

# Robust Access for Wireless Body Area Networks in Public m-Health

[Invited Paper]

Narjes Torabi  
The University of British Columbia  
Vancouver, BC, Canada V6T 1Z4  
ntorabi@ece.ubc.ca

Victor C.M. Leung  
The University of British Columbia  
Vancouver, BC, Canada V6T 1Z4  
vleung@ece.ubc.ca

## ABSTRACT

Recent advances in very-low-power wireless communications have stimulated great interest in the development and application of wireless technology in biomedical applications, including wireless body area networks (BANs). A BAN consists of multiple sensor nodes capable of sampling, processing, and communicating one or more vital signs (e.g., heart rate, brain activity, blood pressure, oxygen saturation) and/or environmental parameters (location, temperature, humidity, light) over extended periods via wireless transmissions over short distances. Low cost implementation and ubiquitous deployment calls for the use of license-exempt ISM bands, in which co-existence of other license-exempt devices, particular WiFi radios, negatively impacts on the robustness of BANs. We present proposals to increase the robustness of wireless access in BANs by identifying and taking advantages of spectrum holes that are unused by co-existing devices. Simulation and experimental results are presented to show the effective of our proposals in increasing the robustness of channel access in BANs.

## Keywords

m-health, medium access control, MAC, license-free spectrum, coexistence.

## 1. INTRODUCTION

The term “m-health” refers to the monitoring of physiological vital signs of a body, when a person is performing his/her normal daily activities. As well, the public m-health service enables m-health for a wide group of people in society. By this service, a person who has worn a Body Area Network (BAN) may move from his/her home to the office, street, shopping mall, etc., as Fig. 1 shows, while his/her health condition is continuously monitored and conveyed to a medical center.

BAN, as an effective approach to eliminate wires in health-care environments, is emerging as a key enabler of public

m-health service. A BAN generally includes a small number of body nodes for sampling body vital signs and a gateway as a bridge for transferring collected health information from the body to a medical center. Since body nodes are tiny battery-powered entities, BANs have stringent energy and complexity requirements and need to operate with low duty cycles.

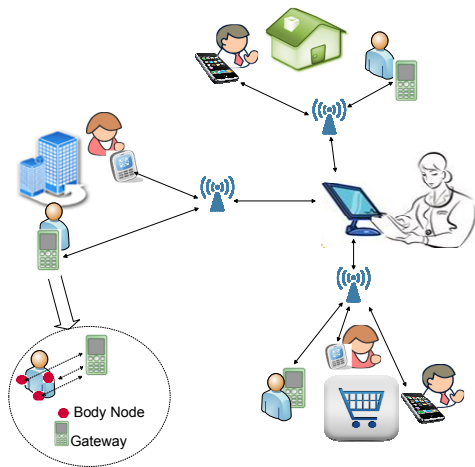
Medical data typically consists of periodically-sampled vital signs and generally have relatively low data rates. Thus, a BAN needs not support a high throughput, unlike conventional wireless networks that aim for throughput maximization. Instead of a high throughput, a BAN requires a guaranteed level of reliable access to the channel to keep a constant flow of medical data toward the gateway. This service-robustness requirement stems from the crucial importance of medical information that needs to be delivered with a minimum delay. However, different service environments on one hand and low-power and complexity constraints on the other hand make it challenging for BANs to meet the service-robustness requirement.

The Federal Communications Commission of the United States has dedicated vacant television band for the Wireless Medical Telemetry Service (WMTS) to protect medical devices from interference. However, WMTS is a regulated band for medical equipment confined only within healthcare facilities. Therefore WMTS is unable to provide seamless connectivity between a person and a medical center for ubiquitous health monitoring in public m-health.

Also, the unlicensed Medical Implant Communication Service (MICS), Ultra Wideband (UWB) and Industrial Scientific Medical (ISM) bands are license-exempt and hence good candidates for pervasive health monitoring.

MICS is intended for transmission of radio signals within the human body and provides a narrow (3MHz) frequency band. These characteristics make MICS unsuitable for public m-health service which commonly targets transmission of on-body medical data. In contrast, ISM and UWB not only provide large bandwidths, but also are widely available globally.

Working in the license-free UWB or ISM band compromises robust service availability of BANs due to the coexistence of a dynamic set of collocated wireless systems with diverse physical and medium access control (MAC) layer specifica-



**Figure 1: Implementation of public m-health system via BANs.**

tions, which work independently without considering timings and traffic requirements of others since there is no central coordinator to manage and synchronize channel access attempts of coexisting systems in a heterogeneous environment. In this regard, authors in [7] experimentally show that in an urban environment, radio interference from coexisting systems can substantially degrade the packet delivery performance of IEEE 802.15.4 BANs operating in the low-power regime.

Despite this coexistence problem, many wireless systems operate in the UWB and ISM bands to take advantage of the license-exempt feature, thus exacerbating the coexistence problem in these shared spectra. Thus there is significant current interest in coexistence management approaches to improve the interference immunity of wireless systems for m-health services. A good example of this approach in a medical context is the 802.11-compliant frequency hopping medical transmitter in the ISM band reported in [4], which provides a higher reliability than a conventional system working in the licensed WMTS band.

The above example illustrates that license-exempt frequency bands are suitable for public m-health services provided that the system is properly designed to achieve the required level of service-robustness by mitigating the negative impact of coexisting systems. This paper reviews our recent work [13] investigating the design challenges for BANs operating in the 2.4 GHz ISM band, and our proposals [13] [12] for managing BAN channel access using cognitive techniques to enhance service robustness. Since IEEE 802.15.4 is a standard for short-range low-power wireless personal area networks (WPANs) operating in ISM frequency band, which is widely considered or already used for BAN implementation, our initial study has identified the beacon corruption problem as the main issue that negatively impacts the service-robustness of BANs employing the IEEE 802.15.4 MAC in a coexistence environment. We have proposed the Beacon Corruption Recovery Scheme (BCRS) [13] as an effective solution to this problem. For more advanced BANs that need not maintain IEEE 802.15.4 compliance, we have

proposed a Centralized BAN Access Scheme (CBAS) [12] that utilized cognitive central node to provide opportunistic access capability over the ISM band and greatly improve service-robustness. We present extensive simulation results to demonstrate the effectiveness of these BAN access schemes in enhancing service robustness.

## 2. RELATED WORK

Several Time Division Multiple Access (TDMA) protocols have been proposed to provide robust access for BANs. TDMA relies on tight synchronization between nodes to provide collision free access. However, in a multi-system coexistent environment, synchronization within a system does not prevent interference from non-cooperating co-located systems. So, even though a body node expects a free TDMA slot, its transmission may still collide with transmissions by other co-located systems. However, many TDMA proposals assume that an interference-free medium is available to provide a reliable service for body nodes. As an example in [8], information about assigned timeslots to each node is carried by some control messages. Therefore, performance of this scheme is heavily constrained by transmission reliability of these messages. This reliability is in question when the BAN works in a shared environment.

Authors in [9] follow the goal of reducing idle listening, collision and overhearing by proposing a TDMA structure. Both master and slaves periodically wake up after sleep time to initiate communications. Since channel condition (busy or idle) is not considered before transmissions, this scheme is effective only if the BAN is free from interference from coexisting systems.

Authors in [11] use channel information for adjusting transmission parameters to handle human body's fading effects. The adaptive modulation scheme adapts to variations of the channel but is not sufficient to deal with coexistence. For instance, in the presence of a persistent interference such as an ongoing file transfer in a nearby wireless local area network (WLAN), the BAN merely decreases its rate to adjust for the poor channel quality. This work does not provide any strategy to address throughput reduction in a BAN due to coexistence, which has a great impact on a BAN's service-robustness.

Authors in [10] introduce an interference-aware prioritized MAC for e-health applications in a hospital environment. This scheme is implemented via two components: an inventory system that tracks the locations of co-located systems, and a radio access controller (RAC) that uses this location information to compute an appropriate transmission power for each co-located. Since this method requires that each service area be equipped with these two components, it may not be suitable for public m-health services that require global or wide-area coverage.

A cognitive radio approach for telemedicine services employing secondary access to spectrum holes left vacant by primary users is considered in [5]. This is a beaconing scheme in which nodes periodically wake up at the start of each sensing period and keep channel-listening until they receive a beacon that informs them about their transmission schedules. In such a network, a secondary user should confine its

impact on primary user’s traffic to a specific disruption limit as defined by the channel owner. However, nodes transmit according to the schedule they have received in the most recent beacon regardless of the primary user’s activity. The use of this approach for public m-health may not be appropriate due to potential service disruptions when the primary user becomes active, as well as interference from other co-existing secondary systems.

Our survey shows that there is a lack of good solution for providing robust wireless access over license-free spectrum for BANs. Our recent work fills the void by proposing robust access scheme, namely BCRS and CBAS, for license-free BANs operating in the presence of coexisting systems.

### 3. ROBUST ACCESS UNDER IEEE 802.15.4 STANDARD

IEEE 802.15.4 [3], a predominant standard for low-power and low-rate WPANs, is recommended by the IEEE 802.15.6 working group for BANs [1]. This section evaluates how well a BAN works based on the IEEE 802.15.4 Beacon-Enabled mode finds a robust access to a shared medium in a co-existence environment. We show that in the presence of IEEE 802.11 WLAN transmissions, the service-robustness of 802.15.4 MAC is significantly degraded due to two factors: 1) Reliance on reception of beacons, periodic synchronization messages, from the WPAN coordinator (PAN-C), and 2) Non-competitive time granularity of the slotted carrier-sensed multiple access (CSMA) in 802.15.4 MAC in comparison to other CSMA-based co-located systems such as 802.11. To overcome these degradations and improve visibility of a BAN among other coexistent networks, we have proposed BCRS [13] that enables a WPAN to recover quickly when it is interfered by a 802.11 WLAN. Note that in this paper we use WPAN and BAN interchangeably.

#### 3.1 Coexistence Issues with IEEE 802.15.4

##### 3.1.1 Beacon Corruption Issue

The beacon packet is the most critical control packet in the IEEE 802.15.4 standard. It synchronizes end devices with the PAN-C and permits them to participate in communications. A PAN-C sends beacons periodically regardless of the availability of the medium to keep the whole network in synchronization. Suppose each WLAN packet transmission lasts for  $L_{WLAN}$  time units. When the WLAN initiates a transmission before the start of the next Beacon Interval (BI) and that transmission overlaps with a beacon, the beacon is corrupted. The vulnerable duration is equivalent to  $L_{WLAN}$  as shown in Fig. 2. The interfered end device misses the beacon and loses its eligibility to participate in communication until it is synchronized again. Therefore, its service is interrupted at least for an entire BI duration. When the PAN-C is surrounded by WLAN interference, the service unavailability is more severe since none of the WPAN end devices receive the beacon correctly and no transmission takes place in the WPAN.

##### 3.1.2 Time Granularity Issue

Both 802.15.4 WPANs and 802.11 WLANs employ CSMA in the MAC layer, with a back-off mechanism to recover from multiple access collisions. They operate at the boundary of their Back-off Units (BU), which are  $320\mu\text{sec}$  and  $9\mu\text{sec}$

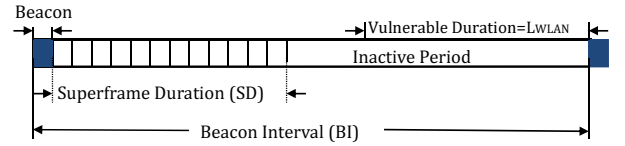


Figure 2: Superframe structure of the IEEE 802.15.4 Beacon-Enabled mode

for 802.15.4 and 802.11g, respectively. When contending for access to a shared channel, the longer BU of WPANs slows their access resulting in loss of access opportunities. Significant differences between the lengths of the BUs and transmission power of these standards lead to the following consequences: 1) the WLAN may aggressively access the shared medium in a co-located WPAN/WLAN scenario and, 2) the WPAN service may experience interruptions over time since its access to the channel is restricted to remaining time gaps between transmissions of the co-located WLAN.

#### 3.2 Beacon Corruption Recovery Scheme

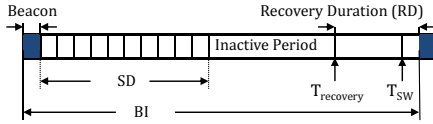
##### 3.2.1 System Parameters and Assumptions

To improve access availability of a BAN to a medium in a WPAN/WLAN coexistence environment, we present BCRS as an extension of IEEE 802.15.4 but before going through the algorithm, some clarification and assumptions are stated.

*Control channel (CCH):* Our method hinges on a dedicated CCH that is used for channel setting and other control information exchanges. This channel should be as free of interference as possible. To select the CCH, we consider that in the 2.4GHz ISM band, the 802.15.4 standard employs 16 non-overlapping channels, while 802.11 employs 14 channels. The frequency range of each 802.11 channel overlaps with four 802.15.4 channels. While the mentioned channel allocation is globally accepted for WPANs, it is subject to regional spectrum regulations. For instance, channels 13 and 14 of IEEE 802.11 WLANs operating in the 2.4 GHz ISM band are not used by most WLAN devices in N. America due to transmit power restrictions, and they may therefore be used for the control channel.

*Channel sensing during inactive period :* Since the Beacon-Enabled mode of 802.15.4 MAC is mainly employed for energy conserving networks, we assume that BI always includes an inactive period, in which power conserving nodes enter sleep mode to conserve energy. Furthermore, as the PAN-C usually does not have a stringent energy conserving constraint compared to other nodes, it can monitor the condition of the WPAN frequency channels during inactive periods. Therefore, the PAN-C can find not only the level of noise on its working frequency but also the list of available (free) WPAN channels.

*Modified beacon packet :* In addition to the network parameters normally set by the PAN-C in the beacon, new configuration parameters as defined below are included in the beacon packets: *Threshold*, *Recovery-Trigger-Time* ( $T_{recovery}$ ) and *Switching-Time* ( $T_{sw}$ ).



**Figure 3: Timing illustration of the proposed method**

*Threshold* : This parameter reflects the interference tolerance level of an end device. If *Threshold* is reached, the end device enters a recovery mode. Different criteria, proportional to the specific monitoring responsibility that an end device supports, could be envisioned as *Threshold*.

*Recovery-Trigger-Time* ( $T_{recovery}$ ): It represents the trigger time for the recovery scheme.

*Switching-Time* ( $T_{SW}$ ): It represents the time at which end devices go to listening mode.

### 3.2.2 Description of BCRS

When a WPAN starts its operation, the PAN-C randomly selects one of the two *CCH*s that are relatively free from WLAN interference for its highly reliable data exchanges and decides on the *Threshold* and  $T_{recovery}$  parameters. Then it encapsulates this additional information into the beacon packet, and sends this periodically at the start of each BI.

In the IEEE 802.15.4 standard, as illustrated in Fig. 2, all end devices go to sleep mode after the expiration of the Superframe Duration (SD). These devices wake up again to receive the next beacon when inactive period is finished. End devices calculate sleep and wake-up times using the beacon reception time as the reference. To accommodate the coexistence scheme, the superframe is enhanced as shown in Fig. 3. *Recovery-Duration* (*RD*) is the length of time that the WPAN works on the *CCH*. Our recovery scheme that enhances IEEE 802.15.4 works as follows:

All WPAN entities wake up and tune their radios to the *CCH* at  $T_{recovery}$ . In fact, during the latest *RD* back-off unit (BU) of the BI, the coexistence method is activated. Each end device that reaches *Threshold*, e.g., by losing a specified number of successive beacons, concludes the presence of an interfering system in its vicinity.

An interfered end device, i.e., one that reaches the *Threshold*, sends an alarm message to PAN-C at a random time between  $T_{recovery}$  and  $T_{SW}$ . Since the *CCH* is approximately interference-free, the sender can be sure that PAN-C receives the message with a high reliability. Afterwards, end devices become silent at  $T_{SW}$  and listen to the *CCH*.

Consequently, when PAN-C receives an alarm message, it finds that one of its end devices has been endangered by interference. Then, PAN-C chooses a new active channel from the list of available WPAN channels (the list that PAN-C obtains during the inactive period) and announces this selected channel through the *CCH* during the latest BU of the

BI beginning at  $T_{SW}$ . All end devices receive this announcement and tune their radios to the new frequency. Thus, the entire network is informed about the new active channel and tunes their radios to it.

PAN-C sends the next beacon using the new frequency at its pre-scheduled time, as expected by the end devices. Finally, the WPAN nodes resume operation in this new channel that is likely free from interference, without losing their synchronization with the PAN-C. Timing of the proposed method is illustrated in Fig. 3.

When PAN-C senses a high noise level on the WPAN working channel, it concludes that interference is present around itself and so predicts that the next beacon will be corrupted with a high probability. Thus, PAN-C proactively invokes the recovery scheme to avoid interference. It means that regardless of receiving an alarm message from end devices or not, PAN-C announces a new frequency channel at the latest BU of the BI.

As a conservative way to protect the WPAN from being partitioned due to less than ideal reception over the *CCH*, PAN-C always announces the WPAN working frequency for the next BI in the latest BU of the BI (started at  $T_{SW}$ ). Therefore, all elements of the network would switch to the new channel at approximately the same time, and network partitioning would not occur. In addition, as soon as one part of the WPAN is affected, the coexistence scheme comes to work and responds to the interference. This mechanism is robust and resistant against WLAN interference due to the use of *CCH*s that are nearly interference free.

## 4. ROBUST ACCESS UNDER CENTRALIZED BAN ACCESS SCHEME

The idea behind BCRS is to prevent the coexistence of a WPAN and WLAN in the same frequency channel by moving a 802.15.4-based BAN to a cleaner channel where BAN service is less compromised by WLAN transmissions. Indeed, BCRS is beneficial when the channel that WPAN switches to not only experiences low WLAN interference but also allows the WPAN to operate on it at least for a good portion of time without a need for another switching. In general, however, finding a channel that remains available for an extended time period may not always be possible especially considering the mobility of BAN users. Therefore, BCRS may often change the working frequency, which consequently increases the overhead of BAN operation. In this regard and to further guarantee a robust service for a WPAN even when interface on different channels is very dynamic, a cognitive medium access scheme called CBAS has been proposed [12] and is reviewed in this section.

CBAS dynamically adjusts the channel access patterns of a BAN to reduce service interruptions caused by interference from coexisting systems. Simulation results indicate that in a coexistence environment, BAN channel access employing CBAS provides less service interruptions, lower packet delays, and higher access rate than that employing IEEE 802.15.4 MAC, including our BCRS extension.

### 4.1 Centralized BAN Access Scheme

### 4.1.1 Assumptions

The proposed CBAS has been designed to operate under the following assumptions:

- *Control Channel*: A dedicated control channel is available for exchanging of control information between the gateway and body nodes.
- Each body node has a unique identity (ID), and the gateway has complete information about this ID and body nodes' sampling rates.
- For power conservation, body nodes enter the low-power sleep mode when they are not exchanging data with the gateway. Body nodes are equipped with passive radio frequency (RF) modules [14] that allow them to receive commands from the gateway on the control channel when they are asleep. A command addressing a body node using its unique ID causes the node to wake up and process the command.
- A pool of  $h$  orthogonal channels is available for BAN operation; e.g., there are 16 candidate channels for 802.15.4 WPANs in the license-free 2.4 GHz ISM band.
- The gateway has the ability to sense the state of all the channels in the channel pool at the same time; in essence, it has cognitive radio capability. As in other work [6], channel sensing is assumed to be perfect.
- The states of channels sensed by the gateway are consistent with that seen by body nodes; i.e., if channel  $x$  is perceived as idle by the gateway it can be reliably used for communications between the gateway and any body node. This assumption is also used in [6] for a Bluetooth system, and is reasonable in our case since body nodes are less than 2 meters from the gateway and the whole BAN can be considered one entity from an external viewpoint.

### 4.1.2 Description of Centralized BAN Access Scheme

Since body nodes have low transmit power, they usually are not able to force high power interferers to respect BAN traffic requirements. In other words, in the presence of contenders with high transmit power, a BAN usually does not succeed in contending for access to the shared license-free band. So, access of body nodes is generally restricted to unused spaces of the spectrum. Since traffic of collocated wireless systems does not have a predictable pattern, these unused spaces are scattered over time. So, in spite of the requirement of public m-health for a reliable and robust service, access of body nodes to the shared medium faces unpredictable interruptions, which varies across the pool of orthogonal channels due to different interference levels. CBAS exploits this diversity to improve the service reliability of a BAN.

To illustrate, suppose there is a pool of three orthogonal channels for BAN's operation and collocated systems occupy these channels as shown in Fig. 4. Suppose that the target BAN is tuned to CH1. Consequently, its access to the shared medium is excluded in the dashed parts of Fig. 2(a), which indicates that BAN service is intermittently interrupted. However, if at the time of service interruption on

CH1, the BAN is tuned to another available channel (if exists), these interruptions are reduced and service reliability improves.

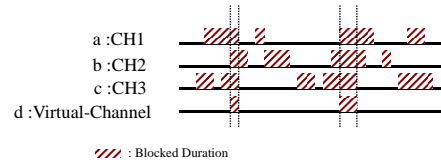


Figure 4: Channel availability pattern

In this example, by sensing channel availability over CH2 and CH3, availability of BAN access to the shared medium is expanded to that of the Virtual-Channel shown in Fig. 2(d). The Virtual-Channel represents the capacity of the shared medium extracted for BAN access when CBAS opportunistically captures the available durations of all candidate channels. In Fig. 2(d), the un-shaded spaces of the Virtual-Channel represent the total access availability for the BAN. Clearly, this improvement in service reliability of BAN traces back to the availability of a channel pool. In other words, if the BAN is constrained to work on only a specific channel all the time, like an 802.15.4-based BAN, its chance of accessing the channel is notably reduced by the activities of coexistent systems. However, channel access is potentially enhanced if the BAN can dynamically tune to an available channel. Based on the above discussion, our proposed CBAS operates as follows:

Step 1: The gateway continuously senses all channels that exist in the pool of orthogonal candidate channels to detect those that are unoccupied, as well as idle spaces that occur between transmissions of co-located networks in the occupied channels, and assigns them to body nodes. It is possible that more than one channels are perceived as idle by the gateway. If so, one of the available channels is chosen based on the specific channel selection strategy that the gateway follows. For example, the gateway chooses an unoccupied channel and stays on it until it becomes unavailable or degraded.

Step 2: The gateway exploits the spectrum space to improve BAN access by allocating the best available channel to the next body node scheduled for transmission, based on the gateway's knowledge of the body nodes' sampling rates. The gateway sends an RTS (using 802.11 protocol) on the allocated channel with an appropriate reservation time to capture it for the duration of the expected data exchange, and sends a command (including the ID of target node plus information about the chosen frequency channel) on the control channel to the specific body node.

Step 3: The passive RF module of the target body node, which finds its ID matches that in the command sent by the gateway on the control channel, wakes up the body node.

Step 4: The body node switches to the assigned channel and exchange data with the gateway on that channel. When data transmission is finished, the body node tunes its radio to the control channel and goes back to sleep.



### 4.1.3 Characteristics and Features of CBAS

1) *CBAS properly services all three categories of periodic, on-demand and emergency data.* For serving periodic data, the free channels identified are allocated to body nodes based on the knowledge that the gateway has about the nodes' sampling rates. Since requests for on-demand traffic are initiated by the gateway, this data is served like periodic one. In fact, when the gateway requires body signal measurements from a specific body node, it simply assigns a free channel to that body node. Finally, for handling emergency situations, when node infers an unusual event, it immediately sends a request through the control channel.

2) *CBAS addresses energy conservatism requirement of BANs.* Since sensing for free channels, assigning them to body nodes, and initiating a link are done centrally at the gateway, CBAS frees the body nodes from the complexities and energy consuming procedures by concentrating these at the gateway. Furthermore, by incorporating passive RF modules [14] in the body nodes, they can switch to low-energy sleep mode as soon as possible without wasting their precious energy on idle listening. Passive RF modules bring the benefit of energy harvesting and no quiescent power consumption from the battery when a body node is waiting for the next command. When a command arrives in the control channel, the passive RF module recovers energy from the command to decode the command and wakes up the body node to further process the command if its ID matches that of the node.

3) *CBAS protects low power transmissions of body nodes from being perceived as noise by co-located systems.* IEEE 802.11 and its compliant networks are CSMA-based wireless systems that employ Clear Channel Assessment (CCA) scheme to check the availability of the medium before capturing it. As it is likely that a BAN works in a shared medium with co-located CSMA-based systems, these systems are expected to defer their contention for the shared medium when the BAN is active. The big difference in the BAN and coexisting network's transmit power levels means that the coexisting network's CCA may sense a clear channel but the BAN's CCA senses a busy channel. This problem penalizes the BAN and makes energy based CCAs insufficient for detecting channel occupancy and avoiding collision. Consequently, protection of BAN packets from potential 802.11 signals is necessary. To accomplish this, when the gateway decides on allocation of a specific available channel to a body node, it sends an RTS with high power on that channel according to the 802.11 standard [2] before sending a command via the control channel.

## 5. PERFORMANCE EVALUATIONS

In this section, BAN service-robustness under IEEE 802.15.4, BCRS and CBAS medium access proposals is evaluated. We consider BAN operation in the 2.4 GHz ISM band using physical layer parameters of the IEEE 802.15.4 WPANs [3]. Interference from coexistent systems is generated by two co-located WLAN work-stations working in each candidate channel. Packet arrivals at the WLAN stations are Poisson with parameters  $\lambda_1$  and  $\lambda_2$ . An analyzer is employed to derive statistics about the percentage of time,  $\sigma$ , in which channel is occupied by WLAN transmissions. By changing  $\lambda_1$  and  $\lambda_2$ , the analyzer derives different values of  $\sigma$  as a representation of the level of interference the BAN experiences

from coexistent WLAN systems. Evaluations are performed and compared when a BAN 1) statically assigned to a single channel and works based on the IEEE 802.15.4 standard, 2) changes its working channel according to BCRS and when it loses two consecutive beacons and 3) has access to a pool of two and three channels and opportunistically captures spectrum holes.

To explore how promptly a BAN finds access to a medium which is also used by WLAN transmissions, a very high arrival rates for body nodes is set to ensure that the BAN aggressively tries to access the shared medium. With this setting, the BAN always has packets for transmissions or equivalently the queues of body nodes are never empty and the BAN persistently tries to capture the medium. In this situation, the time duration between two consecutive BAN transmissions, as illustrated in Fig. 5, shows how long the BAN should wait until it could transmit the next packet.

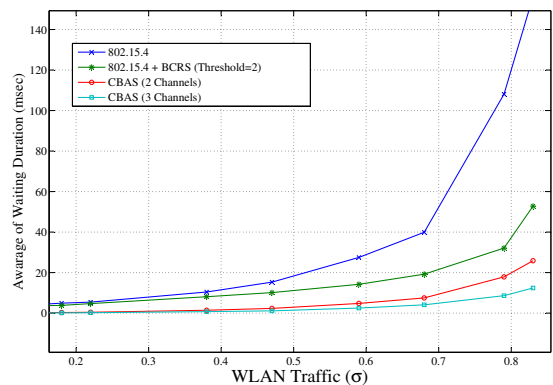


Figure 5: Average of waiting duration

Also, the effective service rate (throughput) of the BAN for the above three schemes is compared in Fig. 6. Note that throughput is calculated as  $Throughput = \frac{\bar{N} \times 256 \times 8}{250000} bps$  where  $\bar{N}$  is the average number of body nodes' packets received successfully by the gateway.

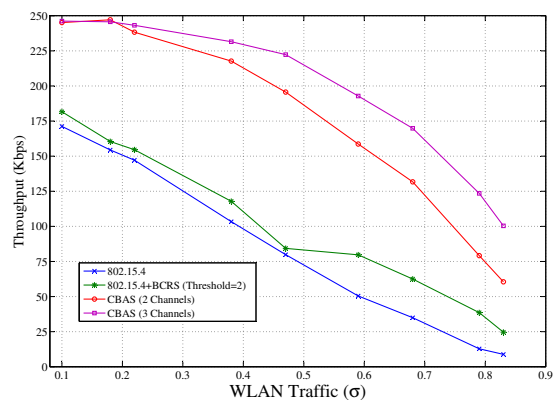


Figure 6: Effective service rate of BAN

As the results indicate, for large WLAN traffic intensities

(high values of  $\sigma$ ), CBAS outperforms 802.15.4 and BCRS because:

- Gateway captures all unused spaces of  $\{\text{CH1, CH2}\} / \{\text{CH1, CH2, CH3}\}$  to improve service availability of body nodes.

- Body nodes do not participate in CSMA procedure to access the medium. So, they do not lose their access opportunities because of their large BU.

- 802.15.4 protocol overheads are removed because body nodes are not required to postpone their medium access to synchronize with PAN-C by receiving beacons and to sense two consecutive idle CCAs before their transmissions.

Since commercially available devices have already been used as body nodes mostly work based on the IEEE 802.15.4, they need to be equipped with a recovery scheme, like BCRS, to improve their interference immunity in a coexistent environment. However, if compatibility with IEEE 802.15.4 is not required, CBAS defiantly offers the most robust service to body nodes in a shared medium among the three different access schemes considered.

## 6. CONCLUSION

Public m-health for continuous monitoring of patients' vital signs anytime and anywhere is practical only when a reliable BAN is available for sensing the body signals and conveying them to the healthcare center via a gateway. License-free bands are suitable for BANs as they are available everywhere, but faces the challenge of link disruptions due to interference from coexisting systems. We have addressed this challenge by proposing 1) BCRS as an extension to IEEE 802.15.4 beacon-enabled mode and 2) CBAS, a centralized access scheme that employs cognitive spectrum sensing capability at the gateway for opportunistic access to free channels. We have presented simulation results, which confirm that a 802.15.4-based BAN suffers from highly unreliable service when it is subject to frequent interruptions from co-located WLAN stations. In contrast, results show that the proposed CBAS significantly improves the BAN's channel availability without imposing processing overheads on low complexity body nodes. By employing the proposed CBAS to improve the reliability and robustness of BANs, realization of public m-health will take one big step forward. On the other hand, if compatibility with IEEE 802.15.4 is required as a design constraint, the proposed BCRS also provides some improvements in service-robust over the existing standard, although the improvements are less than those realized by CBAS.

## 7. ACKNOWLEDGMENT

This work was supported by the Natural Sciences and Engineering Research Council (NSERC) of Canada.

## 8. REFERENCES

- [1] *IEEE 802.15 WPAN task group 6 for body area networks (BAN)*.
- [2] *IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, Nov. 1997, P802.11.
- [3] *IEEE Standard for Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (WPANs)*, 2003. P802.15.4.
- [4] S. Baker, S. King, and J. Welch. Performance measures of ism-band and conventional telemetry. *Engineering in Medicine and Biology Magazine, IEEE*, 23(3):27–36, May–June 2004.
- [5] S. Feng, Z. Liang, and D. Zhao. Providing telemedicine services in an infrastructure-based cognitive radio network. *Wireless Communications, IEEE*, 17(1):96–103, Feb. 2010.
- [6] S. Geirhofer, L. Tong, and B. M. Sadler. Cognitive medium access: Constraining interference based on experimental models. *Selected Areas in Communications, IEEE Journal on*, 26(1):95–105, Jan. 2008.
- [7] J.-H. Hauer, V. Handziski, and A. Wolisz. Experimental study of the impact of WLAN interference on IEEE 802.15.4 Body Area Networks. In *European Workshop on Wireless Sensor Networks*, pages 17–32, 2009.
- [8] S. J. Marinkovic, E. M. Popovici, C. Spagnol, S. Faul, and W. P. Marnane. Energy-efficient low duty cycle MAC protocol for wireless body area networks. *Information Technology in Biomedicine, IEEE Trans. on*, 13(6):915–925, Nov. 2009.
- [9] O. Omeni, O. Eljamaly, and A. Burdett. Energy efficient medium access protocol for wireless medical body area sensor networks. In *Proc. 4th IEEE/EMBS Int. Symp. on Medical Devices and Biosensors*, pages 29–32, Aug. 2007.
- [10] P. Phunchongharn, D. Niyato, E. Hossain, and S. Camorlinga. An EMI-aware prioritized wireless access scheme for e-health applications in hospital environments. *Information Technology in Biomedicine, IEEE Trans. on*, 14(5):1247–1258, Sep. 2010.
- [11] H. Su and X. Zhang. Battery-dynamics driven TDMA MAC protocols for wireless body-area monitoring networks in healthcare applications. *Selected Areas in Communications, IEEE Journal on*, 27(4):424–434, May 2009.
- [12] N. Torabi and V. C. M. Leung. Robust license-free body area network access for reliable public m-health services. In *Proc. IEEE Int. Conf. on e-Health Networking Applications and Services (Healthcom)*, June 2011.
- [13] N. Torabi, W. Wong, and V. C. M. Leung. A robust coexistence scheme for IEEE 802.15.4 wireless personal area networks. In *Proc. IEEE Consumer Communications and Networking Conf.*, pages 1031–1035, Jan. 2011.
- [14] X. Zhang, H. Jiang, X. Chen, L. Zhang, and Z. Wang. An energy efficient implementation of on-demand MAC protocol in medical wireless body sensor networks. In *Proc. IEEE Int. Symp. on Circuits and Systems*, pages 3094–3097, May 2009.