energy [8] and has better performance in terms of packet loss and delay than IEEE 802.15.6 [9].

Several approaches which have been proposed for sensors network cannot be applied for WBAN, because of the entire mobility of the network and the movement of each sensor in different body parts. For example, the TSCH mode of MAC layer proposed by Mengchuan *et al*. [10] aims to detect neighbouring interfering networks, to collaborate with them in forming a common schedule that provides channel hopping and reserve certain amount of bandwidth (time) for each flow. However, the network attachment and collaboration requires a non-suitable delay to reach an improved and stable state in view of the high mobility, high movement and high topology change of the WBAN.

The channel hopping approach is able to switch the working channel to the channel that has less interferences and better transmission quality [11]. However, it requires complex radio hardware and high-performing filters.

The time assignment approach in MAC layer reschedules data packet transmissions into free time space; however it requires exchange of additional information and establishment of expensive communications that allow WBAN to consume more energy.

Coordination with interfering network could not be possible in the case of Wi-Fi interference, due to the dissimilarity of their standard specifications. Many researches enabled the communication between WBAN master node and the Wi-Fi network by using fake Wi-Fi packets (RTS: Request to Send) to allocate the channel for WBAN's transmissions [12] or by using fake (CTS: Clear to Send) packets to prevent Wi-Fi devices from sending data for a sufficient duration [13]. This method is flexible and tries to adapt with WBAN's standard without any modification. However, it requires an additional and powerful node that supports expensive computations and communicates with the two networks simultaneously.

Sarra *et al*. [1] use Multi-Hop topology and dynamic routing protocol. This method uses low transmission power and routes the data packets through the path that has less interferences and better transmission. This method provides reliability and connectivity. However, it needs the exchanges of routing packets and it produces unfair communication since the more selected nodes process more traffic than the others. Consequently, their batteries are more likely to die earlier.

Some default parameters in WBAN network contribute to the increase of interference effects. For this, adequate adjustment of their values is a simple method that helps to optimize coexistence of WBAN with the interfering networks. In this work, we were interested in adopting this method because, unlike the above interference mitigation techniques, it does not require complex processing, expensive communication, or the installation of extra equipment. In addition, the mechanism of different protocols OSI layers remains the same, without modification. For instance, in literature, parameters adjustments methods to mitigate interferences are:

- reducing transmission power [1],
- decreasing the value of energy detection [14],
- changing the type of modulation [15],
- decreasing the data rate [15],
- reducing the duty cycle [15],
- increasing the inter-generation time of packet [1] [14].

However, modification of the above parameters generates limitations: higher transmission power produces more energy consumption; lower energy detection generates more packet drops due to the TXFIFO overflow; the adaptive modulation, data rate and duty cycle affect the WBAN's quality of service; increasing the inter-generation time of packet reduces the probability of packet collision, but cannot be applied for all WBAN applications, because it increases the transmission delay.

In this work, we not only choose parameters that reduce the effects of interferences, but also maintain the quality of service of the WBAN network. More details will be given in the fourth, fifth and sixth sections of this paper.

3. Problem Statement and MAC Mechanism

In this section we describe the coexistence problem as well as the MAC mechanism of the WBAN and the interfering network.

3.1. Coexistence Issues

WBAN provides continuous mobile services without preventing the user from practising his daily activities.

Although it offers real time and ubiquitous services and applications, it is more likely to operate close to the Wi-Fi network, which leads to interferences. The Wi-Fi is the market name of a Local Area Network based of one of IEEE 802.11 standards. IEEE 802.11b/g/n standard uses the 2.4 GHz band. Figure 1 shows the center frequencies and overlapped channels of both IEEE 802.15.4 and IEEE 802.11. There is a considerable overlap between most channels of the two standards. When the two networks operate in vicinity of each other, simultaneous transmissions of the two networks lead to data collisions and losses. Wi-Fi threatens more the WBAN networks regarding its high transmission power and large bandwidth. Thus, managing co-existence of the two networks is important to maintain the required quality of service of low power WBAN application.

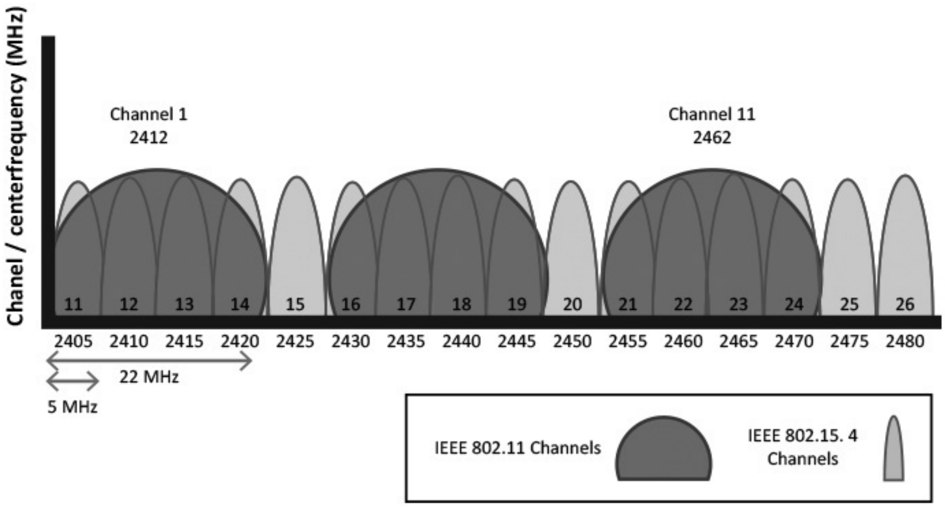

Figure 1. IEEE 802.11 and IEEE 802.15.4 Channels in the 2.4 GHz ISM Band. There are considerable overlaps between most channels of the two standards.

3.2. MAC Mechanism

An efficient MAC layer provides regulated access to the shared band to avoid packet collision.

The MAC layer of IEEE 802.15.4 supports two modes of operation: beacon enabled and non-beacon enabled mode. During the non-beacon enabled mode, the medium is accessed by unslotted CSMA/CA mechanism. The device that wants to transmit a packet sees if the channel is free, otherwise it waits a random period. Using the beacon enabled mode, all nodes should be synchronized with the coordinator. When a beacon is received from the coordinator, all devices are informed about the duration of the superframe (the activity period of the coordinator) and the time of data transmission. It guarantees that bandwidth to priority sensor in CFP (Contention Free Period); the others, non-priority sensors can transmit randomly in CAP (Contention Access Period).

However, the beacon of a coordinator is transmitted without using CSMA/CA. Thus, the beacon can be easily lost in the case of Wi-Fi interference. Consequently, data transmission will be postponed to the next superframe and will produce a larger delay. The non-beacon mode that we used in this work is more scalable and it does not need expensive processing and time synchronization. Moreover, it is more robust in the presence of Wi-Fi interference. If Wi-Fi network and WBAN use the same unslotted CSMA/CA as MAC protocol, both of them can detect collision and proceed to avoid it. The common CSMA/CA algorithm used by the two networks is described in Figure 2.

The advantage of using a common contention-based CSMA/CA protocol is that the two networks sense the medium before proceeding

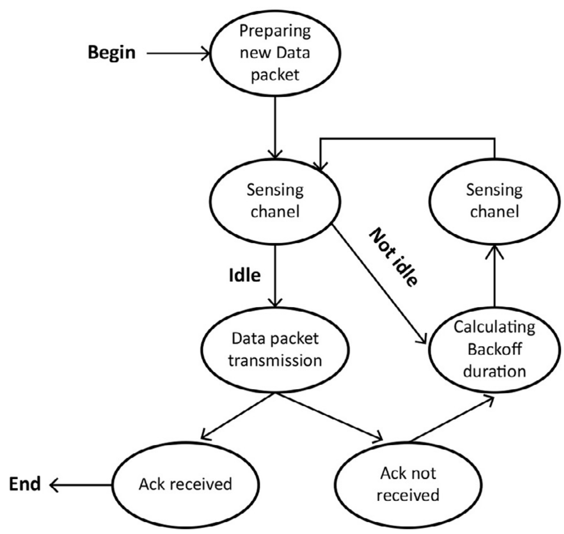

Figure 2. CSMA/CA algorithm for contention based MAC protocol. It is used by WBAN and Wi-Fi to sense the medium before the transmission which avoids collisions and interferences.

to transmission, which avoids collisions and interferences. However, they do not have the same process to calculate backoff duration and they do not have the same value of parameters.

When the WBAN based unslotted CSMA/CA node decides to transmit a data packet, it waits for a backoff period "*TWBANBackoff*". The WBAN backoff period consists of the time slot "*Tslot*" multiplied by a value picked from $[0, 2^{BE} - 1]$. Initially, the *BE* begins with $BE_{\min}$ and is increased in every failed attempt of transmission until reaching $BE_{\max}$. When the backoff period expires and the channel is found idle during the "*CCA*" duration, the WBAN node begins the transmission of his packet. If it is correctly transmitted, the WBAN node will receive an ACK before the "*SIFS*" period. If the backoff period expires and the channel is found busy, or if the packet is not correctly transmitted, *BE* and *NB* (number of backoff) will be incremented by 1 and the WBAN node will retry backoff process.

The IEEE 802.11 node starts transmission when it finds the medium free for Inter Frame Space Duration "*DIFS*". Otherwise, it picks a value "*CW*: Contention Window size" from $[1, CW_{\max}]$ and waits for backoff period "*TwifiBackoff*". The *CW* is decreased (–1) whenever the Wi-Fi node finds the medium free and paused when it is found busy. After the expiration of "*TwifiBackoff*", Wi-Fi node starts transmission. If it does not receive an ACK, it doubles the *CW* value and repeats the backoff process until obtaining successful transmission (*CW* becomes $CW_{\min}$) or until reaching the maximum number of retransmissions (then the packet will be deleted).

Parameters specifications of both WBAN and Wi-Fi MAC layer are described in Table 1. Although the CSMA/CA MAC protocol of the two networks can adapt well and can avoid collisions, the differences in parameter values make Wi-Fi more advantageous and less harmful for WBAN; the Wi-Fi network has larger packet size, lower waiting time to access the medium, higher transmission power and higher throughput.

4. Performance Improvement

In view of the resource constraints of WBAN's nodes, in this part, we aim to improve the WBAN reliability under Wi-Fi interference by introducing a simple and low cost method. The idea is to decrease the values of some WBAN's MAC parameters: the frame size, the CCA and the *Tslot*. First, we compare and analyze the effect of decreasing the values of these parameters *PARM*. Second, we discuss the effect of having lower values compared with the higher ones; and then we will perform progressive reductions to set the highest possible parameters that can be efficient and reliable in the current interferences conditions. The new value of one parameter $PARM_{new}$ is obtained by dividing the initial value $PARM_{initial}$ by a factor called $\alpha \in \{1, \ldots, \alpha_{\max} = 8\}$; the original parameter value is assigned when α is equal to 1:

Table 1. Parameter values used for WBAN and Wi-Fi MAC layer.

IEEE 802.15.4	
CCA	128 µs
MAC Frame size	512 Bytes
Tslot	320 µs
BE_{avg} *BE* *NB*	3 2 – 5 0 – 5
Data rate	250 Kbps
SIFS	192 µs
Ack size	5 Bytes
Tx power	1.1 mW

IEEE 802.11	
DIFS	28 µs
Frame size	11520 Bytes
Tslot	9 µs
CW_{avg}	8
Data rate	11 to 54 Mbps
SIFS	10 µs
Ack size	38 Bytes
Tx power	100 mW

$$PARM_{new} = \frac{PARM_{initial}}{\alpha} \tag{14}$$

The limit value of $FrameSize_{threshold}$, $CCA_{threshold}$ and $Tslot_{threshold}$ applied in our theoretical and simulation analysis is respectively 128 bits, 64 µs and 160 µs. It should be adjusted according to the WBAN application requirement.

$$FrameSize_{threshold} = Framesize_{initial} / \alpha_{\max}$$
$$CCA_{threshold} = CCA_{initial} / \alpha_{\max}$$
$$Tslot_{threshold} = Tslot_{initial} / \alpha_{\max}$$

The WBAN based IEEE 802.15.4 is not static and the emergence of Wi-Fi devices in close vicinity is not predictable. Therefore, mitigation strategy of WBAN based IEEE 802.15.4 system should deal with variable level of interference. Adaptive interference mitigation schemes have the advantages of interferences self-detecting, self-adaptation and self-adjustment. We conceived an adaptive algorithm Algorithm 1 that assigns the default values of parameters (*FrameSize*, *CCA* and *Tslot*) in favourable conditions and modifies them gradually in the case of successive data losses caused by interferences. α_1 is the divisor of the frame size, α_2 is the divisor of the *CCA* and α_3 is the divisor of the *Tslot*. α is general and represents the α_1, α_2 and the α_3. These values will not necessarily have the same values. For example, if the WBAN application does not accept a value less than 512 bytes to get the required data rate, α_1 remains equal to 1, $\alpha_{\max} = 1$ and $FrameSize_{threshold} = 512$ bytes; on the other hand, we can decrease the other values of *CCA* and *Tslot*. β is the incrementing value of α and it depends on the parameter to be adjusted.

The dynamic feature of the algorithm makes it suitable for all mobile networks that use the IEEE 802.15.4 (WBAN, vehicular network...) and that suddenly meet unexpected interfering Wi-Fi network.

The algorithm could be applied for other networks different from WBAN, provided that it determines the appropriate threshold values ($FrameSize_{threshold}$, $CCA_{threshold}$, $Tslot_{threshold}$) for the current application in which it offers the desired quality of service.

The progressive decrease of parameters checks the highest possible parameters that could be efficient and reliable. If there are no losses and the algorithm is set to the initial value, this may cause loss again. So, the progressive increase of the parameter value (decrease of α value) could be a good idea to be considered in our future work.

5. Theoretical Analysis

5.1. Probability of WBAN Successful Channel Access

In this subsection, we aim to study the probability of successful transmission in WBAN un-

Algorithm 1. Parameters adjustment algorithm to mitigate Wi-Fi interferences on Wireless Body Network. According to the previous results, we conceived this adaptive algorithm to assign the default values of parameters (*FrameSize*, *CCA* and *Tslot*) in the favourable conditions and modify them gradually in the case of successive data loss caused by interferences. α_1 is the divisor of the frame size, α_2 is the divisor of the *CCA* and α_3 is the divisor of the *Tslot*. β is the incrementing value of α and it depends on the parameter to be adjusted.

if (Ack not received before *SIFS* period)
  if ($FrameSize \le FrameSize_{threshold}$)
    $\alpha_1 = \alpha_1 + \beta_1$
    $FrameSize = \frac{FrameSize_{initial}}{\alpha_1}$
  end if
  if ($CCA \le CCA_{threshold}$)
    $\alpha_2 = \alpha_2 + \beta_2$
    $CCA = \frac{CCA_{initial}}{\alpha_2}$
  end if
  if ($Tslot \le Tslot_{threshold}$)
    $\alpha_3 = \alpha_3 + \beta_3$
    $Tslot = \frac{Tslot_{initial}}{\alpha_3}$
  end if
else
    $FrameSize = FrameSize_{\text{initial}}$
    $CCA = CCA_{\text{initial}}$
    $Tslot = Tslot_{initial}$
    $\alpha_1 = \alpha_2 = \alpha_3 = 1$
    end if

der Wi-Fi interferences. For simplicity, we assume that WBAN is composed of only 1 node in order to neglect the node contention effect in accessing the shared medium. Initially, we considered that the Wi-Fi network is composed of only 1 transmitter and we will study the effect of multiple Wi-Fi nodes in Section 6. We define two cases [5]: the first case in Figure 3 occurs when the Wi-Fi node is able to sense the WBAN transmissions; the second one in Figure 4 occurs when the Wi-Fi node is not able to sense WBAN transmissions.

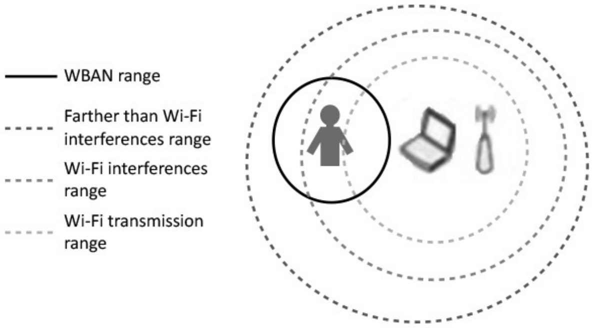

Figure 3. Case 1: The Wi-Fi node is able to sense WBAN transmissions because the body is inside Wi-Fi transmission range (before the Wi-Fi interferences range).

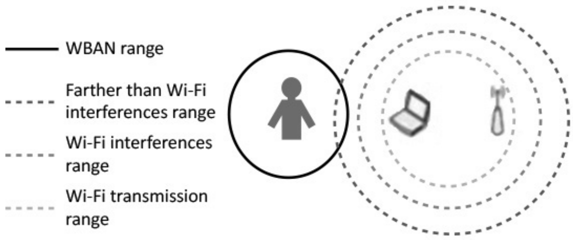

Figure 4. Case 2: The Wi-Fi node is not able to sense WBAN transmissions because the body is far from Wi-Fi transmission range.

To successfully transmit a WBAN packet, the duration DWBAN should at maximum be equal to the duration before transmitting a new Wi-Fi packet DWifi (Equation (1) and (2)).

$$DWBAN = DWifi \tag{1}$$

$$\begin{cases} Case\ 1: TWBANBackoff + CCA \\ \quad = IT + DIFS + TwifiBackoff \\ Case\ 2: TWBANBackoff + CCA + Tp \\ \quad + SIFS + Tack \\ \quad = IT + DIFS + TwifiBackoff \end{cases} \tag{2}$$

Accordingly, a WBAN node has successful transmission when the inter-arrival time of Wi-Fi packet $IT\min$ satisfies the Equations (3) and (4).

$$\begin{cases} Case\ 1: IT\min = TWBANBackoff + CCA \\ \quad - DIFS - TwifiBackoff \\ Case\ 2: IT\min = TWBANBackoff + CCA \\ \quad + Tp + SIFS + Tack \\ \quad - DIFS - TwifiBackoff \end{cases} \tag{3}$$

$$\begin{cases} Case\ 1: IT\min = Tslot * \left(2^{BE} - 1\right) + CCA \\ \quad - DIFS - Tslotwifi * CW \\ Case\ 2: IT\min = Tslot * \left(2^{BE} - 1\right) + CCA \\ \quad + Tp + SIFS + Tack \\ \quad - DIFS - Tslotwifi * CW \end{cases} \tag{4}$$

We model the inter-arrival time of Wi-Fi packet as an exponential distribution with data arrival of λ packets per second. The probability of successful WBAN channel access *Psucc* is given by this formula (5) [5]:

$$Psucc = \int_{IT\min}^{\infty} \lambda e^{\lambda t} = e^{-\lambda T\min} \tag{5}$$

The probability of successful WBAN transmission in the presence of *N* interfering Wi-Fi nodes is formulated as follows [5]:

$$Psucc(N) = \prod_{i=1}^{N} e^{-\lambda_i IT\min i} = e^{-N\lambda IT\min}$$

5.2. Delay of WBAN Packet Transmission

In this part, we aim to study the delay of WBAN packet transmission. The average delay T_{mean} is given by this formula (6):

$$\overline{T_{mean}} = \sum_{i=1}^{\infty} T(i) * P(i) \tag{6}$$

$T(i)$ and $P(i)$ are the delay of packet transmission and respectively, the probability to have successful transmission for the i-th essay. $T(i)$ and $P(i)$ are defined as follows:

$$T(i)\begin{cases} T(1) = T_{succ1} & (1^{\text{st}}\, essay) \\ T(2) = T_{fail1} + T_{succ2} & (2^{\text{nd}}\, essay) \\ T(3) = 2 * T_{fail2} + T_{succ3} & (3^{\text{rd}}\, essay) \\ \vdots & \\ T(i) = (i-1) T_{fail(i-1)} + T_{succ(i)} & (i^{\text{th}} essay) \end{cases} \tag{7}$$

$$T(i)\begin{cases} P(1) = 1-q & (1^{\text{st}}\, essay) \\ P(2) = q(1-q) & (2^{\text{nd}}\, essay) \\ P(3) = q^2(1-q) & (3^{\text{rd}}\, essay) \\ \vdots & \\ P(i) = q^{(i-1)}(q-1) & (i^{\text{th}} essay) \end{cases} \tag{8}$$

T_{succ} and T_{fail} are the duration of one transmission attempt in the successful case and, respectively, in the failed case. q is the probability to have failed transmission. T_{mean} can be expressed:

$$\begin{aligned}\overline{T_{mean}} &= (1-q) T_{succ1} + q(1-q)\left(T_{succ2} + T_{fail1}\right) \\ &+ q^2(1-q)\left(T_{succ3} + T_{fail1} + T_{fail2}\right) + \ldots \\ &+ q^i(1-q)\left(T_{succi} + T_{fail1} + T_{fail2} + \ldots + T_{fail(i-1)}\right) \approx 0\end{aligned} \tag{9}$$

$$\overline{T_{mean}} \approx (1-q) T_{succ1} + q(1-q)\left(T_{succ2} + T_{fail1}\right)$$

T_{succ1} and T_{succ2} can be written as:

$$\begin{aligned}T_{succ1} &= Tslot * \left(2^{BEinitial} - 1\right) + CAA \\ &+ Tp + SIFS + Tack\end{aligned} \tag{10}$$

$$\begin{aligned}T_{succ2} &= Tslot * \left(2^{BEinitial+1} - 1\right) + CAA \\ &+ Tp + SIFS + Tack\end{aligned} \tag{11}$$

To define T_{fail1}, two cases are presented:

Case 1 (Figure 3)**:** In this case, WBAN nodes and Wi-Fi nodes are able to detect the transmission of each other. Then, the WBAN node's transmission will fail because it found the channel busy. For the second essay of transmission, $BE_{initial}$ will be increased by 1.

Case 2 (Figure 4)**:** WBAN nodes and Wi-Fi nodes are not able to detect the transmission of each other. Then, WBAN node's transmission will fail due to packet collision and the missing of Ack. For the second attempt of transmission, $BE_{initial}$ will be increased by 1.

Accordingly, T_{fail1} would be expressed as follows:

$$\begin{cases} Case\ 1: T_{fail1} = Tslot * \left(2^{BEinitial} - 1\right) + CCA \\ Case\ 2: T_{fail1} = Tslot * \left(2^{BEinitial} - 1\right) + CCA \\ \qquad + Tp + SIFS + Tack \end{cases} \tag{12}$$

The resulted T_{mean} becomes:

$$\overline{T_{mean}} \approx T_{succ1} + q\left(T_{fail1} + Tslot * 2^{BEinitial}\right) \tag{13}$$

5.3. Results and Discussion

The studies in [16], [17] show the effect of the distance between the two networks on the IEEE 802.15.4 packet reception rate PRR. They have proved that as the distance between Wi-Fi node and IEEE 802.15.4 nodes is increased, the PRR also increases. The authors in [16] elucidate that there is not much difference in PRR when the interferer is 8 m away and when there is no interferer; whereas the authors in [17] prove that 100% of valid packets are received more than 35 meters away from IEEE 802.11g network. This might be because extending the distance weakens the Wi-Fi transmission power which increases the signal-to-noise of the receiver and, accordingly, reduces the bit error rate and the packet error rate.

Even if the WBAN is in the Wi-Fi coverage, it is possible that, at the last few meters (before getting out of its coverage), the Wi-Fi cannot hear the WBAN transmissions, which will cause packets collisions or WBAN packets retentions, whatever the strength of the Wi-Fi transmission power. In our study, we will explain the positioning effect of the WBAN over the Wi-Fi network range (1st case: the Wi-Fi is near and able to listen to WBAN transmission; 2nd case where Wi-Fi is far and is not able to listen to WBAN transmission), because this has a significant impact on the time slot reservation and, accordingly, on the reliability of packet transmission.

The probability of successful packet transmission in WBAN is described in Figures 5 and 6. The mean delay of WBAN packet transmission is presented in Figure 7.

Results elucidate that the reliability is significantly better when the WBAN node is localized before the interference range of Wi-Fi node (case 1). Because, while WBAN node is transmitting, the Wi-Fi node senses the medium, finds it busy and waits until the transmission is completed. However, in the second case, the Wi-Fi node is not able to detect WBAN transmissions. Thus, when it begins packet transmission, collision can occur. The Wi-Fi packet will not be very affected by WBAN packet and considers it as noise, because it uses larger packet size and higher transmission power. In contrast, the WBAN packet will be affected and dropped.

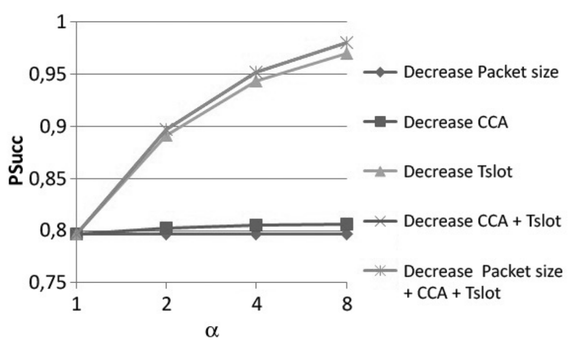

Figure 5. The probability of WBAN successful transmissions with different scenarios (Case 1). PSucc has been significantly better when the WBAN node is localized at the interference range of Wi-Fi node. Because, while WBAN node is transmitting, the Wi-Fi node sensed the medium, found it busy and waited until the transmission was completed. The decrease of *Tslot* and the decrease of *Tslot* and *CCA* show improvement in *PSucc*. However, the decrease of Packet size has no effect in this case. The line of (decrease Packet size + *CCA* + *Tslot*) hides the line of (Decrease of *CCA* and *Tslot*).

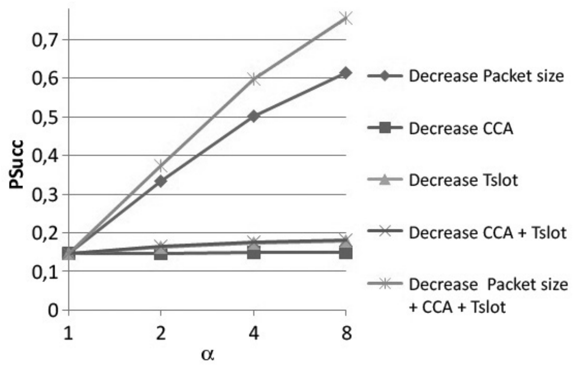

Figure 6. The probability of WBAN successful transmissions with different scenarios (Case 2). The Wi-Fi node is not able to detect WBAN transmissions. Thus, when it begins packet transmission, the collision will occurr. The decrease of packet size and the decrease of all parameters show improvement in *PSucc*.

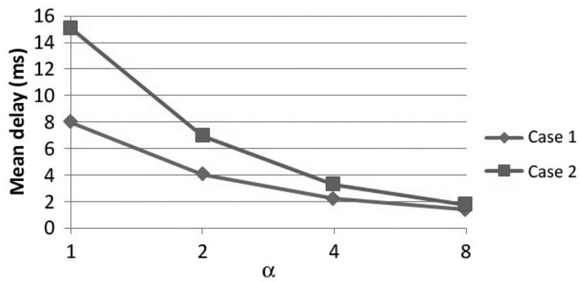

Figure 7. The mean delay of WBAN packet transmission under one interfering Wi-Fi node. The delay of packet transmission is better in the case 1 than the case 2 and it is improved in both cases.

For the first case, results indicate that the decrease of *Tslot* improves the probability of successful transmission in WBAN; as for the second case, the decrease of packet size makes improvement. For both cases, the decrease of the three parameters (*CCA*, *Tslot* and the packet size) at the same time gives the best results. In the first case, the decrease of *CCA* and *Tslot* produces the same results as the decrease of the three parameters. This is because the decrease of packet size has no effect on *PSucc*.

Even if the two networks can listen to each other, the difference in their *MAC* layer operation makes the Wi-Fi network more advantageous to access the shared medium. WBAN node has longer waiting durations before accessing the channel, compared to Wi-Fi devices. The "*CCA*" and "*TWBANBackoff*" time of IEEE 802.15.4 are longer than "*DIFS*" and "*Twifi-Backoff*". Then, the Wi-Fi nodes are the fastest to access the channel, because its backoff counter reaches zero earlier than the backoff used by IEEE 802.15.4.

Figure 7 shows that the mean delay of WBAN packet transmission is better in the case 1 and it decreases when the value of alpha is increased.

Generally, the results show that the decrease of all the three parameter values is the best case to improve the probability of successful WBAN transmission and the mean delay of WBAN packet transmission, either in the first case or in the second case.

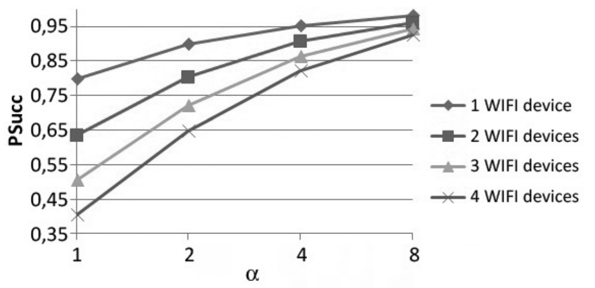

Figure 8. Improvement of the probability of WBAN successful transmissions with *N* interfering Wi-Fi nodes using our parameters adjusment approach (case 1). *Psucc* was improved in a convergent manner whenever *α* value was increased.

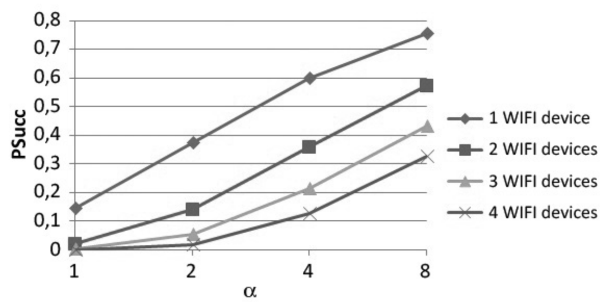

Figure 9. Improvement of the probability of WBAN successful transmissions with *N* interfering Wi-Fi nodes using our parameters adjusment approach (case 2). *Psucc* was improved in a slightly divergent manner whenever *α* value was increased.

Results in Figures 8 and 9 show that *Psucc* has been affected also by the number of interfering Wi-Fi nodes. They also show that *Psucc* is improved in both cases whenever α value is increased. Results in Figure 10 show that there is no significant effect of the number of Wi-Fi nodes on the mean delay of WBAN packet transmission. A successful packet transmission takes less duration when the WBAN node is localized before the interference range of Wi-Fi node (the first case), and it is considerably decreased by the increase of *α* value.

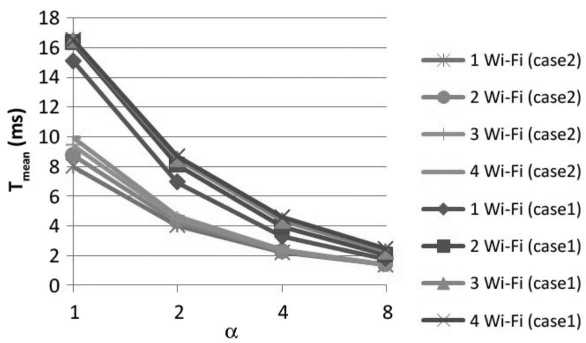

Figure 10. The mean delay of WBAN packet transmission under *N*-interfering Wi-Fi nodes (cases 1 and 2). A successful packet transmission takes less duration when the WBAN node is localized before the interference range of Wi-Fi node (the first case).

6. Simulation Analysis

6.1. Simulation Set Up

In this section, we conduct the simulation to investigate potential interference effect of Wi-Fi on WBAN and to demonstrate the effectiveness of our proposal in improving the reliability of the body network. The experiment is performed using MiXiM framework of OMNET++ simulator. We adopt MoBAN [18] (a configurable mobility model for WBAN) as an adequate model for the particular mobility of the WBAN and the movement of the body's parts. It is available as an add-on in the mobility framework of the MiXiM simulator. It is able to precisely model the posture of the body and the movement's behaviour and it can be configured to be used for performance evaluation of different scenarios. The number of sensors is set to 12. Figure

11 describes the body's nodes positions in our simulation. The WBAN is simulated to move in a space area of 100 m^2 and change posture and places periodically. The possible postures are "running", "walking", "sitting", "standing" and "lying down".

We consider the default parameters of IEEE 802.11 for Wi-Fi and IEEE 802.15.4 for WBAN. In Wi-Fi nodes, we do not consider the RTS/CTS mechanism and the packet size was set to be 1440 bytes where the network operates under maximum offered load [5]. Using the "TrafficGen" application, WBAN's nodes and Wi-Fi's nodes periodically generate broadcast messages using respectively Inter-departure packet time of 0.01 s and 0.001 s. For example, the inter-departure time of packet of ECG application is every 0.004 s (sampling rate of 250 Hz). This makes our experiment operate in faster packet generation. The scenarios of this experiment are somewhat strict in terms of the number and the traffic rate of the interfering networks and in terms of the number of the WBAN nodes; this is in order to evaluate the performance of the WBAN network and our method in the worst conditions. Moreover, the limit value of $FrameSize_{threshold}$, $CCA_{threshold}$ and $Tslot_{threshold}$ can be adjusted according to the WBAN application requirement; in this simulation we consider respectively the value of 128 bits, 64 μs and 160 μs.

The choice of $Framesize_{threshold}$ depends on the application quality of service. For example, the real time electrocardiogram (ECG) of 3 leads requires a payload of 48 bits (3 $*$ 16 bits = 3 $*$ sampling resolution) and a MAC header of 13 bytes (104 bits) [19]; the ECG packet size becomes 152 bits (19 bytes).

The Carrier sense of the CSMA/CA detects if there exists the Wi-Fi signal, then the *CCA* reports that the medium is busy. We reduced the sensing duration in order to minimize the waiting time before transmission. The IEEE 802.11g has a very short sensing period of 28 μs which makes him faster to gain the medium access. We set the $CCA_{threshold}$ to 64 μs in order to sense 16 bits ($250 \cdot 10^3 * 64 \cdot 10^{-3} = 16$ bits) of IEEE 802.15.4 frame and 3456 ($54 \cdot 10^6 * 64 \cdot 10^{-6} = 3456$ bits) bits of Wi-Fi frame transmitted in the medium. We tested the $Tslot_{threshold}$ of 160 μs which is half of the original *Tslot* value ($\alpha_3 = 2$). We tested theoretically the impact of having reduction in *Framesize*, *CCA*, *Tslot*. However, the effects of changing the threshold values of these parameters are theoretically presented, they are not tested in the simulation and could be an interesting contribution for our incoming work.

The initial value of α is 1, it also represents the minimum value. The maximum α value is defined whenever the threshold value of the parameter is reached. The α value increases in the case of data loss and whenever the threshold value of the parameter is not reached; and it decreases otherwise.

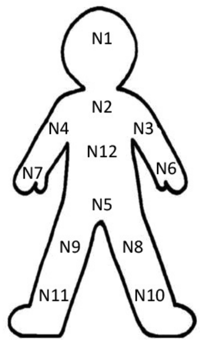

Figure 11. The body's nodes position. Nodes' names are from *N*1 to *N*12.

6.2. Simulation Results

Decreasing only the *Backoffs unit* time and the *CCA* time reduces the waiting time before transmitting, which improves the delay of WBAN packet transmission. However, in our previous study [2], we showed that this increases the number of dropped packets and the number of *Backoff*. It is because after the expiration of these two periods, it is more likely that the medium will be found busy due to the long propagation duration of the large packet. In our present approach, which reduces the packet size in addition to the *Backoff unit time* and the *CCA* time, the node finds the medium free after a shorter period and the propagation delay of the packet is reduced. Researchers in [20] have shown also that the packet length can affect the reliability of IEEE 802.15.4 under Wi-Fi interference; accordingly, they also take advantage of this parameter to improve the desired packets' chance of survival. They proposed a dynamic mechanism that decreases the effective data payload length with the increase of Wi-Fi traffic rate. However, relying only on this parameter may decrease the throughput of WBAN system, which cannot be suitable for a lot of applications. In our proposed algorithm, we exploited the effectiveness of this parameter and other important MAC parameters responsible for the access policies to the shared medium (*CCA* and *Tslot*).

The results of the simulation of our approach are presented in Figures 12, 13 and 14. They show that with this method, the number of dropped packets, the number of *Backoffs* and the transmission delay are decreased.

The increased number of Wi-Fi nodes devices that concurrently want to access the shared medium increases the interfering traffic in the shared medium. This consequently increases the probability of IEEE 802.15.4 packet collision. Researchers in [20] admitted also that the high traffic of Wi-Fi increases the level of interference. "When the Wi-Fi traffic rate is over 500 packets/second, there is very little chance for the strategy to locate the idle slots due to the high duty cycle of Wi-Fi system" [20]. In our experiment, the results show an increase of backoff number, the delay and packet drop with the increase of the number of Wi-Fi devices.

The dynamic feature of the algorithm makes it suitable for all mobile networks that use the IEEE 802.15.4 (WBAN, vehicular network...) and (suddenly) meet unexpected interfering Wi-Fi network.

A frequency agility based interference avoidance algorithm has been proposed in [21], it

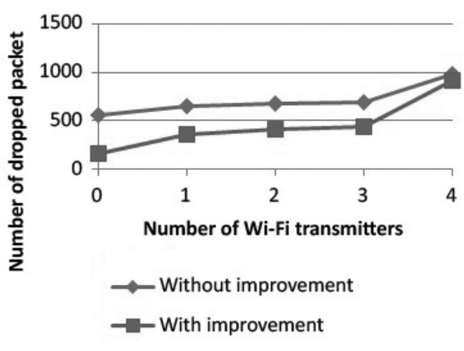

Figure 12. Number of dropped packets in WBAN. Simulation results show that our approach decreases the number of dropped packets.

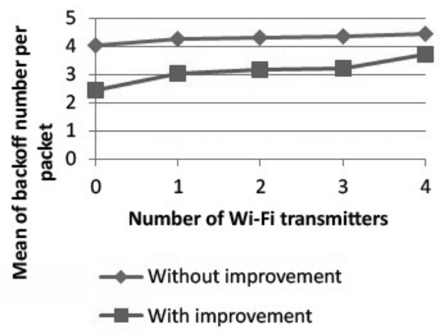

Figure 13. Means of backoff number per WBAN packet. Simulation results show that our approach decreases the number of backoff.

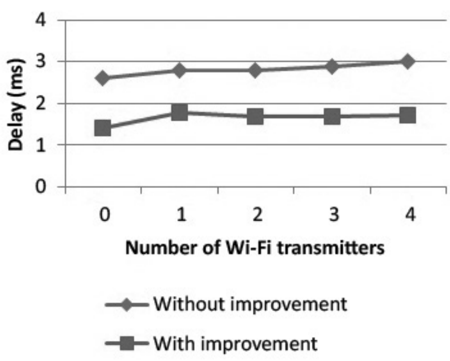

Figure 14. Delay of packet transmission in WBAN. Simulation results show that our approach decreases the transmission delay.

detects interference and adaptively switches nodes to safe channel to dynamically avoid WLAN interference. As we have shown previously, simulation results also show that failed transmissions are much higher under the heavy interferences. However, there is not a big difference in the results when the algorithm changes the channel frequency. Moreover, studies in [22] indicate that channelization and hopping to a new channel take time when the interferences vary faster than the MAC controller can adapt [23].

In [23], the authors propose an adaptive algorithm that adjusts a higher transmission power, lower packet size and higher inter-departure time of packet when it detects performance degradation in the presence of Wi-Fi interferences. According to [24], [25], the smaller the packet size, the less it is to suffer from interference. Increase of the packet size engenders higher data throughput, higher RAM (Random Access

Memory) consumption and increases the probability of data collision in the presence of interferences [25]. In [23], the dynamic setting of packet size improves packets transmission just as we have shown in our experiment. However, in our theoretical study, the probability of successful transmissions is improved when decreasing the packet size only if the Wi-Fi node is not able to detect WBAN transmissions. The authors in [23] also explain that dynamic increase of the inter-sending time of data packets leads to the traffic minimization in the presence of interference and reduces the probability of collision with Wi-Fi packets. However, this may be applicable only for applications that do not need real time data sending like heart beat monitoring. They also dynamically increase the transmission power in order to resist the high Wi-Fi transmission power. This improves the reliability of data transmission, but consumes more energy in cases of interferences. Thus, a good selection of threshold values in the dynamic algorithm maintains the required quality of service while resisting Wi-Fi interferences. The effects of choosing different threshold values in our dynamic algorithm are theoretically showed, but not tested in our simulation analysis; this could be an interesting contribution for our incoming work.

Another point to be improved in our adaptive algorithm is that the detection of transmission failure is not restricted to the non-reception of ACK packet after sending the packet, but also it is due to the channel access failures. Studies in [26] propose a new estimator consisting of merging the Clear Channel Assessment count with the Packet Reception Rate. Results show that this distinguishes persistent IEEE 802.11 bgn traffic more robustly.

7. Conclusion

To avoid Wi-Fi interferences from the WBAN network, we followed a well-defined approach. We used first the IEEE 802.15.4 technology which is more suitable for the WBAN, and next we favored the use of CSMA/CA MAC protocol, the most robust against Wi-Fi interference. The non-bacon CSMA/CA is more scalable and it does not need expensive processing and time synchronization. Moreover, it is more robust in the presence of Wi-Fi interference. Wi-Fi networks and any network that uses CSMA/CA as MAC protocol could detect collisions and proceed to avoid it. The advantage of using a common contention-based CSMA/CA protocol is that the two networks sense the medium before proceeding to transmission, which avoids collisions and interferences. However, data collisions still occur between the two networks. This is because they do not have the same process to calculate Backoff duration and they do not have the same value of MAC parameters. The differences of parameter values make the Wi-Fi more advantageous and harmful for WBAN; the Wi-Fi network has larger packet size, smaller waiting time to access the medium, higher transmission power and higher throughput (Table 1). There are many efficient methods to avoid the effect of Wi-Fi interferences, but they could not be applied for the constrained WBAN network. An adequate adjustment of conveniently tested parameter values in the MAC protocol of the WBAN is a simpler and uncomplicated method that helps to optimize the coexistence of both networks. It consists of decreasing the value of packet size, *CCA* duration and backoff timeslot. This does not require complex processing, expensive communication, or installation of extra equipment. This makes it convenient for the limited size battery, memory and process of the WBAN. Moreover, variability of the environment due to the mobility of WBAN prefers a setting of the appropriate values according to the presence of interference. Then, we conceived a dynamic algorithm that assigns the default values of parameters in favourable conditions (to maintain the original standard and good data rate) and modifies them in the case of data losses caused by interferences. Theoretical results showed that the probability and the mean delay of successful WBAN transmission have been considerably improved even in the presence of higher number of Wi-Fi nodes. Simulation results also show that our approach reduces the number of dropped packets, the number of backoffs and the transmission delay.

In the next work, we aim to compare these results with real experiments. Other open issues which remain important are the effects of the body shadowing and movement on the reliability of WBAN.

References

[1] E. Sarra *et al.*, "Coexistence Improvement of Wearable Body Area Network (WBAN) In Medical Environment", in *IEEE International Conference on Communications*, Australia, 2014, pp. 5694–5699.
https://doi.org/10.1109/ICC.2014.6884229

[2] S. Essafi and E. Tahar, "Performance Improvement of the Wireless Body Area Network (WBAN) under Interferences", in *IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*, Munich, Germany, 2016, pp 1–6.
https://doi.org/10.1109/HealthCom.2016.7749507

[3] J. A. Mohamad *et al.*, "Dynamic Channel Access Scheme for Interference Mitigation in Relay-assisted Intra-WBANs", in *International Conference on Protocol Engineering (ICPE) and International Conference on New Technologies of Distributed Systems (NTDS)*, 2015, pp 1–6.
https://doi.org/10.1109/NOTERE.2015.7293511

[4] S. Essafi and E. Tahar, "Co-channel Interference In Wireless Body Area Network: Mitigations and Challenges", *Global Summit on Computer and Information Technology*, Sousse, Tunisia, 2017.

[5] H. Thaier *et al.*, "A Survey of Wireless Technologies Coexistence in WBAN: Analysis and Open Research Issues", *Wireless Networks*, vol. 20, pp. 2165–2199, 2014.
https://doi.org/10.1007/s11276-014-0736-8

[6] M. Jose, "A Study on Power Consumption for Internet of Thing", Master thesis in Innovation and Research in Informatics, FIB, Barcelona.

[7] K. Jasleen, "Wirless Body Area Network: Comparison of IEEE 802.15.4 an IEEE 802.15.6", M.E-information security, THAPAR University, PATIALA.

[8] L. Benoit *et al.*, "A Survey on Wireless Body Area Networks", *Wireless Networks*, vol. 17, pp 1–18.
https://doi.org/10.1007/s11276-010-0252-4

[9] J. S. Ranjit and S. Shin, "A Modified IEEE 802.15.4 Superframe Structure for Guaranteed Handling in Wireless Body Area Network", *Network Protocol and Algorithm*, vol. 5, 2013.
https://doi.org/10.5296/npa.v5i2.3375

[10] Z. Mengchuan *et al.*, "Distributed Scheduling of Enhanced Beacons for IEEE802.15.4-TSCH Body Area Networks", in *ADHOC-NOW 2016: Ad-hoc, Mobile, and Wireless Networks*, 2016, pp. 3–16.
https://doi.org/10.1007/978-3-319-40509-4_1

[11] G. Reema *et al.*, "MAC Protocols in Wireless Body Area Networks: A Review", Int. J. Comput. Appl., vol. 140, pp. 0975–8887, 2016.
https://doi.org/10.5120/ijca2016909446

[12] K. Yena *et al.*, "Coexistence of ZigBee-Based WBAN and WiFi for Health Telemonitoring Systems", *IEEE Journal of Biomedical and Health Informatics*, vol. 20, pp. 222–230, 2016.
https://doi.org/10.1109/JBHI.2014.2387867

[13] J. Hou *et al.*, "Minimizing 802.11 Interference on Zigbee Medical Sensors", in *BodyNets '09 Proceedings of the Fourth International Conference on Body Area Networks ICST*, Los Angeles, California, 2009, article no. 5.
https://doi.org/10.4108/ICST.BODYNETS2009.6029

[14] Y. Tang *et al.*, "Study of Clear Channel Assessment Mechanism for ZigBee Packet Transmission Under Wi-Fi Interference", in *2013 IEEE 10th Consumer Communications and Networking Conference (CCNC)*, pp. 765–768.
https://doi.org/10.1109/CCNC.2013.6488545

[15] W. B.Yang and K Sayrafian, "Interference Mitigation Using Adaptive Schemes in Body Area Networks", *International Journal of Wireless Information Networks*, vol. 19, no. 3, pp. 193–200.
https://doi.org/10.1007/s10776-012-0192-2

[16] D. Mankar and S. Bharat, "Dynamic Performance Analysis of IEEE 802.15.4 Devices under Various RF Interferences", *International Conference on Inventive Computation Technologies (ICICT)*, 2016.
https://doi.org/10.1109/INVENTIVE.2016.7823212

[17] C. Mike Liang *et al.*, "Surviving Wi-Fi Interference in Low Power ZigBee Networks", *SenSys'10*.
https://doi.org/10.1145/1869983.1870014

[18] M. Nabi *et al.*, "A Configurable Mobility Model for Wireless Body Area Networks", in *4th International Conference on Simulation Tools and Techniques ICST*, 2011.
https://doi.org/10.4108/icst.simutools.2011.245511

[19] X. Liang and I. Balasingham, "Performance Analysis of the IEEE 802.15.4 Based ECG Monitoring Network", *Proceedings of the Seventh IASTED International Conference Wireless and Optical Communications*.
https://doi.org/10.1.1.460.5356

[20] F. Yao and S. Yang, "Mitigating Interference in IEEE 802.15.4 Network with Dynamic Energy", in *9th IEEE International Conference on Networking, Sensing and Control (ICNSC)*, 2012.
https://doi.org/10.1109/ICNSC.2012.6204907

[21] S. Wagh Sharad *et al.*, "Performance Evaluation of IEEE 802.15.4 Protocol Under Coexistence of WiFi 802.11b", *Procedia Computer Science*, vol. 57, pp. 745–751, 2015.
https://doi.org/10.1016/j.procs.2015.07.467

[22] L. W. Hanlen *et al.*, "Cochannel Interference in Body Area Networks with Indoor Measurements at 2.4 GHZ: Distance-to-Interferer is a Poor Estimate of Received Interference Power", *Interna-*

tional Journal of Wireless Information Networks, vol. 17, pp. 113–125, 2010. https://doi.org/10.1007/s10776-010-0123-z

[23] S Essafi *et al*., "Coexistence Improvement of Wearable Body Area Network (WBAN) in Medical Environment", *IEEE ICC 2014 – Wireless Communications Symposium*, 2014. https://doi.org/10.1109/ICC.2014.6884229

[24] A. Vlavianos *et al*., "Assessing Link Quality in IEEE 802.11 Wireless Networks: Which is the Right Metric?", *IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications – PIMRC*, 2008, pp. 1–6. https://doi.org/10.1109/PIMRC.2008.4699837

[25] O. Gnawali *et al*., "Collection Tree Protocol", *Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems (SenSys 2009)*, Berkeley CA USA, 2009. https://doi.org/10.1145/1644038.1644040

[26] C. Leong Lim *et al*., "Dynamic Performance of IEEE 802.15.4 Devices Under Persistent WiFi Traffic", *International Conference on Recent Advances in Internet of Things (RIoT)*, 2015. https://doi.org/10.1109/RIOT.2015.7104914

Received: October 2017
Revised: July 2018
Accepted: July 2018

Contact addresses:
Sarra Essafi
Communication System Laboratory Sys'Com
National Engineering School of Tunis
University Tunis El Manar
Tunis, Tunisia
e-mail: sarra.essafi.pro@gmail.com

Tahar Ezzedine
Communication System Laboratory Sys'Com
National Engineering School of Tunis
University Tunis El Manar
Tunis, Tunisia
e-mail: tahar.ezzedine@enit.rnu.tn

SARRA ESSAFI received a PhD from National Engineering School of Tunis at the University of Tunis El Manar Tunis, Tunisia. She is a researcher in Communication System Laboratory. She obtained a Master degree in computing specialty network from UPMC Sorbonne University Paris 6. Her research interests lie in the area of wireless networks, wireless sensor network (WSN) and wireless body area network (WBAN). Her studies focused on providing the reliability of networks through theoretical, simulated and real experience. Since 2013, she has collaborated with LIPADE Laboratory at the University of Paris Descartes (Paris 5) and AlianStic Laboratory at ESIGETEL University.

TAHAR EZZEDINE received the MSc degree, the PhD degree and the HDR degree in Telecommunications, all from the National School of Engineers of Tunis (ENIT), Tunisia. He is currently a Full Professor at the Department of Information and Communication Technology and founder/leader of an R&D group for research and development of wireless sensors network in different fields enclosing GIS systems at SysCom Research Lab. His interests also include smart objects and IOT.