WiCop: Engineering WiFi Temporal White-Spaces for Safe Operations of Wireless Body Area Networks in Medical Applications

Yufei Wang*, Qixin Wang*, Zheng Zeng†, Guanbo Zheng‡, Rong Zheng§*
* Dept. of Computing, The Hong Kong Polytechnic University,
† Dept. of Computer Science, University of Illinois at Urbana-Champaign
‡ Dept. of Electrical Engineering, University of Houston
§ Dept. of Computer Science, University of Houston
Email: csqwang@comp.polyu.edu.hk

***Abstract*—ZigBee and other wireless technologies operating in the (2.4GHz) ISM band are being applied in *Wireless Body Area Networks* (WBAN) for many medical applications. However, these low duty cycle, low power, and low data rate medical WBANs suffer from WiFi co-channel interferences. WiFi interference can lead to longer latency and higher packet losses in WBANs, which can be particularly harmful to safety-critical applications with stringent temporal requirements. Existing solutions to WiFi-WBAN coexistence either require modifications to WiFi or WBAN devices, or have limited applicability. In this paper, by exploiting the *Clear Channel Assessment* (CCA) mechanisms in WiFi devices, we propose a novel policing framework, WiCop, that can effectively control the temporal white-spaces between WiFi transmissions. Specifically, the WiCop Fake-PHY-Header policing strategy uses a fake WiFi PHY preamble-header broadcast to mute other WiFi interferers for the duration of WBAN active interval; while the WiCop DSSS-Nulling policing strategy uses repeated WiFi PHY preamble (with its spectrum side lobe nulled by a band-pass filter) to mute other WiFi interferers throughout the duration of WBAN active interval. The resulted WiFi temporal white-spaces can be utilized for delivering low duty cycle WBAN traffic. We have implemented and validated WiCop on SORA, a software defined radio platform. Experiments show that with the assistance of the proposed WiCop policing schemes, the packet reception rate of a ZigBee-based WBAN can increase by up to 43.8% in presence of a busy WiFi interferer.**

***Keywords*-WBAN, WiFi, reliability, coexistence, safety**

I. Introduction

Wireless Body Area Networks (WBAN) plays a key role in future e-health [1]. For example, one important WBAN application is multi-parameter monitoring, where multiple vital signs of a patient are monitored continuously. These vital signs are sampled by the sensors mounted on the patient, and displayed on a central monitor. Traditionally, sensors are wirely connected to the central monitor. Wire connections limit the mobility of patients, and if sensors fall off due to patients' movements, or if people trip over wires, accidents may happen. To mitigate these problems, WBANs are proposed to connect the many sensors, monitors, and other medical devices wirelessly. There are many possible WBAN medical applications. One typical example is the multi-parameter monitoring. In multi-parameter monitoring, the sensors and the monitor form a single-hop wireless network with the monitor acting as a base-station and sensors as clients.

WBANs can be built upon various candidate wireless technologies operating in different *Radio Frequency* (RF) bands. For example, the IEEE 802.15.6 WBAN standardization working group are considering traditional *Wireless Medical Telemetry Service* (WMTS) band, *Industrial Scientific and Medical* (ISM) 2.4GHz band, *Ultra Wide Bandwidth* (UWB) band etc. in their discussions. Among these RF bands, the ISM band is the most attractive due to its license-free nature, and consequently a wide range of available devices and vendors. Among the technologies in the ISM band, ZigBee, Bluetooth, and the draft IEEE 802.15.6 2.4GHz standard suit WBANs the best due to their low power consumption, low radiation, and low cost [1]. However, all of them may suffer from coexistence interference from the nowadays pervasive WiFi (aka IEEE 802.11) networks [2][3][4][5][6], which run on the same ISM 2.4GHz band. Though the coexistence interference may not be a major concern for low duty-cycle non-critical applications such as body temperature monitoring [7], it is not the case for WBAN applications with stringent requirements on packet delivery ratio and/or latency. One example is *Electrocardiography* (ECG) monitoring [8]. The IEEE 1073 [9] standard mandates that each ECG sample be delivered within 500ms [8]. A sample delivered after its 500ms deadline is considered lost, which means a fault happens.

To give an idea on the WiFi coexistence challenge, Fig. 1 (quoted from [10]) shows the *Packet Reception Rate* (PRR) of a ZigBee link under WiFi interference. The PRR drops below 20% when the ZigBee receiver is 15 feet away from a WiFi (specifically, IEEE 802.11g) interferer. This shows that WiFi interference is a significant threat to ZigBee-based WBANs.

To deal with the WBAN-WiFi coexistence challenge, three categories of solutions have been proposed, each with its own limitations. The first category of solutions aim to operate WBAN over RF channels sufficiently away from the active WiFi RF channels [7]. For instance, in US, a ZigBee-based WBAN can use ZigBee channel 25 and 26, which do not overlap with any WiFi RF channels [10]. However, this greatly

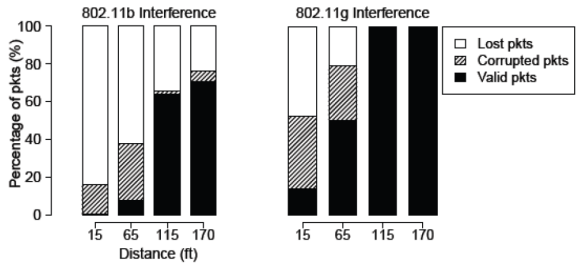


Fig. 1. *Packet Reception Rate* (PRR) of a ZigBee link under WiFi interference (quoted from [10]). The X axis indicates the distance from the ZigBee receiver to the WiFi transmitter; the Y axis is the PRR of the ZigBee link. In the left sub-graph, the WiFi interferer is an IEEE 802.11b device; while in the right sub-graph, the interferer is an IEEE 802.11g device. IEEE 802.11b/g are the two major subtypes of WiFi (IEEE 802.11) devices.

limits the RF spectrum that WBANs can use. The second category of solutions revise current WBAN or WiFi standards, adding intelligent coexistence schemes to make WBAN or WiFi devices more aware of one another [10][11]. However, the demand to modify existing standards/implementations makes it hard to use *Commercially-Off-The-Shelf* (COTS) devices. The third category of solutions try to spatially separate WBANs from WiFi networks via careful configuration-time planning. However, this is often difficult as WiFi networks may not be under the same administration domain as WBANs. Furthermore, unintended usage of mobile WiFi devices may still cause spurious outages in WBANs[1].

In this paper, we propose WiCop, a novel policing framework different from the aforementioned three categories of solutions. WiCop addresses the WBAN-WiFi coexistence problem by effectively controlling the temporal white-spaces (gaps) between consecutive WiFi transmissions. Though temporal white-spaces are abundant in light to medium loaded WiFi networks [10], they are scarce in heavy loaded WiFi networks and tend to be irregular. Our approach "engineers" the intervals and lengths of WiFi temporal white-spaces, and utilizes them to deliver low duty cycle WBAN traffic with minimum impacts on WiFi. WiCop exploits the *Clear Channel Assessment* (CCA) mechanisms in the WiFi standard. Two policing schemes are proposed: 1) Fake-PHY-Header and 2) DSSS-Nulling. We have implemented and validated WiCop on SORA [12], a software defined radio platform. Experiments show that under WiFi interference, WiCop can raise WBAN packet delivery rates by up to 40%.

The rest of this paper is organized as follows. Section II briefly introduces WiFi (IEEE 802.11) standard. Section III presents a case study showing the significance of WiFi co-channel interference on WBAN, using ECG monitoring as the medical application background. Section IV proposes the WiCop policing framework to engineer WiFi interference traffic's temporal white-spaces for WBAN communications. Section V elaborates how the WiCop framework is implemented on Microsoft SORA software defined radio platform. Section VI evaluates our WiCop framework through experiments. Section VII discusses related work. Section VIII concludes the paper.

[1]Repeated probe requests have been reported on certain WiFi devices when they are not associated with particular APs.

II. Background

Before delving into the details of WiCop, we first give an overview of the WiFi (aka IEEE 802.11) standard. The WiFi standard boils down to several subtype standards, of which, most of nowadays COTS WiFi devices comply with the subtype standard of IEEE 802.11a, b, g, or n. IEEE 802.11b is the first to reach mass production, which runs *Direct Sequence Spread Spectrum* (DSSS) in the 2.4GHz ISM band. IEEE 802.11a emerges next, and runs *Orthogonal Frequency Division Multiplexing* (OFDM) in the 5GHz ISM band, a less frequently used RF band due to more stringent line-of-sight transmission constraints. IEEE 802.11g supports IEEE 802.11a-like OFDM in the 2.4GHz ISM band, meanwhile is fully backward compatible with IEEE 802.11b. IEEE 802.11n mainly enhances the previous three by adding *Multiple Input Multiple Output* (MIMO) anntenna support.

In the following, we shall only look at those common features of IEEE 802.11a/b/g/n that are critical to our WiCop strategies.

Full Occupation of 2.4GHz ISM Band: Every WiFi subtype standard predefines a fixed set of RF channels. Though a single WiFi network can only use one of these predefined RF channels, when several WiFi networks coexist in an area, they will try or will be configured to use non-overlapping RF channels. This can easily exhaust the whole 2.4GHz ISM band. For example, two coexisting IEEE 802.11n networks are enough to occupy the whole 2.4GHz ISM band. Such scenario is not uncommon nowadays given the ubiquitous presence of WiFi networks. When all such WiFi networks are active, jamming the whole 2.4GHz ISM band, it is hard to carry out WBAN communications, no matter the WBAN uses ZigBee, Bluetooth, or the draft IEEE 802.15.6 2.4GHz standard.

Common Packet Formats: Due to backward compatibility considerations, all subtypes of WiFi running in 2.4GHz ISM band recognize the IEEE 802.11b packet format.

Viewing from the *Physical Layer* (PHY), we can abstract an IEEE 802.11b packet as three consecutive segments (see Fig. 2): PHY preamble, PHY header, and DATA[2].

The PHY preamble is for receiver carrier acquisition.

The PHY header contains several fields that carry control/management information. What is important is the LENGTH field, a 16-bit unsigned integer indicating the number of microseconds required to transmit the DATA segment. This implies that a maximum of 65535μs can be reserved for DATA segment.

[2]which correspond to *Physical Layer Convergence Protocol* (PLCP) preamble + *Start Frame Delimiter* (SFD), PLCP header, and *PLCP Service Data Unit* (PSDU) respectively according to standard jargon [13].

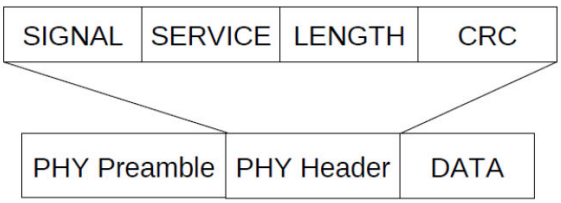


Fig. 2. IEEE 802.11b PHY packet format.

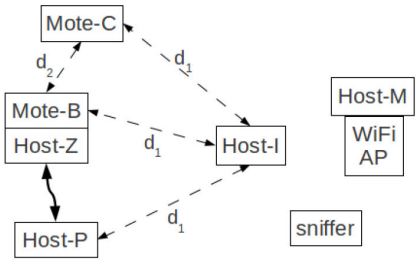


Fig. 3. Experiment Layout

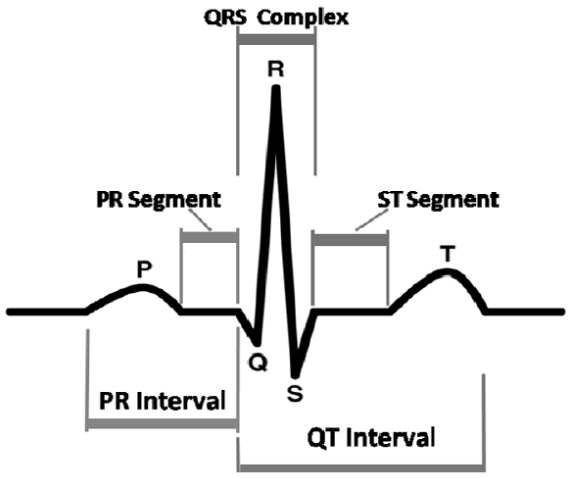


Fig. 4. Schematic representation of normal ECG[17]

Clear Channel Assessment (CCA): All subtypes of WiFi carry out *Carrier Sense Multiple Access* (CSMA) MAC protocol. According to CSMA, an IEEE 802.11 node shall always listen to the wireless medium before transmission. Only when the wireless medium is idle will the node start transmitting. This procedure is called *Clear Channel Assessment* (CCA).

There are three types of CCA: *Energy Detection* (ED) only, *Carrier Sense* (CS) only, and ED+CS (the combination of ED and CS). ED-only CCA measures the wireless medium spectral power level; if it is greater than a threshold, the wireless medium is considered busy. CS-only CCA tries to capture WiFi PHY preambles; if a PHY preamble is successfully captured, the wireless medium is considered busy. Usually, CS-only CCA also looks into the content of the PHY header immediately following the captured PHY preamble (if there is one) to provide more accurate CCA evaluations. ED+CS CCA does both. In practice, CS-only CCA and ED+CS CCA are most widely implemented [14][15].

III. A Case Study on ECG Monitoring

In this section, we study the performance of a ZigBee WBAN for ECG monitoring under WiFi interference, so as to empirically show the necessity of addressing the WBAN-WiFi coexistence problem.

A. Experiment Setup

Fig. 3 shows the layout of the experiment. The ECG monitoring WBAN consists of one base station and one ECG sensor, implemented by two TMote Sky nodes (aka *motes*, a well-known ZigBee device) [16] respectively. In Fig. 3, the base station is denoted as *Mote-B*, and the ECG sensor is denoted as *Mote-C*; the distance between *Mote-B* and *Mote-C* is d_2. The transmission power of *Mote-B* and *Mote-C* is set to the maximum: 0dBm. *Host-Z* is a laptop connected with *Mote-B* through USB for data collection. *Host-I* is the WiFi interferer. It sends packets to WiFi *Access Point* (AP) via an IEEE 802.11g wireless connection. The distance from *Host-I* to *Mote-B* and *Mote-C* are both d_1. In addition, *Host-M* is connected to the WiFi AP to record WiFi interference traffic between *Host-I* and the WiFi AP. An additional WiFi *sniffer* is deployed which passively logs WiFi events on the wireless medium. *Host-P* runs WiCop and is not used in this experiment.

Upon reception of ECG samples from the ECG sensor, the ECG base station reconstructs the ECG traces. A typical ECG trace for one heart beat period is shown in Fig. 4. An ECG trace normally contains P-wave, QRS complex, and T-wave[17]. The QRS complex usually has a much bigger amplitude than the P-wave[17], and contains rich frequency components. Therefore, good ECG monitoring needs high sampling rate. In our case study, the ECG sensor samples at 250Hz, a typical value for quality ECG monitoring [18]; and each sample is 8-bit. The ECG sensor (*Mote-C*) sends the base station (*Mote-B*) one packet every 100ms. Hence each packet contains 250Hz $\times$ 100ms = 25 new ECG samples, which we call an *ECG sample chunk*. In addition, to increase reliability, the ECG sensor (*Mote-C*) buffers the immediate 2 previous ECG sample chunks to be sent in the same packet as the new ECG sample chunk. Hence each packet contains 3 ECG sample chunks, i.e., $25 \times 3 = 75$ ECG samples; and every ECG sample is retransmitted 3 times. At the typical ZigBee raw bit rate of 250kbps, the transmission time cost of each packet is less than 4ms.

B. Performance Metric

To evaluate the performance of ECG monitoring under WiFi interference, we consider two metrics. The first metric is *Packet Reception Rate* (PRR), defined as the probability that a packet is successfully received.

Let $T_{polling}$ denote the ECG packet transmission period ($T_{polling} = 100$ms in our case study). As mentioned before,

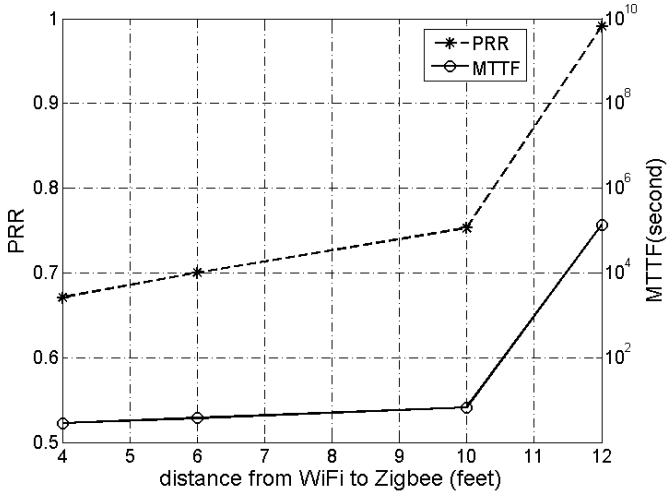


Fig. 5. PRR and MTTF of ECG monitoring WBAN under 802.11g interference

ECG samples are only transmitted in the grouping of ECG sample chunks; and each ECG sample chunk is retransmitted $N_{re} = 3$ times within $T_{polling} \times N_{re} = 300$ms (which is within the typical ECG sample delivery deadline [8]). An ECG sample chunk is lost iff it fails all its N_{re} retransmissions.

We hence introduce a second metric, *Mean Time To Failure* (MTTF), which is the expected duration between two ECG sample chunk losses. Using Markov chain analysis, we have

$$MTTF = \frac{T_{polling}}{PER^{N_{re}}}, \tag{1}$$

where $PER \stackrel{def}{=} 1 - PRR$.

C. Experiment Results and Observations

With the layout set as Fig. 3, we let *Host-I* transmit at an application layer rate of 30Mbps to the WiFi AP to emulate WiFi interference. The transmission power of *Host-I* is 30mW, a typical value adopted in practice [19]. As the distance from *Host-I* to *Mote-B* varies from 12 feet to 4 feet, the PRR decreases from 98% to 67% (see Fig. 5). At 67% PRR, the MTTF is 2.8s. In other words, on average every 2.8s, an ECG sample chunk may be lost. This would be a serious problem, as shown by Fig. 6.

Fig. 6 illustrates what it means when one ECG sample chunk is lost. In the figure, the solid line curve is the actual ECG curve; the dashed line curve is the ECG curve received at the base station (for ease of illustration, we moved this curve 350mV downward). The ECG sample chunk for $300 \sim 400$ms is lost. This results in the loss of a whole QRS complex, which carries critical information on the heart.

IV. WiCop Policing Strategies

In this section, we present the details of WiCop in regulating WiFi temporal white-spaces. The basic idea is to exploit the WiFi CCA mechanisms: sending WiFi compliant signals to refrain WiFi stations from transmitting.

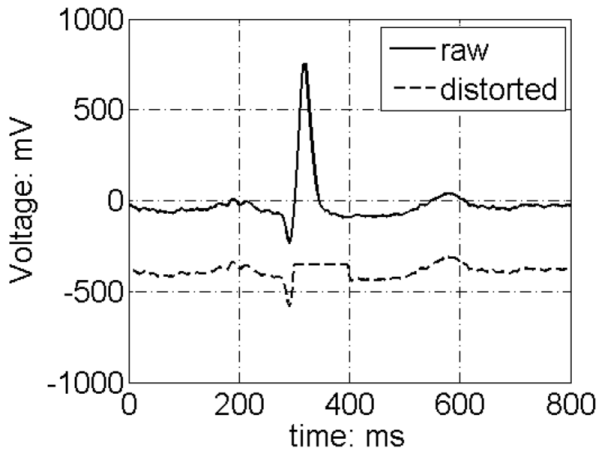


Fig. 6. Comparison of the raw and the (after-packet-loss) distorted ECG

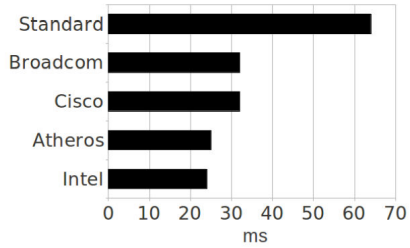


Fig. 7. Maximum duration a WiFi device mutes upon receiving a WiFi packet (whose PHY header LENGTH field is set to maximum).

A. Strategy I: Fake-PHY-Header

Policing Signal: As mentioned in Section II, viewing from PHY layer, a WiFi packet transmission begins with a PHY preamble, followed by a PHY header, and then the DATA. The PHY header carries a LENGTH field (see Fig. 2), a 16-digit unsigned integer specifying the number of microseconds that WiFi packet lasts.

When a WiFi device detects a PHY preamble and decodes the following PHY header, it will mute (i.e., refrain from transmitting) for a number of microseconds depending on the received LENGTH field and the device's specific implementation.

As the LENGTH field is a 16-bit unsigned integer, in theory, a maximum of 65535μs can be reserved. However, our calibration measurements show that the actual maximum duration that can be reserved is vendor dependent, as shown in Fig. 7. Fortunately, Fig. 7 also show all WiFi devices from major vendors can mute for at least 24ms. This is enough for reserving temporal white-spaces for our ECG monitoring WBAN communications: with each WBAN packet containing 75 8-bit samples, our WBAN only needs no more than 4ms to send a packet from the ECG sensor to the base station.

MAC Protocol: In this paper, we only focus on the scenario that WBAN carries out centralized polling, with a *WBAN polling period* of $T_{polling}$ (e.g., our case study in Section III

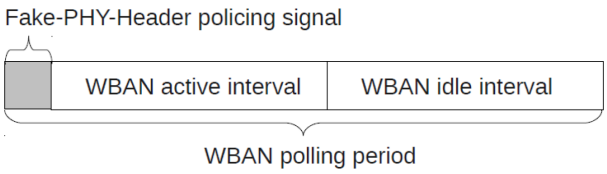


Fig. 8. Temporal scheme of Fake-PHY-Header policing

assumes a WBAN polling period of $T_{polling} = 100$ms). During each WBAN polling period, there is an interval that we call *WBAN active interval*. WBAN communications are only carried out during this WBAN active interval.

To policing means to force WiFi interferers to mute during the WBAN active interval in each WBAN polling period. To do this, we add an *policing node* to the WBAN. The policing node runs the WiCop framework by properly sending policing signals and controlling the WBAN operations. Ideally, the policing node shall reside on the same host as (or directly wired with) the WBAN base station, for easy control of the WBAN operations. One specific implementation is described by Fig. 3, where *Host-P* functions as the policing node, and is wired to the WBAN base station (*Mote-B*) through high-speed Ethernet.

In the temporal domain, the policing node and the WBAN base station must carry out a coordinated *Multiple Access Layer* (MAC) protocol to achieve the policing effect.

With the above in mind, Fig. 8 explains the Fake-PHY-Header MAC protocol in the temporal domain.

Each WBAN polling period is started with a policing node broadcast (the so called *Fake-PHY-Header beacon*): a fake WiFi packet with only PHY preamble and PHY header. Although this fake WiFi packet does not have DATA segment, its PHY header's LENGTH field still claims a packet duration equivalent to the temporal length of the WBAN active interval (hence "faking"). Immediately following this fake WiFi packet, the WBAN active interval starts (this can be achieved by application layer communications between the policing node and the WBAN base station), where the WBAN base station can poll its client(s).

The intuition of Fake-PHY-Header policing is that on hearing the Fake-PHY-Header beacon, a WiFi interferer will mute for the following WBAN active interval, creating a temporal white-space for WBAN to communicate.

B. Strategy II: DSSS-Nulling

Policing Signal: It is well-known that the continuous sending of repeated WiFi PHY preambles can jam other WiFi devices' transmissions [14][20]. Since WiFi PHY preamble is a DSSS modulated signal, we call the continuous sending of repeated WiFi PHY preamble "*DSSS-Jamming*". We intend to use DSSS-Jamming as another means of policing. However, DSSS-Jamming not only jams WiFi devices, it also jams other co-channel wireless devices. To solve this problem, we reshape the DSSS-Jamming signal with a band-pass filter to generate the desired policing signal. We call such generated

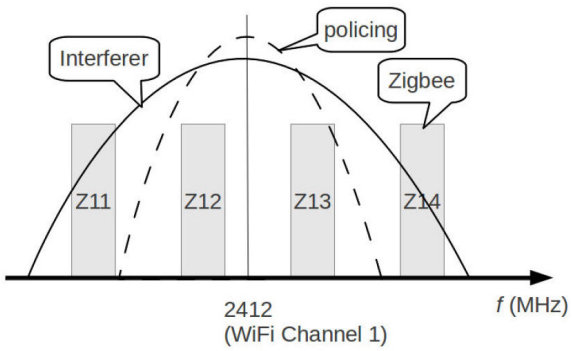


Fig. 9. PSD of WiFi interferer signal, DSSS-Nulling policing signal, and ZigBee signal

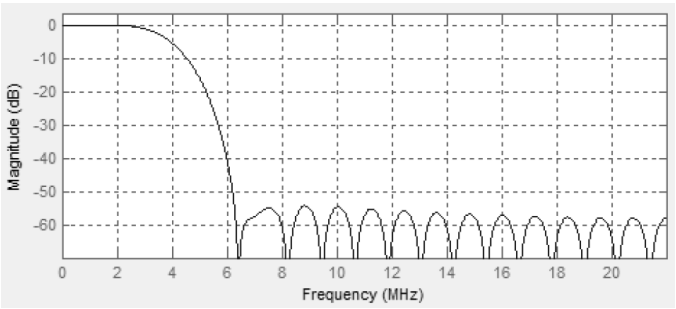


Fig. 10. Frequency response of the FIR that reshapes DSSS-Jamming signal into DSSS-Nulling signal (baseband equivalent spectrum)

policing signal "*DSSS-Nulling*" (i.e., the sides of the DSSS-Jamming signal spectrum are "nulled" to create spaces for WBAN signals) signal, and the corresponding policing scheme the "*DSSS-Nulling*" policing.

Fig. 9 compares the *Power Spectral Density* (PSD) of WiFi interferer signal, DSSS-Nulling policing signal, and ZigBee signal. When a DSSS-Nulling signal is present, a WiFi device thinks the carrier is busy and backs off. In contrast, as DSSS-Nulling signal does not occupy ZigBee channel $Z11$ and $Z14$, ZigBee communications are still possible.

In our prototype implementation, the band-pass filter to reshape DSSS-Jamming signal is a raised cosine *Finite Impulse Response* (FIR) filter, which results in a DSSS-Nulling signal bandwidth of 8MHz (in comparison, WiFi signal bandwidth is 22MHz). MATLAB simulations show that the side lobe of this filter is -55dB (Fig. 10). In other words, DSSS-Nulling signal's interference power on WBAN is 55dB less than that of DSSS-Jamming signal.

Alternatively, one can use other forms of noise signal (e.g., simply a sine wave) in the WiFi band to jam/police WiFi transmission. However, as DSSS-Nulling signal carries repeated WiFi PHY preamble information (though damaged by the band-pass filter), it can more effectively jam WiFi devices that support CS-only or ED+CS CCA. Based on Tanenbaum and Wetherall [21], we can infer DSSS-Nulling signal can use 20dB less power than other forms of noise to jam a ED+CS CCA WiFi device.

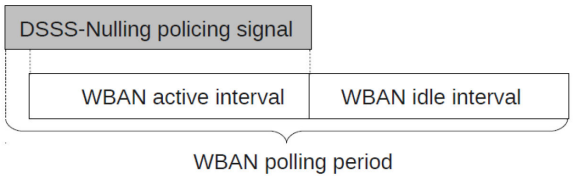


Fig. 11. Temporal scheme of of DSSS-Nulling policing

MAC Protocol: Same as the Fake-PHY-Header policing case, DSSS-Nulling policing still assumes the WBAN runs centralized polling and the policing node resides on the same host as (or is directly wired to) the WBAN base station. But instead of *preceding* a WBAN active interval, the DSSS-Nulling signal persists throughout the WBAN active interval as shown by Fig. 11.

C. Comparisons of Policing Strategies

Let us first assume each policing signal broadcast succeeds in suppressing all WiFi interferers.

In each WBAN polling period, there only needs to be one Fake-PHY-Header broadcast, which occupies 22MHz of spectrum (the standard WiFi PHY preamble/header spectrum bandwidth) and 0.2ms. Such a broadcast allows 4 ZigBee channels to communicate throughout one WBAN active interval. Therefore, the efficiency of Fake-PHY-Header policing is

$$\begin{aligned}\eta_{fake\_phy\_hdr} &\overset{def}{=} \frac{\text{Time-Spectrum Reserved for WBAN}}{\text{Time-Spectrum Overhead}} \\ &= \frac{4B_{zigbee}T_{wban\_act\_int}}{22 \times 0.2} \\ &= \frac{B_{zigbee}T_{wban\_act\_int}}{1.1}, \end{aligned} \quad (2)$$

where constant B_{zigbee}(MHz) is the bandwidth of a ZigBee channel, $T_{wban\_act\_int}$(ms) is the length of WBAN active interval.

Through experiments, we find effective DSSS-Nulling policing signal occupies at least 8MHz of spectrum. Meanwhile, DSSS-Nulling signal must persist throughout the WBAN active interval. This implies DSSS-Nulling policing can only help reserve two ZigBee channels throughout the WBAN active interval. Therefore, the efficiency of DSSS-Nulling policing is

$$\begin{aligned}\eta_{dsss\_nulling} &\overset{def}{=} \frac{\text{Time-Spectrum Reserved for WBAN}}{\text{Time-Spectrum Overhead}} \\ &= \frac{2B_{zigbee}T_{wban\_act\_int}}{8 \times T_{wban\_act\_int}} \\ &= \frac{B_{zigbee}}{4}. \end{aligned} \quad (3)$$

As $T_{wban\_act\_int}$ is usually 4ms $\sim$ 40ms, at the first glance, Formula (2) and (3) implies Fake-PHY-Header is more efficient than DSSS-Nulling. However, remember this is under the assumption that each policing signal broadcast succeeds in suppressing all WiFi interferers. In practice, DSSS-Nulling is much more reliable than Fake-PHY-Header in suppressing all WiFi interferers, as the former repeatedly broadcasts WiFi PHY preamble throughout the WBAN active interval; while the latter only broadcasts WiFi PHY preamble (and header) once.

A more comprehensive comparison between Fake-PHY-Header and DSSS-Nulling policing is summarized by Table I.

TABLE I
COMPARISON OF FAKE-PHY-HEADER AND DSSS-NULLING POLICING

	Fake-PHY-Header	DSSS-Nulling
Time-Spectrum Efficiency (if policing broadcast succeeds)	$\frac{B_{zigbee}T_{wban\_act\_int}}{1.1}$	$\frac{B_{zigbee}}{4}$
Success Probability	Low	High
Affected WiFi Interferer	CS-only CCA, CS+ED CCA	CS-only CCA, CS+ED CCA, ED-only CCA

V. IMPLEMENTATION

We implemented WiCop upon *Microsoft Research Software Radio* (SORA) [12] platform.

A SORA platform consists of the following hardware: a desktop computer (denoted as *Host-P* in Fig. 3), a *Radio Control Board* (RCB), and a third-party radio daughter board. The radio daughter board that we use is USRP XCVR2450.

Correspondingly, the SORA platform software mainly consists of the various software defined radio drivers and the corresponding development tools. For WiCop, we mainly implemented the aforementioned policing strategies upon SORA Soft WiFi driver v1.0 (simplified as "*SORA driver*" in the following). The details are as follows.

As shown by Fig. 12, in order to transmit a policing signal, WiCop sends a policing packet down through the SORA stack, which involves five layers (including three layers in the SORA driver: *Link Layer* (LL), MAC, and PHY). Each layer carries out special processing of the policing packet.

At the application layer (denoted as "Police App" in Fig. 12), WiCop customizes the payload of the policing packet according to the specific policing strategy used. For Fake-PHY-Header policing, the policing packet payload is nulled. For DSSS-Nulling policing, the policing packet payload length is adjusted according to WBAN active interval length, and the payload digits are all set to one. At the network layer (denoted as "UDP socket" in Fig. 12), a special IP/MAC address is used to flag the policing packet. In the LL layer, upon detecting the flagged IP/MAC address, we add special tags to the policing packet's descriptor (a data structure in SORA to record packet information). In the MAC layer, policing packets' backoff is deliberately shortened (to less than standard IEEE DIFS) to achieve a higher priority when contending with WiFi interferers. In the PHY layer, special processing is done according to the tag in the policing packet's descriptor. For Fake-PHY-Header policing packet, we customize the LENGTH field to cover the whole WBAN active interval. For DSSS-Nulling

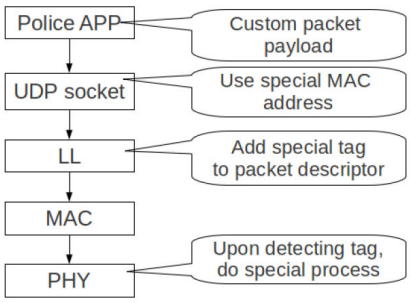


Fig. 12. Procedure of sending a policing packet

policing packet, we apply the band-pass filter to null its spectrum side lobe.

To realize the WiCop policing strategies, the policing node must work with the WBAN base station simultaneously. In our experiment set up (see Fig. 3), this is achieved by wiring the policing node (*Host-P*) and the WBAN base station (*Mote-B*) host (*Host-Z*) with high speed Ethernet.

VI. Evaluation

We evaluated WiCop through experiments.

A. Effects on WiFi Temporal White-Spaces

We first compare the WiFi temporal white-spaces when there is and is not WiCop policing. The experiment set up reuses Fig. 3's layout. *Host-I* is the WiFi interferer, which keeps sending WiFi traffic to WiFi AP. *Host-P* is the WiCop policing node, which is wired to the WBAN base station *Mote-B* (via *Host-Z*). The WBAN polling period is 10ms, and the WBAN active interval is less than 5ms. To protect such WBAN, the policing node broadcasts policing signal every 10ms, claiming a WBAN active interval of 5ms. This affects the WiFi interference traffic, which is recorded by *Host-M*, as *Host-M* monitors the WiFi AP (the WiFi interference traffic destination). Fig. 13 shows two typical excerpts of the WiFi interference traffic trace, one from when there is no WiCop policing, and the other from when there is WiCop policing (without loss of generality, the specific policing strategy used in this example is Fake-PHY-Header).

It is easy to see that when there is no policing, there is few WiFi temporal white-spaces wide enough to allow the 5ms WBAN active intervals (see Fig. 13(a)). In contrast, when there is policing, WiFi temporal white-spaces of more than 5ms wide emerge every 10ms, enough to allow the periodical WBAN communication: with period of 10ms and WBAN active interval length of 5ms.

We then compare the effectiveness between Fake-PHY-Header policing and DSSS-Nulling policing. Fig. 14 compares the statistics of WiFi temporal white-space lengths under these two policing strategies. For each policing strategy, we rerun the aforementioned experiment for 25s, with a WBAN polling period of 25ms and WBAN active interval of 5ms. Therefore, $25\text{s}/25\text{ms} = 1000$ WiFi temporal white-spaces of length $\geq$ 5ms should be created, if the policing is successful. This

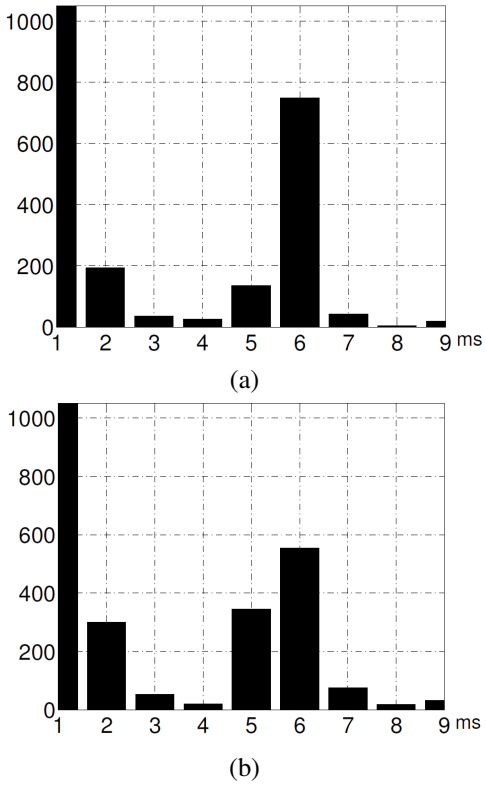


Fig. 14. (a) Histogram showing WiFi temporal white-space distribution under Fake-PHY-Header policing (b) Histogram showing WiFi temporal white-space distribution under DSSS-Nulling policing. The X axis is the range of the lengths of WiFi temporal white-spaces (granularity: 1ms); the Y axis is the the number of such WiFi temporal white-spaces encountered throughout the 25s experiment trial. Y axis is truncated at 1050 to save page space: temporal white-spaces in the $0 \sim 1$ms range are mostly those between consecutively transmitted WiFi packets. WiCop sends a policing packet every 25ms to claim 5ms of WBAN active interval.

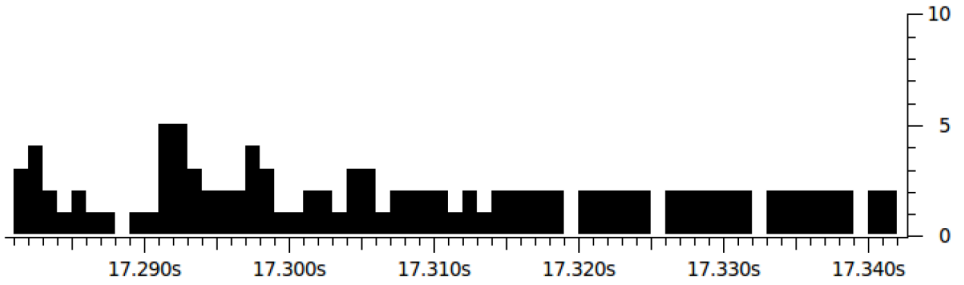
matches the results of Fig. 14, i.e., both Fake-PHY-Header and DSSS-Nulling achieve the goal of creating wanted WiFi temporal white-spaces. Note Fig. 14 also shows there are a large number of WiFi temporal white-spaces of length less than 1ms. This is because when WiFi is allowed to transmit continuously, there are short temporal white-spaces (each less than 1ms) between consecutive WiFi packets.

It is also of interest to see how WiFi transmissions are negatively affected by WiCop. Fig. 15 shows the throughput of TCP and UDP connections over WiFi when there is policing. The WBAN polling period is still 25ms. As the claimed length of WBAN active interval increases, the WiFi throughout decreases. However, when the claimed WBAN active interval is 5ms, the decreases of TCP/UDP throughput are both mild. This shows that our policing strategies enable the coexistence of WiFi and WBAN.

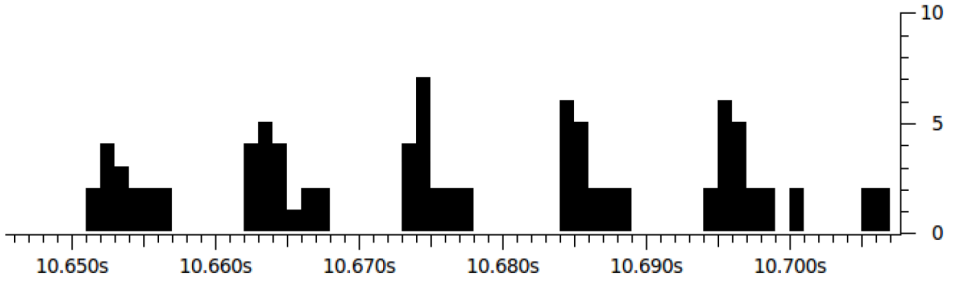
B. Effects on WBAN Performance

Now, we are in the position to evaluate the effects of WiCop on WBAN performance.

We reuse the experiment layout of Fig. 3. All wireless links are *Non-Line-Of-Sight* (NLOS).



(a)



(b)

Fig. 13. (a) WiFi interference traffic when there is no policing (b) WiFi interference traffic when there is policing. The X axis is time (unit: second); the Y axis is the the number of packets received in each 1ms time slot. In case of (b), WiCop sends a Fake-PHY-Header policing packet every 10ms to claim 5ms of WBAN active interval.

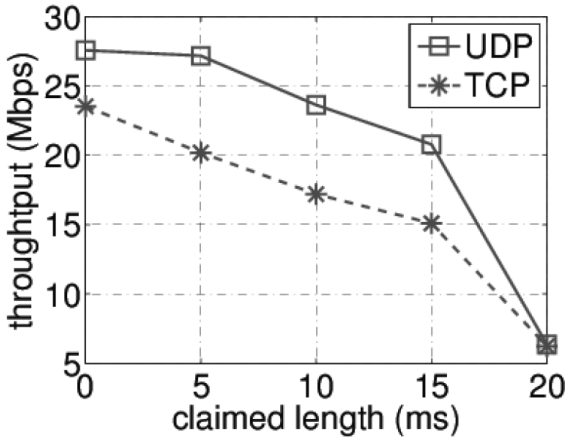


Fig. 15. WiFi throughput degradation under WiCop policing. X axis is the claimed length of WBAN active interval; Y axis is the throughput of WiFi interference traffic. WBAN polling period is 25ms.

The WBAN is a centralized ZigBee WBAN, which runs a WBAN polling period of 100ms, and a WBAN active interval of 5ms. Both the WBAN base station and WBAN client (*Mote-C*) transmits at 0dBm over a mutual distance of $d_2 = 4$ feet.

The WiFi interferer (*Host-I*) runs IEEE 802.11g and transmits at power level of 30dBm. Its distances to the WBAN base station (*Mote-B*), WBAN client (*Mote-C*), and WiCop policing node (*Host-P*) are all set to $d_1 = 6$ feet. The WiFi interference source end data rate is set to 15Mbps, 20Mbps, and 25Mbps respectively. For each WiFi interference source end data rate, three experiment trials are carried out, respectively corresponds to no policing, Fake-PHY-Header policing, and DSSS-Nulling policing. Each trial lasts 300s.

The results are summarized by Fig. 16 and Fig. 17, which plot the PRR and MTTF of the WBAN respectively.

A number of observations can be made. First, under heavy WiFi interference (e.g., when WiFi interference source end data rate is 25Mbps), the WBAN PRR degrades significantly if there is no policing. Second, DSSS-Nulling policing performs better than Fake-PHY-Header policing in maintaining WBAN PRR under heavy WiFi interference. This is because DSSS-Nulling policing signal continuously repeats throughout the WBAN active interval; while Fake-PHY-Header policing signal is just broadcasted once, right before each WBAN active interval. Third, WiCop can significantly improve WBAN performance under WiFi interference. For example, under heavy WiFi interference (25Mbps trials), DSSS-Nulling policing can improve PRR by 43.8% (from 0.683 to 0.982), and improve MTTF from 3.1 seconds to 4.8 hours.

VII. Related Work

In this section, we provide a brief overview of related work pertaining to WiCop in the area of 1) WBAN and WiFi coexistence, 2) Denial of Service attack (DoS) to WLANs, and 3) experimental evaluation in real medical settings.

A. Coexistence

It is widely accepted that WiFi can severely interfere ZigBee communication [11][3][2]. Huang et. al.[11] argued that the performance degradation of ZigBee in the presence of WiFi interference is caused by two main reasons, namely power asymmetry and carrier sense based CCA. Accordingly, Huang

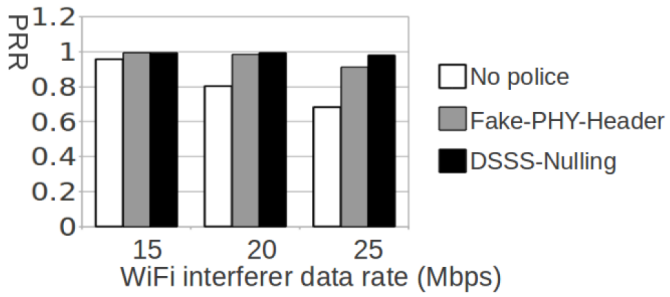


Fig. 16. WBAN PRR under different WiFi interference source end data rates

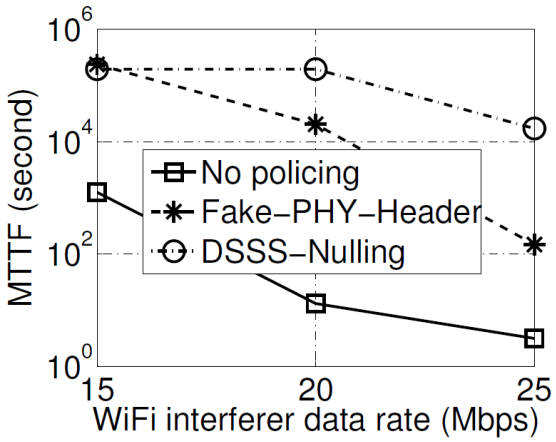


Fig. 17. WBAN MTTF under different WiFi interference source end data rates

designed a MAC protocol to detect and use the idle time slice (white-spaces) in WiFi sessions. Shin et. al.[3] conducted numerical analysis and simulations to evaluate the PER of ZigBee communication under the interference of WiFi. It is argued that WiFi would not impact ZigBee communication if the separation of their center frequency is bigger than 7MHz. The experiments in [2] showed that WiFi might interfere ZigBee transmission significantly under certain conditions even with a center frequency offset of 18MHz. Recently, many researchers found that ZigBee transmitters might impact WiFi performance under certain conditions [22][10][23]. Most of these works use packet loss rates to measure the performance of WBAN. However, in our work, applying ZigBee to latency sensitive application, we use both MTTF and PRR as performance metrics.

Hou[4] uses the duration field of the RTS MAC header to reserve time. In the design, before broadcasting a beacon, a ZigBee base station first send an RTS packet to reserve a channel. This design bears similarity with the proposed Fake-PHY-Header policing strategy, but Fake-PHY-Header has one advantage over it: Fake-PHY-Header introduces less control overhead. The reason is that Hou's approach requires sending a whole packet to reserve the channel, while our approach only sends out a packet header, which takes less air time. Hou's design is more suitable to reserve a long duration. However, WBANs typically support low duty cycle applications, and thus continuous long duration is not needed.

Liang[10] proposes a mechanism to detect and estimate the white-spaces in WiFi transmission and designs an MAC protocol to utilize white-spaces of different lengths. Arkoulis[24] proposes a simple and efficient method to detect a single operational frequency channel that guarantees satisfactory communication. However, in some cases, whites-paces in time and frequency domain may not exist or are insufficient. WiCop, in contrast, enforces whites-paces on demand to support WBAN traffic.

B. DoS

A few work has investigated mechanisms for jamming WiFi transmissions from a security point of view. Karhima [25] evaluated WiFi's tolerance to wide-band and narrow-band jamming. Park [26] and Mishra [27] studied partial-band jamming to WiFi. The defect of current IEEE 802.11 standard has also been exploited to attack WiFi. Gummadi et.al. [14] found that some WiFi cards were sensitive to beacon losses. Thus, jamming periodic beacon is an effective means to attack WiFi. Our work aims to provide co-existence between WLANs and WBANs. Thus, malicious attacking methods, such as jamming beacon, fake death packet, are not considered. Wullems [20] used the DSSSTESTMODE of a WiFi device to jam WLANs. In this optional working mode, a WiFi device will transmit continuous DSSS preambles, so that the other WiFi devices in range will sense the channel as busy. Bellard [28] used commercial hardware to carry out de-authentication and virtual carrier-sense attack. They found that the later was not as effective as the former. Thuente [29] studied several intelligent jamming methods with the requirement of low power and low detection probability, including DIFS waiting jamming, ACK corruption jamming, fake RTS jamming, etc..

C. Experimental Evaluation in Medical Environments

Paksuniemi et. al. [30] reveals problem areas in patient monitoring when applying Bluetooth, ZigBee and UWB to vital sign monitoring in ICU and operating rooms. Chipara et. al. [7] designed and deployed ZigBee based patient monitoring in a general hospital unit. Ko et. al. [31] conducted experiments on the patient monitoring in emergency rooms. However, few of these works considers the interference from other wireless technologies.

Garudadri [32] applied Compressed Sensing to ECG. This approach uses the redundancy in periodic ECG trace, to mitigate distortion under high packet losses. This approach is orthogonal to WiCop and can be used in conjunction with WiCop to further improve the robustness of ECG monitoring.

Finally, it should be noted that WiCop is a general mechanism to regulate white-spaces in WiFi transmissions. Though we have demonstrated its effectiveness with ZigBee-based WBANs, it can be utilized to protect WBANs based on other wireless technologies operating in the ISM bands.

VIII. Conclusion

Our empirical study confirms that for safety-critical WBAN medical applications (such as ECG) with stringent temporal requirements, co-channel WiFi interference is an eminent threat. To address this WBAN-WiFi coexistence challenge, we can exploit WiFi's CCA mechanisms to propose the WiCop policing framework. By deploying Fake-PHY-Header and DSSS-Nulling policing strategies, the WiCop policing framework can effectively engineer the temporal white-spaces of WiFi transmissions, reserving enough resource for WBAN communications without significantly affecting WiFi performance. We implemented and validated WiCop on SORA, a software defined radio platform. Experiments show that with the assistance of the proposed WiCop policing strategies, even under heavy WiFi interference, the packet reception rate of a ZigBee-based WBAN can increase by up to 43.8%.

As future work, we will extend WiCop in a number of directions. First, we are interested in determining the optimal bandwidth for the *DSSS-Nulling*. Second, we will experiment with more WiFi devices and profile their compatibility. Third, we will study the effect of WiCop on TCP over WiFi and reduce the degradation to the later.

Acknowledgement

The research project related to this paper in Hong Kong Polytechnic University (HK PolyU) is supported in part by Hong Kong RGC General Research Fund (GRF) PolyU 5245/09E, The HK PolyU Internal Competitive Research Grant (DA) A-PJ68, HK PolyU Newly Recruited Junior Academic Staff Grant A-PJ80, HK PolyU Fund for CERG Project Rated 3.5 (DA) grant A-PK46, and Department of Computing start up fund. Guanbo Zheng and Rong Zheng are supported in part by the US National Science Foundation (NSF) under award CNS-0832089 and CNS-1117560. Rong Zheng is also supported in part by the HK PolyU Department of Computing Sabbatical Visitor Program. We thank Prof. P. R. Kumar, Prof. Lui Sha, and Prof. Marco Caccamo in UIUC for providing facilities and equipments for this research; we thank Dr. Kun Tan in Microsoft Research (Asia) for helpful discussions on SORA; and we thank the comments from anonymous reviewers that help improving this paper.

References

[1] M. . J. W. Patel, "Applications, challenges, and prospective in emerging body area networking technologies," *IEEE Wireless Comm.*, vol. 17, p. 80, Feb. 2010.

[2] R. de Francisco, L. Huang, and G. Dolmans, "Coexistence of wban and wlan in medical envrionments," 2009.

[3] S. Y. Shin, S. Choi, H. S. Park, and W. H. Kwon, "Packet error rate analysis of ieee 802.15.4 under ieee 802.11b interference," *LNCS: Wired/Wireless Internet Communications*, vol. 3510, no. 2005, pp. 279–288, 2005.

[4] J. Hou, B. Chang, D.-K. Cho, and M. Gerla, "Minimizing 802.11 interference on zigbee medical sensors," in *BodyNets '09 Proceedings of the Fourth International Conference on Body Area Networks*, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering) ICST, Brussels, Belgium, 2009.

[5] N. Golmie, R. V. DYCK, A. SOLTANIAN, A. TONNERRE, and O. REBALA, "Interference evaluation of bluetooth and ieee 802.11b systems," *Wireless Networks*, vol. 9, pp. 201–211, 2003.

[6] Y. Wang and Q. Wang, "Evaluating the ieee 802.15.6 2.4ghz wban proposal on medical multi-parameter monitoring under wifi/bluetooth interference," vol. 2, no. 3, pp. 48–62, 2011.

[7] O. Chipara, C. Lu, T. C. Bailey, and G.-C. Roman, "Reliable clinical monitoring using wireless sensor networks: experiences in a step-down hospital unit," in *Proceedings of the 8th ACM Conference on Embedded Networked Sensor Systems*, 2010.

[8] N. Chevrollier and N. Golmie, *On the Use of Wireless Network Technologies in Healthcare Environments*. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.106.3216&rep=rep1&type=pdf, 2005.

[9] *IEEE Standard 1073*, 1998.

[10] C.-J. M. Liang, N. B. Priyantha, J. Liu, and A. Terzis, "Surviving wi-fi interference in low power zigbee networks," in *Proceedings of the 8th ACM Conference on Embedded Networked Sensor Systems*, 2010.

[11] J. Huang, G. Xing, G. Zhou, and R. Zhou, *Beyond Co-existence: Exploiting WiFi White Space for ZigBee Performance Assurance*. http://www.cse.msu.edu/~glxing/, 2009.

[12] K. Tan, H. Liu, J. Zhang, Y. Zhang, J. Fang, and G. M. Voelker, "Sora: high-performance software radio using general-purpose multi-core processors," *Communications of the ACM*, vol. 54, no. 5, Jan. 2011.

[13] *IEEE Standard 802.11*, 1997.

[14] R. Gummadi, D. Wetherall, B. Greenstein, and S. Seshan, "Understanding and mitigating the impact of rf interference on 802.11 networks," 2007.

[15] *IEEE Standard 802.11*, 2007.

[16] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer Networks*, vol. 52, no. 12, pp. 2292 – 2330, 2008.

[17] *Electrocardiography*. http://en.wikipedia.org/wiki/Electrocardiography.

[18] *PhysioNet*. http://www.physionet.org.

[19] N. Golmie, D. Cypher, and O. Rebala, "Performance analysis of low rate wireless technologies for medical applications," *Computer Communications*, vol. 28, no. 10, pp. 1266–1275, 2009.

[20] C. Wullems, K. Tham, J. Smith, and M. Looi, "A trivial denial of service attack on ieee 802.11 direct sequence spread spectrum wireless lans," in *Wireless Telecommunications Symposium*, 2004.

[21] A. S. Tanenbaum and D. J. Wetherall, *Computer Networks*. Prentice Hall PTR, 2010.

[22] S. Pollin, I. Tan, B. Hodge, C. Chun, and A. Bahai, "Harmful coexistence between 802.15.4 and 802.11: A measurement-based study," in *Proceedings of Cognitive Radio Oriented Wireless Networks and Communications*, 2008.

[23] an Hinrich Hauer, V. Handziski, and A. Wolisz, "Experimental study of the impact of wlan interference on ieee 802.15.4 body area networks," in *Lecture Notes in Computer Science*, vol. 5432, 2009, pp. 17–32.

[24] S. Arkoulis, D.-E. Spanos, S. Barbounakis, A. Zafeiropoulos, and N. Mitrou, "Cognitive radio-aided wireless sensor networks for emergency response," vol. 21, December 2010.

[25] T. Karhima, A. Silvennoinen, M. Hall, and S.-G. Haggman, "Ieee 802.ltb1g wlan tolerance to jamming," in *Military Communications Conference*, 2004.

[26] J. Park, D. kim, C. Kang, and D. Hong, "Effect of partial band jamming on ofdm-based wlan in 802.11g," in *Proceedings of Acoustics, Speech, and Signal Processing*, 2003.

[27] A. Mishra, V. Shrivastava, S. Banerjee, and W. Arbaugh, "Partially overlapped channels not considered harmful," in *Proceedings of the joint international conference on Measurement and modeling of computer systems*, 2006.

[28] J. Bellardo and S. Savage, "802.11 denial-of-service attacks: real vulnerabilities and practical solutions," in *Proceedings of the 12th conference on USENIX Security Symposium*, vol. 12, 1994.

[29] D. J. Thuente and M. Acharya, "Intelligent jamming in wireless networks with applications to 802.11 b and other networks," in *Proc. of IEEE MILCOM*, 2006.

[30] M. Paksuniemi, H. Sorvoja, E. Alasaarela, and R. Myllyla, "Wireless sensor and data transmission needs and technologies for patient monitoring in the operating room and intensive care unit," in *Paper presented at Engineering in Medicine and Biology Society*, 2005.

[31] J. Ko, J. H. Lim, Y. Chen, R. Musvaloiu-E, A. Terzis, G. M. Masson, T. Gao, W. Destler, L. Selavo, and R. P. Dutton, "Medisn: Medical emergency detection in sensor networks," in *Transactions on Embedded Computing Systems (TECS)*, vol. 10, 2010.

[32] H. Garudadri, P. Baheti, S. Majumdar, C. Lauer, F. Masse, J. van de Molengraft, and J. Penders, "Artifacts mitigation in ambulatory ecg telemetry," in *e-Health Networking Applications and Services*, 2010.