Improving the Communication Reliability of Body Sensor Networks Based on the IEEE 802.15.4 Protocol

Diogo Gomes, MSc, and José A. Afonso, PhD

Algoritmi Center, University of Minho, Campus of Azurem, Guimarães, Portugal.

Abstract

Body sensor networks (BSNs) enable continuous monitoring of patients anywhere, with minimum constraints to daily life activities. Although the IEEE 802.15.4 and ZigBee® (ZigBee Alliance, San Ramon, CA) standards were mainly developed for use in wireless sensors network (WSN) applications, they are also widely used in BSN applications because of device characteristics such as low power, low cost, and small form factor. However, compared with WSNs, BSNs present some very distinctive characteristics in terms of traffic and mobility patterns, heterogeneity of the nodes, and quality of service requirements. This article evaluates the suitability of the carrier sense multiple access–collision avoidance protocol, used by the IEEE 802.15.4 and ZigBee standards, for data-intensive BSN applications, through the execution of experimental tests in different evaluation scenarios, in order to take into account the effects of contention, clock drift, and hidden nodes on the communication reliability. Results show that the delivery ratio may decrease substantially during transitory periods, which can last for several minutes, to a minimum of 90% with retransmissions and 13% without retransmissions. This article also proposes and evaluates the performance of the BSN contention avoidance mechanism, which was designed to solve the identified reliability problems. This mechanism was able to restore the delivery ratio to 100% even in the scenario without retransmissions.

Key words: *body sensor networks, IEEE 802.15.4, ZigBee, communication reliability, hidden nodes, clock drift*

Introduction

Mobile telemedicine systems based on body sensor networks (BSNs) allow patients to engage in their daily life activities while they are monitored continuously anytime, anywhere. A BSN is mainly composed of wearable or implantable sensor devices and a wireless network to transport the collected data from the users' bodies to an outside location.[1] BSNs can be used to monitor diverse body parameters, such as temperature, blood pressure, oxygen saturation, body posture, electroencephalogram, and electrocardiogram (ECG).[2] BSN-based monitoring can provide substantial benefits both to the patients and to the healthcare system, contributing to increase the quality and reduce the cost of healthcare. The continuous patient monitoring during long periods made possible by BSNs enables the early detection and prevention of conditions that cannot always be identified using conventional monitoring equipment during short sessions, replacing more expensive treatments later on. In this sense, BSNs can be used to detect, for example, episodic abnormalities such as transient surges in blood pressure or arrhythmias, which are associated with many cardiac diseases.[3,4] Other applications areas of BSNs include rehabilitation[5] and biofeedback.[6]

The IEEE 802.15.4 standard[7] specifies both the physical and medium access control (MAC) layers for low power, low data rate, and low-cost wireless network devices. The physical layer uses the direct sequence spread spectrum and defines different transmission rates and bands: 250 kilobits per second (Kbps) for the 2.4-GHz band and 20/40 Kbps for the 868/915-MHz band, among other possible optional configurations. The MAC layer defines two different operation modes: a non–beacon-enabled mode, which uses an unslotted carrier sense multiple access–collision avoidance (CSMA-CA) algorithm, and a beacon-enabled mode, which defines a superframe structure and uses a slotted CSMA-CA variation. An optional scheme, called guaranteed time slot (GTS), which allows the allocation of dedicated slots for the nodes in the superframes, is also defined by the standard.

ZigBee®[8,9] (ZigBee Alliance, San Ramon, CA) is a low-power wireless network standard designed for monitoring and control applications. The two lower layers of ZigBee are specified by the IEEE 802.15.4 standard. Above these layers, the ZigBee stack defines several other layers, including the network and application layers. The ZigBee standard supports star and multihop topologies.

IEEE 802.15.4 and ZigBee are widely adopted standards conceived primarily for use in wireless sensor networks (WSNs), with multiple compliant devices on the market from several manufacturers. Currently, these are also the most widely used standards in BSNs.[1,2]

BSNs share some characteristics with WSNs, such as the concern with the cost, size, and energy consumption of the sensor devices; however, they present some significant differences. BSNs usually generate periodic and, frequently, data-intensive traffic (e.g., ECG, electroencephalogram, and body posture), in contrast with WSNs, which typically generate event-based and low data rate traffic. Many BSNs are also composed by heterogeneous nodes with different traffic rates and capabilities, whereas most WSNs are composed by homogeneous sensor nodes. BSNs applications also tend to impose more strict quality of service requirements[10] to the wireless network in terms of communication reliability and delay.

This article evaluates the suitability of the unslotted CSMA-CA protocol, used by the IEEE 802.15.4 and ZigBee standards, for data-intensive BSN applications, through the execution of experimental tests in different evaluation scenarios, in order to take into account the effects of contention, clock drift, and hidden nodes on the performance of the network. The main quality of service metric evaluated in this article is the delivery ratio (DR), which is a measure of the communication reliability of the network. This article also proposes and evaluates the performance of BSN contention avoidance (BCA), a low-complexity MAC mechanism designed to solve the problems identified during the evaluation of the CSMA-CA protocol.

Several works in the literature present performance evaluation results regarding IEEE 802.15.4 and/or ZigBee protocols, for different application scenarios, based on analytical models[11–13] or simulations.[14,15] On the other hand, this article, by relying on experimental results, takes into account variables present in real-world implementations that have impact on performance but are overlooked in most theoretical models, such as the processing load at the software stack in the network nodes.

Two research groups[16,17] have presented experimental results concerning the DR of IEEE 802.15.4-based and ZigBee-based BSN systems, respectively. In both cases, the measured DR was above 99.9%. However, these works use only sensors that generate low data rate traffic (blood pressure, heart rate, and blood oxygen saturation monitors); therefore, most of the time the sensor nodes do not have to compete to transmit their data packets. This article, on the other hand, considers the use of sensor nodes that generate data-intensive traffic, which poses the problem of contention. Reliability problems have been addressed in the transport of ECG traffic on ZigBee networks related with the presence of hidden nodes and clock drift effects.[18] However, unlike this report the authors do not propose a solution to these problems.

Evaluation Materials and Methods

GENERAL CONFIGURATIONS

The hardware platform used in the tests was the CC2530 development kit, which is provided by Texas Instruments (Dallas, TX), a leading supplier of ZigBee products. It is based on the CC2530[19] system on chip, which integrates a microcontroller and a transceiver in the same chip. The microcontroller is based on the 8051 architecture, whereas the transceiver is compliant with the IEEE 802.15.4 standard in the 2.4-GHz frequency band. The ZigBee stack provided by Texas Instruments is called Z-Stack. This work uses the version Z-Stack-CC2530-2.4.0-1.4.0, which supports the two stack profiles of the ZigBee 2007 specification: ZigBee and ZigBee Pro.

All tests were made using a star topology composed by ZigBee end devices (EDs) (representing the BSN sensor nodes) that generate and send data packets periodically to the ZigBee coordinator using the IEEE 802.15.4 unslotted CSMA-CA algorithm. The main quality of service metric evaluated was the DR, which is the ratio of the number of successfully delivered packets to the number of packets generated by the source node application.

The IEEE 802.15.4 channel 26 was used in the tests because of the absence of interference from other sources, such as nearby Wi-Fi networks, which was verified using a spectrum analyzer. Likewise, the transmission power and placement of the nodes were set to assure there were no packet losses due to path loss or shadowing effects between the EDs and the coordinator because the purpose of this study was to evaluate only the losses due to collisions caused by contention, clock drift, and hidden nodes.

Table 1 displays relevant IEEE 802.15.4 parameters, in the context of the experiments presented in this article, and their respective values. For the variable parameters, the default values were used. In the tests without retransmissions, the acknowledgment frame was not transmitted. Each test finished after the coordinator received 5,000 packets from the end devices. The tests presented in this article used the ZigBee Pro stack profile. In these tests, the periodic ZigBee Pro link status messages and IEEE 802.15.4 data requests commands were disabled. Other tests were performed using the ZigBee stack profile and with these commands enabled, but no relevant differences were observed.

The tests used traffic parameters from a wearable motion capture system[20] for body posture monitoring, based on inertial sensors that were developed using the same CC2530 modules used in this article. Each sensor node in this system contained six sensors (three accelerometers and three magnetometers). Typical motion capture applications require a frame rate of 30 frames per second; therefore, the sensors are sampled at 30 Hz. The data packet generation interval was set to 100 ms, which means that each packet carries three samples from each one of the six sensors, for a total of 18 samples of 12 bits each. A 16-bit sample of the node's battery voltage was also included;

Table 1. Relevant IEEE 802.15.4 Parameters

PARAMETER	VALUE
Data rate (at the 2.4-GHz band)	250 Kbps
Symbol period (at the 2.4-GHz band)	16 μs
The maximum number of backoffs that CSMA-CA will attempt before declaring channel access failure (macMaxCSMABackoffs) (default = 4)	[0.5]
The minimum value of the CSMA-CA backoff exponent (macMinBE) (default = 3)	[0–3]
The maximum value of the CSMA-CA backoff exponent (macMaxBE)	5
The number of symbols forming a unit backoff period (aUnitBackoffPeriod)	20
Turnaround time (at the 2.4-GHz band)	192 μs
The maximum number of retransmissions allowed by the 802.15.4 MAC layer after a transmission failure (aMaxFrameRetries)	3
ACK frame length	11 bytes

ACK, acknowledgment; CSMA-CA, carrier sense multiple access–collision avoidance; MAC, medium access control; Kbps, kilobits per second.

therefore, the payload length for the data packets was 232 bits (29 bytes). The overhead introduced by all ZigBee layers accounts for a total of 33 bytes, which results in a data packet length of 62 bytes, which corresponds to a packet transmission time (T_{Packet}) of 1.984 ms at 250 Kbps. Similar data-intensive traffic can be found in other BSN applications, such the monitoring of ECG signals from patients, where the sampling rate can be as high as 250 Hz per electrode.[21]

CLOCK DRIFT MODEL

This section presents a model that uses the differential clock drift between two ZigBee end devices to estimate the duration of two parameters: the contention period (T_{Cnt}), defined as the period during which the two EDs using the unslotted CSMA-CA algorithm will contend for the channel due to the clock drift, and the contention repetition interval (T_{CntRep}).

In order to obtain the clock drift of the EDs, each ED*n* was physically connected to the coordinator (base station [BS]), in order to measure the number of added or missing oscillations ($ticks_{drifted}$), within a period *T*, in comparison with the coordinator's clock. The differential clock drift between the BS and ED*n* can be calculated through Eq. 1:

$$D_{BS,EDn} = \frac{ticks_{drifted}}{f_{osc} \times T} \quad (1)$$

where f_{osc} is the nominal clock frequency of the CC2530 microcontroller (32 MHz). The differential clock drift between ED1 and ED2 can be obtained, without the knowledge of the absolute clock drift of the EDs (D_{EDn}), from the respective differential clock drifts in relation to the BS:

$$D_{ED1,ED2} = D_{BS,ED1} - D_{BS,ED2} = D_{ED2} - D_{ED1} \quad (2)$$

Several unsynchronized devices transmitting periodic traffic with the same nominal period will eventually contend for the wireless channel because of the clock drift effect. If the differential clock drift between ED1 and ED2 is $D_{ED1,ED2}$ and the nominal transmission period of the nodes is given by T_{ED}, then both nodes will start to contend for the wireless channel every T_{CntRep} seconds. The value of T_{CntRep} can be obtained through Eq. 3:

$$T_{CntRep} = \frac{T_{ED}}{D_{ED1,ED2}} \quad (3)$$

The T_{Cnt} during which two devices will compete for the channel can be obtained through the following equation:

$$T_{Cnt} = \frac{T_{Vul}}{D_{ED1,ED2}} \quad (4)$$

where T_{Vul} is the vulnerability window, which is the time window under which the transmissions of two nodes may interfere with each other.

EXPERIMENTAL SETUPS

Three different experimental setups were conceived to evaluate the suitability of the IEEE 802.15.4 CSMA-CA protocol for BSN applications. The corresponding results are presented in the next section.

The first experiment evaluates the effect of contention on the performance of a BSN without hidden nodes. In this experimental setup, a periodic trigger signal from the coordinator was used to generate an interrupt on a pin of the ZigBee EDs. The main objective of the trigger is to create a scenario of contention where the EDs generate packets simultaneously, which represents the worst-case contention scenario.

The other two experiments were performed using two EDs hidden from each other (but visible to the coordinator). For that purpose, these tests were performed inside an anechoic chamber, to avoid multipath propagation, and metal plates were placed between the EDs to obstruct each other's signal. Except for the use of hidden nodes, the second experiment is similar to the first one.

In the third experiment, the trigger signal that was used to force the simultaneous generation of data packets in the previous experiments was removed. The purpose of this experiment is to evaluate the effect of the node's clock drift on the network performance along the time and to validate the proposed clock drift model. In order to facilitate the identification of the values for T_{Cnt} and T_{CntRep}, two measures were taken. The first one was the use of hidden nodes, so nodes are unable to backoff because of carrier sense. The second measure was to perform the experiment with the retransmission mechanism disabled. Under such conditions, the length of the vulnerability window can be calculated using the following expression:

$$T_{Vul} = 2 \times (T_{Backoff\_max} + T_{Packet}) \quad (5)$$

where $T_{Backoff\_max}$ is the maximum backoff time, which has a value of 2.24 ms when the backoff exponent is 3, and T_{Packet} is the packet transmission time.

Results and Discussion

CONTENTION WITHOUT HIDDEN NODES

Table 2 presents the results obtained in the first experiment regarding the following metrics: DR; mean and maximum end-to-end delay; and energy consumption per packet at the ED. The end-to-end delay is the time elapsed since the packet is sent by the source node (ED) application layer until it reaches the destination node (coordinator) application layer. The energy consumption was evaluated for the CC2530, considering a supply voltage of 3.3 V, a current consumption of 27.7 mA during the active periods, and a negligible current consumption (around 1 μA) during inactive periods.

Because the first two rows of results in *Table 2* concern a BSN with a single ED, the DR is 100% even without retransmissions because there is no contention. In contrast, for the BSN with two EDs, the contention causes packet errors because of collisions, decreasing the DR to 91.7% without retransmissions. Nevertheless, the retransmission mechanism is able to correct the errors and restore the DR to 100%.

At the MAC level, the packet delay is the sum of the backoff time ($T_{Backoff}$), turnaround time (T_{TA}), and T_{Packet}. However, the measured

Table 2. Results for the Tests Without Hidden Nodes

EVALUATION SCENARIO	DELIVERY RATIO (%)	MEAN DELAY (MS)	MAXIMUM DELAY (MS)	ENERGY PER PACKET (MJ)
One ED				
Without retransmission	100	9	12	0.62
With retransmission	100	9	12	0.84
Two EDs				
Without retransmission	91.7	11	23	0.80
With retransmission	100	12	26	1.12

ED, end device.

delays presented in *Table 2* are larger than the sum of these components. Two other relevant delay components introduced by the software stack were identified: a delay from the moment the sender application calls the application programming interface function to transmit the packet until the data reach the MAC layer ($T_{\mathrm{APP}\rightarrow\mathrm{MAC}}$) and a delay at the receiver in the opposite direction ($T_{\mathrm{MAC}\rightarrow\mathrm{APP}}$). These delays depend on the payload length and processing load at the nodes. The mean values of these delays for the Z-Stack, measured for different payload lengths, are shown in *Table 3*.

The higher delay and energy consumption values with two EDs in *Table 2*, compared with the corresponding values with one ED, are due to additional backoffs (and retransmissions, when enabled) caused by contention. Additional energy is also spent in the scenarios with retransmission for the acknowledgment notification to propagate from the MAC layer to the application layer.

Table 3. Mean Delay Between the Medium Access Control and Application Layers of the Z-Stack

PAYLOAD LENGTH (BYTES)	$T_{APP\rightarrow MAC}$	$T_{MAC\rightarrow APP}$
10	3.28	1.78
20	3.37	1.87
30	3.48	1.90
40	3.57	1.94
50	3.68	2.01
60	3.77	2.07
70	3.90	2.15
80	3.95	2.16
90	4.04	2.23

Data (time [*T*] values) are in milliseconds.

APP, application; MAC, medium access control.

CONTENTION WITH HIDDEN NODES

In this experiment, the measured DR with retransmissions enabled was approximately 90%, whereas for the test without retransmissions the DR was approximately 13%. Previous measurements without hidden nodes (*Table 2*) resulted in DRs of 100% and 91.7% for the tests with and without retransmissions, respectively. Therefore, when compared with the results without hidden nodes, the experimental results with hidden nodes show a substantial decrease in the DR during periods of contention. Even with the retransmissions enabled, the network was not able to recover from all the packet errors. Given that the presence of hidden nodes is expected in the normal operation of a BSN, these results show that contention may severely degrade the communication reliability of the network and, consequently, make it unable to satisfy the quality of service requirements of BSN applications.

CLOCK DRIFT EFFECT

For this experiment, the differential clock drifts, in parts per million (ppm), between five EDs (ED0–ED4) and the BS were measured. *Table 4* shows the differential clock drifts between a device *n* and the BS ($D_{\mathrm{BS,ED}n}$), measured using the process described in the previous section, as well as the respective drift values between devices *m* and *n* ($D_{\mathrm{ED}m,\mathrm{ED}n}$), calculated using Eq. 2.

We have chosen ED0 and ED1 for the experimental performance evaluation and model validation. For these nodes, the differential clock drift is $D_{\mathrm{ED0,ED1}} = 3.5$ ppm. Using these values, in Eq. 4, we obtain a T_{Cnt} value of approximately 40 min. The T_{CntRep} period, which can be obtained through Eq. 3, is approximately 7 h 56 min. If the average differential clock drift among the five EDs that were tested was used (1.62 ppm), T_{Cnt} and T_{CntRep} would be 1 h 27 min and 17 h 9 min, respectively, which means that, on average, the contention between devices, and the consequent network performance degradation, would take a longer period to repeat but would also last longer.

Figure 1 shows the results obtained in this experiment, which started at 18:15:10 and ended at 13:02:44 the next day. The DR was 100% most of the time of this experiment, which corresponds to noncontention periods. The DR decreases when a contention period

Table 4. Measured Differential Clock Drifts

DEVICE *N*	$D_{\mathrm{BS,ED}N}$	$D_{\mathrm{ED0,ED}N}$	$D_{\mathrm{ED1,ED}N}$	$D_{\mathrm{ED2,ED}N}$	$D_{\mathrm{ED3,ED}N}$	$D_{\mathrm{ED4,ED}N}$
0	3.6	0				
1	0.1	3.5	0			
2	−1	4.6	1.1	0		
3	−0.5	4.1	0.6	−0.5	0	
4	0.2	3.4	−0.1	−1.2	−0.7	0

Data are in parts per million.

BS, base station; ED, end device.

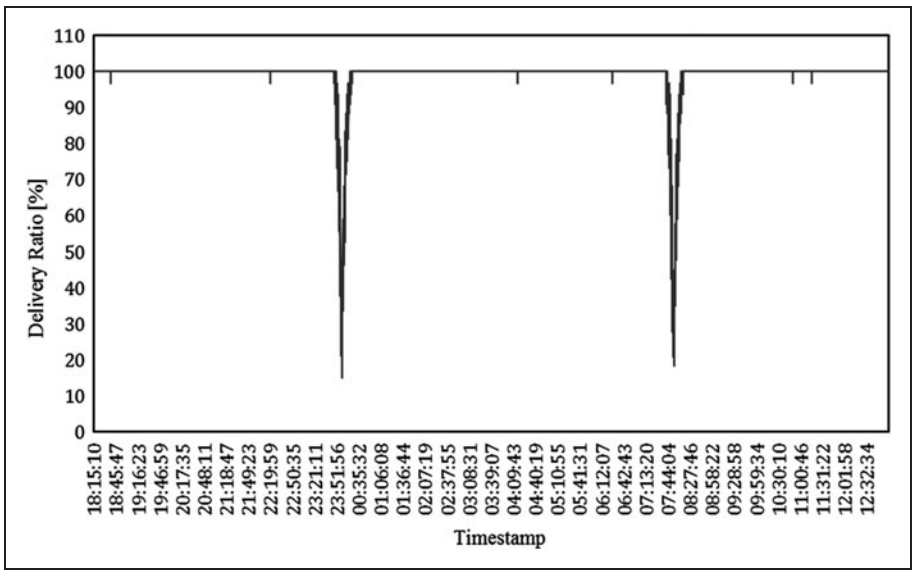

Fig. 1. Delivery ratio over time with clock drift and two hidden nodes.

starts, reaches a minimum (which is very close to the DR of 13% obtained in the previous section) when both devices are generating packets simultaneously, and then increases again until the end of the contention period. Taking into account these boundaries, the interference period lasted for approximately 40 min. The value of contention repetition interval obtained from *Figure 1* is approximately 7 h 53 min. Therefore, the measured T_{Cnt} and T_{CntRep} periods are very close to the values predicted by the proposed theoretical model.

BCA Mechanism

The results presented in the previous section lead to the conclusion that the implementation of a network synchronization procedure can be useful to eliminate the negative impact of the clock drift effect shown in *Figure 1* on the performance of IEEE 802.15.4/ZigBee BSNs. However, such a procedure is not enough, and may be even prejudicial, given the periodic nature of the traffic generated by BSN nodes, if the packet generation instants chosen by two or more nodes happen to be close. Therefore, it is also necessary to provide a mechanism to distribute the traffic generated by the nodes along the time, in order to avoid repeated contention, which can lead to packet errors due to collision, especially in the presence of hidden nodes, due to failure of the carrier sense mechanism.

RELATED WORK

Several authors[22–24] have proposed solutions to the hidden node problem in IEEE 802.15.4/ZigBee WSNs. These solutions are based on grouping strategies, where the nodes are grouped according with their hidden node relationships in a way that each group contains only nodes that are not hidden from each other. The network bandwidth is then divided into slots, and each slot is attributed to a group.

In some cases, the grouping strategy assumes that the coordinator can distinguish a hidden node collision from a normal collision, based on the time when the collision occurs.[24] This distinction be very hard to achieve and implies a non-negligible change to the IEEE 802.15.4 physical layer. The grouping and regrouping procedures include the discovery of hidden node situations, information collection from the nodes, group assigning, and notification of grouping results to the nodes. These procedures are relatively complex and consume substantial bandwidth and energy from the nodes, which is problematic given the resource constraints of these devices. Furthermore, unlike WSNs, the mobile nature of BSN nodes (for instance, a group of patients being monitored at a hospital) may increase the frequency of the regrouping events and, consequently, the overhead introduced by the grouping strategy.

PROPOSED MECHANISM

The grouping strategies referred in the previous section may be suitable for WSNs, where sensor nodes normally generate sporadic traffic, enabling several nonhidden nodes to share the same slot. However, given that the traffic of BSNs is mostly periodic, nodes in the same group would have to contend for the same slot repeatedly, which would increase the probability of collisions.

Therefore, in the proposed BCA mechanism, each slot is assigned to a single BSN node, regardless if it is hidden or not from other nodes. One advantage of this mechanism is that it can be implemented at the application level; therefore, it does not require any change in the IEEE 802.15.4/ZigBee protocol layers.

Figure 2 presents an example of the superframe structure defined by the BCA mechanism, where the beacons are used for synchronization, and the virtual time slots (VTSs) are assigned to the nodes. The number of VTSs and the superframe period are broadcast in the beacon. The actual number of VTSs per superframe and the VTS intervals can be higher than the values provided on this example.

Many BSN applications are characterized by heterogeneous sensor nodes that generate traffic at different bit rates[21,25] (e.g., ECG and body temperature). The BCA mechanism allows multiple nodes that generate traffic at lower rates to share the same VTS in different superframes, thereby increasing the number of sensor nodes supported by the network. According to the example of *Figure 2*, the superframe period is set to the packet generation interval of the sensor node with higher data rate (*n1*), which was assigned to VTS number 3. On the other hand, nodes *n2* and *n3*, which have half the packet rate of *n1*, share the VTS 1 on alternate superframes, with a VTS interval of two superframes.

The IEEE 802.15.4 MAC layer provides an optional scheme, called GTS, which allows the allocation of dedicated slots for the nodes.

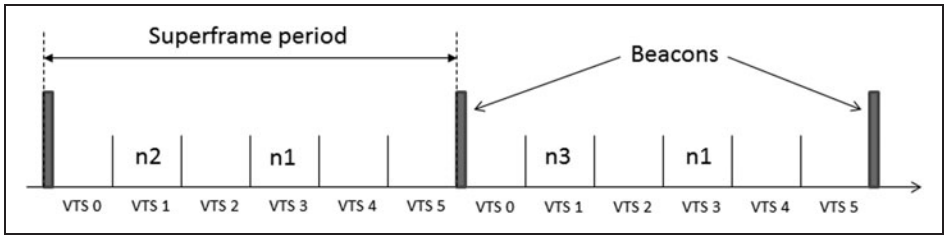

Fig. 2. Example of the superframe structure and slot allocation in the body sensor network contention avoidance mechanism. n, node; VTS, virtual time slot.

However, there are several drawbacks on its utilization compared with the BCA mechanism. The GTS scheme is limited to a maximum of seven allocations. Moreover, unlike the BCA mechanism, nodes cannot share the same slot in different superframes. These limitations make the GTS scheme unsuitable for many BSN applications that may require more nodes, such as motion capture (which require in the order of 15 nodes per user to track all body movements) or the monitoring of physiological signals from multiple patients in a hospital ward at the same time. The nodes also have to listen to the beacon in all superframes before transmitting and cannot transmit their data packet in a superframe if they miss the corresponding beacon, which have impact on the energy consumption and reliability, respectively. Another drawback is that the GTS scheme is not available on ZigBee stacks such as the Z-Stack, owing to the increased complexity of introducing it in mesh or tree topologies. Finally, in the GTS scheme, a node starts the transmission of its packet in the beginning of the allocated slot, regardless of the presence of interference from another source (e.g., a Wi-Fi transmission) that may corrupt the packet. In contrast, the BCA mechanism, which uses the CSMA-CA protocol, is able to sense the busy channel and back off in this case.

Figure 3 shows the BCA algorithm in the coordinator application. When a packet arrives at the coordinator, the algorithm verifies if the packet is a VTS request from a sensor node, which contains the desired VTS interval (expressed as an integer multiple of the superframe period), or if it is a data packet. If it is a VTS request, the algorithm searches for a suitable available VTS, assigns it to the node, and transmits a VTS response to the node. The VTS response contains the following fields: the assigned VTS number; the VTS interval; and the VTS offset, which is the identification of the first superframe at which the node can start to use the VTS, starting from the current superframe.

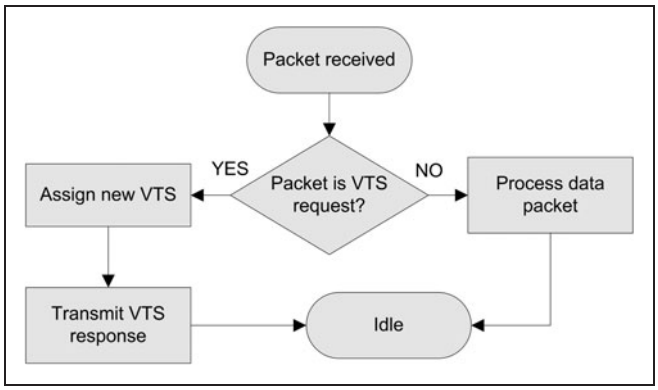

Fig. 3. Body sensor network contention avoidance algorithm in the coordinator. VTS, virtual time slot.

The BCA algorithm in the sensor node application is shown in *Figure 4*. When a beacon is received, the node resynchronizes with the coordinator. After that, if the node does not have a VTS assigned, it will read the superframe period and number of VTSs per superframe from the beacon. Next, it will transmit a VTS request containing the required VTS interval, using VTS 0, which is reserved for this purpose. On the other hand, if the VTS is already assigned, the node will just set a timer for the reception of a next beacon and enter in the sleep state to save energy. When the node receives the VTS response, it sets an event for the transmission of a data packet in the next assigned VTS, according to the VTS number, interval, and offset information provided by the VTS response. When the node receives the transmit packet event, it transmits the data packet. After that, it sets an event (based on the VTS interval) for the transmission of the next data packet in the next assigned VTS and returns to the sleep state.

The sensor node does not need to wake up at every superframe to listen to the corresponding beacon and resynchronize. Instead, the next beacon reception can be scheduled to occur after a number of superframes calculated based on the desired clock accuracy. For example, considering a maximum accepted clock deviation of 200 μs and the maximum clock drift accepted by the IEEE 802.15.4 standard (40 ppm), the sensor nodes would only have to wake up to listen to a beacon every 2.5 s, which corresponds to 1 beacon out of 25 for a superframe period of 100 ms. If a drift compensation mechanism is used for time synchronization, the sensor nodes may be even allowed to sleep during longer times.[26]

An issue regarding the implementation of all functionalities of the BCA mechanism at the application layer is the limited accuracy on the identification of the assigned VTS boundary at the sensor node, due to the errors introduced by $T_{\mathrm{MAC}\rightarrow\mathrm{APP}}$ on synchronization and $T_{\mathrm{APP}\rightarrow\mathrm{MAC}}$ on the packet sending time. One way to reduce the errors is to take into account the effect of these delays, characterized on *Table 3*, on the corresponding functionalities of the mechanism. Another option is to implement these functionalities at the MAC layer level.

EXPERIMENTAL SETUP AND RESULTS

In order to evaluate the effectiveness of the BCA mechanism, tests were performed using the same experimental setup as the third experiment described previously, which is composed by two hidden nodes sending data to a coordinator with the

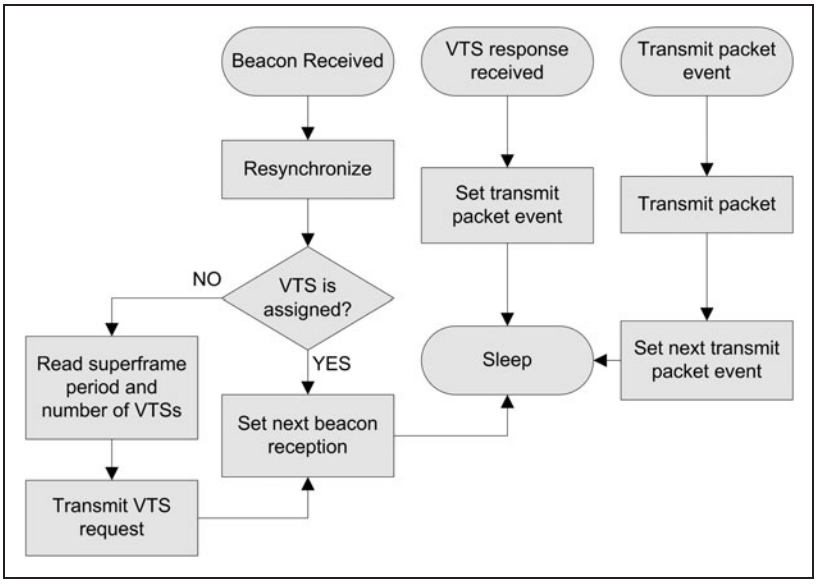

Fig. 4. Body sensor network contention avoidance algorithm in the sensor node. VTS, virtual time slot.

retransmission mechanism disabled. Because the functionality of generation of periodic beacons was not yet available on the Z-Stack at the time the tests were done, we opted to use the TIMAC (version TIMAC-CC530-1.3.1), also from Texas Instruments, which only implements the IEEE 802.15.4 MAC layer. Nevertheless, because of the use of the star topology, the absence of the upper ZigBee layers does not have influence in the results of these tests. The number of bytes introduced by the ZigBee headers was added to the payload of the data packets, in order to produce packets with the same size as those used in the previous tests.

Because the IEEE 802.15.4 protocol only allows a limited set of superframe periods, the superframe period was configured to 122.88 ms, which is the closest value to the 100 ms used in the previous tests. Each node transmits a data packet per superframe in the VTS assigned by the BCA mechanism. The number of VTSs was set to eight, which means that each VTS has a length of 15.36 ms, which is more than sufficient for a node to transmit its packet inside the assigned VTS.

The longest test was executed during a period of 26 h 34 min. During this test, the measured DR remained at 100% all the time. Other tests were made under the same conditions, with the same outcome. These results contrast with those presented in *Figure 1*, where the DR was affected by the clock drift and the hidden node problem, reaching values as low as 13%.

Because the nodes are scheduled to transmit their data packets at different times, no energy is wasted on contention. Therefore, the energy consumption per packet with the use of the BCA mechanism (0.63 mJ, for a clock accuracy of 200 μs) is only slightly higher than the value shown in *Table 2* for one ED, owing to the periodic beacon listening, but yet much lower than the value for the scenario with two EDs.

Conclusions

BSNs can provide substantial benefits both to the patients and to the healthcare system, contributing to increase the quality and reduce the cost of healthcare. This article identified communication reliability problems associated to the operation of the IEEE 802.15.4 protocol in the context of BSNs, associated with contention, hidden nodes, and clock drift effects. The proposed BCA mechanism was able to solve these problems. This mechanism is easy to implement, does not require changes in the IEEE 802.15.4 standard, and is able to support devices with heterogeneous traffic rates.

Acknowledgments

This work was supported by FEDER funds through "Programa Operacional Fatores de Competitividade–COMPETE" and by National Funds through the Portuguese Foundation for Science and Technology in the scope of Project FCOMP-01-0124-FEDER-022674.

Disclosure Statement

No competing financial interests exist.

REFERENCES

1. Chen M, Gonzales S, Vasilakos A, Cao H, Leung VC. Body area networks: A survey. *Mobile Netw Applic* **2011;**16:171–193.
2. Pantelopoulos A, Bourbakis N. A survey on wearable sensor-based systems for health monitoring and prognosis. *IEEE Trans Syst Man Cybernet C* **2012;**40:1–12.
3. Lo B, Yang GZ. Key technical challenges and current implementations of body sensor networks. In: *Proceedings of BSN 2005.* London: Springer, **2005;**1–5.
4. Chen AH, Huang SY, Hong PS, Cheng CH, Lin EJ. HDPS: Heart disease prediction system. *Comput Cardiol* **2011;**38:557–560.
5. Hadjidj A, Souil M, Bouabdallah A, Challal Y, Owen H. Wireless sensor networks for rehabilitation applications: Challenges and opportunities. *J Netw Comput Applic* **2013;**36:1–15.
6. Liu GZ, Huang BY, Wang L. A wearable respiratory biofeedback system based on generalized body sensor network. *Telemed J E Health* **2011;**17:348–357.
7. *IEEE Std 802.15.4-2006. Part 15.4: Wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (WPANs).* Piscataway, NJ: IEEE, **2006.**
8. ZigBee Standards Organization. *ZigBee specification.* Document 053474r17. San Ramon, CA: ZigBee Alliance, **2008**.
9. Gislason D. *Zigbee wireless networking.* Amsterdam: Newnes, Elsevier B.V., **2008.**
10. López HF, Afonso JA, Correia JH, Simões R. The need for standardized tests to evaluate the reliability of data transport in wireless medical systems. *Lecture Notes ICST* **2012;**102:137–145.
11. Liang X, Balasingham I. Performance analysis of the IEEE 802.15.4 based ECG monitoring network. In: *Proceedings of Seventh IASTED International*

Conferences Wireless and Optical Communications. Montreal: International Association of Science and Technology for Development, **2007;**99–104.

12. Chen Z, Lin C, Wen H, Yin H. An analytical model for evaluating IEEE 802.15.4 CSMA/CA protocol in low-rate wireless application. In: *Proceedings of AINAW 2007, Ontario, Canada.* Piscataway, NJ: IEEE, **2007;**899–904.
13. Choi JS, Zhou MC. Performance analysis of ZigBee-based body sensor networks. In: *Proceedings of IEEE SMC 2010, Istanbul, Turkey.* Piscataway, NJ: IEEE, **2010;**2427–2433.
14. Lu G, Krishnamachari B, Raghavendra CS. Performance evaluation of the IEEE 802.15.4 MAC for low-rate low-power wireless networks. In: *Proceedings of IEEE IPCCC 2004, Phoenix, AZ.* Piscataway, NJ: IEEE, **2004;**701–706.
15. Zheng J, Lee MJ. A comprehensive performance study of IEEE 802.15.4. *Sensor Netw Operation* 2006;4:1–14.
16. Ko J, Gao T, Terzis A. Empirical study of a medical sensor application in an urban emergency department. In: *Proceedings of BodyNets '09, Los Angeles, CA.* Gent, Belgium: ICST, **2009;**1–8.
17. Hande A, Polk T, Walker W, Bhatia D. Self-powered wireless sensor networks for remote patient monitoring in hospitals. *Sensors (Basel)* **2006;**6: 1102–1117.
18. López HF, Afonso JA, Correia JH, Simões R. Towards the design of efficient nonbeacon-enabled ZigBee networks. *Comput Netw* **2012;**56: 2714–2725.
19. Texas Instruments. *A true system-on-chip solution for 2.4-GHz IEEE 802.15.4 and ZigBee applications. CC2530 datasheet.* Dallas: Texas Instruments, **2011.**
20. Afonso JA, Correia JH, Silva HR, Rocha LA. Body kinetics monitoring system. International Patent WO/2008/018810. February 14, **2008.**
21. Paksuniemi M, Sorvoja H, Alasaarela E, Myllylä R. Wireless sensor and data transmission needs and technologies for patient monitoring in the operating room and intensive care unit. In: *Proceedings of 27th IEEE EMBC, Shanghai, China.* Piscataway, NJ: IEEE, **2005;**5182–5185.
22. Koubâa A, Severino R, Alves M, Tovar E. Improving quality-of-service in wireless sensor networks by mitigating hidden-node collisions. *IEEE Trans Ind Inform* **2009;**5:299–313.
23. Kwon CW, Tek RJ, Kim KH, Yoo SH. Dynamic group allocation scheme for avoiding hidden node problem in IEEE 802.15.4. In: *Proceedings of ISCIT 2009, Incheon, Korea.* Piscataway, NJ: IEEE, **2009;**637–638.
24. Hwang L, Sheu S, Shih Y, Cheng Y. Grouping strategy for solving hidden node problem in IEEE 802.15.4 LR-WPAN. In: *Proceedings of First International Conference on Wireless Internet, Budapest, Hungary.* Piscataway, NJ, IEEE, **2005;**26–32.
25. Arnon S, Bhastekar D, Kedar D, Tauber A. A comparative study of wireless communication network configurations for medical applications. *IEEE Wireless Commun* **2003;**10(1):56–61.
26. Vilares P. Adaptive time synchronization protocol for BANs [MSc thesis]. Porto, Portugal: University of Porto, **2012.**

Address correspondence to:
José Augusto Afonso, PhD
Algoritmi Center
University of Minho
Campus of Azurem
Guimarães, Portugal

E-mail: jose.afonso@dei.uminho.pt

Received: May 20, 2013
Accepted: June 20, 2013