This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE ICC 2009 proceedings

Interferer Classification, Channel Selection and Transmission Adaptation for Wireless Sensor Networks

Kaushik R. Chowdhury and Ian F. Akyildiz
Broadband Wireless Networking Laboratory
School of Electrical and Computer Engineering
Georgia Institute of Technology
Atlanta, GA 30332
Email: {kaushikc, ian}@ece.gatech.edu

***Abstract*—Wireless sensor networks (WSNs) are being increasingly deployed in office blocks or residential areas for commercial applications, such as home automation, meter reading, surveillance, among others. At these locations, the WSNs experience interference in the $2.4\,\mathrm{GHz}$ unlicensed band due to wireless LANs (WLANs) and commercial microwave devices, leading up to 92% packet losses. In this paper, an algorithmic framework is proposed, that allows the sensor nodes to identify the type of the interferer and its operational channel, so that the former may adapt their own transmission to reduce packet losses in the network. Our proposed interference classification approach comprises of an (i) offline measurement of the spectral characteristics of the WLAN and microwave devices to obtain a reference spectrum shape, and (ii) matching the observed spectral pattern during network operation with the stored reference shape The knowledge of the interferer characteristics is then leveraged by the sensor nodes to decide their transmission channel, packet scheduling times and sleep-awake cycles. Results reveal that our approach incurs up to $50-70\%$ energy savings in the WSN, by reducing interference related packet losses.**

I. Introduction

Wireless sensor networks (WSN) comprise of simple, resource constrained nodes that are being increasingly used for military use, environmental monitoring and data gathering applications [1]. In addition to these, several commercial applications of WSNs have been envisaged, such as, home automation, meter reading and surveillance that may be deployed in residential areas or office blocks. These sites may already be under the coverage of commercial wireless LANs (WLANs) or have electrical devices such as microwave ovens operating in the vicinity. The radiation from these devices results in interference for the WSN, and for the specific case of the WLAN, experiments reveal nearly 92% packet losses [2] [3]. As there is a significant energy cost associated with packet retransmissions, the co-existence of the WSN with the WLAN and microwave interferers is of critical importance.

The commercial WLANs based on the IEEE 802.11b/g standard [4], and the WSN operating under the specifications of the IEEE $802.15.4$ standard [5], use the $2.4\,\mathrm{GHz}$ ISM band. While the WLAN devices are not constrained in energy, the sensor nodes are battery powered and must proactively avoid concurrent transmissions. The commercial microwave ovens also generate interfering radiation in the ISM band during their operation. Recent research has mainly focussed on measuring the performance degradation caused by the effect of WLAN and microwave technologies on the devices based on the IEEE $802.15.4$ standard [8]. Efforts have also been made to quantify the effect of these external interferers on the ZigBee devices that add the medium access control (MAC) layer to the physical layer specifications laid down by the $802.15.4$ standard [9]. The effect of channel scanning and learning based on the past history on the sensor-WLAN co-existence is explored in [3]. The experimental findings show that though there exists measurable packet loss due to the microwave oven on the IEEE $802.15.4$ based sensors, the WLAN affects them at large distances, in the order of tens of meters, with packet errors nearly an order of magnitude higher.

An important difference between the WLAN and the microwave interference lies in their respective transmission cycles. While the WLAN devices rely on opportunistically gaining the control of the channel when it is vacant, the microwave oven operates at a fixed, pre-decided duty cycle ranging from $30-50\,\%$ [6] [7]. Thus, by knowing the *type* of the interferer, the WSN can choose its transmission channel and reporting frequency so that there is minimum network interference. The key contributions of our work are as follows:

- We propose an algorithm that allows us to classify an unknown source of interference based on the observed channel power measurements.
- We propose a scheme for choosing the transmission channel and packet scheduling for the WSN to leverage the identified interferer characteristics, and reduce interference related losses.

The rest of this paper is organized as follows: Section II, describes our experiments with WLAN and microwave ovens and the proposed interferer classification technique. Section III presents our scheme for adapting the transmission of the WSN. We undertake a thorough performance evaluation in Section IV, and finally, Section V concludes our work.

978-1-4244-3435-0/09/$25.00 ©2009 IEEE

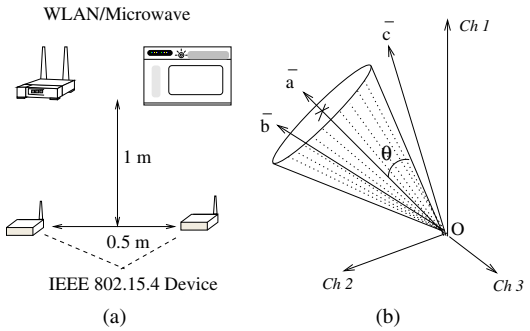


Fig. 1. The experimental setup to measure the WLAN and microwave interference (a) and the allowed conical region for classification of the interferer (b).

II. Interferer Identification and Channel Selection

In this section, we first describe a set of experiments to study the spectral shape of the power emitted by IEEE 802.11b WLANs [4] and microwave in the $2.4\,\mathrm{GHz}$ band. Having obtained the reference spectral shape (which we define as the *spectral signature*), we describe our algorithm for identifying the interferer type and channel. This is then used by the sensor nodes to choose the best available channel.

For our experiments, we used a pair of IEEE $802.15.4$ based (test) sensors equipped with a TI-Chipcon CC2420 radio [10] for sweeping through the available $5\,\mathrm{MHz}$ channels. In each channel, the test sensors measure (i) the interference power or received signal strength strength (RSS) and the (ii) packet success rate (PSR) by sending a total of 100 packets. The sensors are separated by $0.5\,\mathrm{m}$ and the straight line joining them is at a $1\,\mathrm{m}$ perpendicular distance from the interferer device, as shown in Figure 1(a).

A. WLAN Experiments

The WLAN transmitter, equipped with a Netgear MA401 802.11b card, pinged the receiver with 64 byte packets continuously at a rate of $11\,\mathrm{Mbps}$ on channel 8. As the first step, we measured the received power in each of the channels in the test device. The experiments were carried out inside a radio frequency shielded Faraday cage. The cage provides noise insulation of up to $-97\,\mathrm{dBm}$, thus allowing precision experiments with the devices. Figure 2(a) shows that the measured power in the channels of the test device follows the spectrum of the IEEE 802.11b standard. The channels $18-21$ are the most affected, as shown by the lower packet success rate (PSR) in Figure 2(b). These four sensor channels come under the coverage of the WLAN channel, which has a spread of $22\,\mathrm{MHz}$[1]. We shall consider this characteristic behavior in our subsequent analysis for detecting the presence of a WLAN.

B. Microwave Experiments

Our setup consists of a Daewoo KOR-6NB5 microwave, operating at $1\,\mathrm{KW}$. From Figure 2(c), we see that the received power from the microwave oven peaks at about $2455-2460\,\mathrm{MHz}$ affecting channels 20 and 21 strongly. However, there exists a significant sideband power centered in the vicinity of channels 17 and 19, at about $2440\,\mathrm{MHz}$. Consequently, the channels 17, 19, 20, and 21 in the test device are most strongly affected by the microwave operation, as is shown in Figure 2(d). Of these, channel 21 exhibits relatively higher performance degradation with an approximate PSR of 0.88. Interestingly, unlike the WLAN, the degraded channels are not contiguous. As seen in Figure 2(c), Our findings are consistent with [6] on the effect of microwave devices on Bluetooth, which has a similar channel structure as defined in the IEEE $802.15.4$ standard.

We next propose an algorithm for identifying the presence of these interferers based on their power spectral signatures.

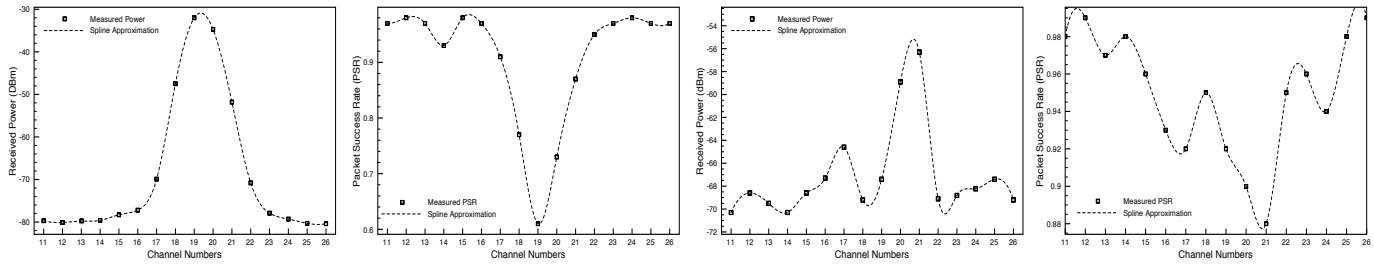
C. Interferer Identification

We propose an algorithm that allows nodes to classify the interferer based on the power received in each of the affected channels, defined as its *spectral signature*. We do this by comparing the spectral signature with a reference signature obtained by prior experimentation. Our approach accounts for the fact that the received signal may be affected by ambient noise and other temporary outages, thus distorting the overall spectral shape.

We now describe our scheme using a simple scenario, in which, an interferer affects three channels $C = \{c_1, c_2, c_3\}$. This algorithm is then extended for the specific cases of the microwave and WLAN interferers. The sensor node first measures the received power, b_1, b_2 and b_3 respectively, for each of the channels in set C. Visualizing the channels as a set of orthogonal axes, from Figure 1(b), we see that they form the x, y and z axes of a cartesian coordinate system. A vector can now be constructed as $\vec{b} = b_1\hat{c_1} + b_2\hat{c_2} + b_3\hat{b_3}$, that compactly represents the sensed power value in the three channels. Additionally, the unit vector along that direction is given by, $\hat{b} = \frac{\vec{b}}{|b|}$. This unit vector captures the relation between the power values sensed in the channels through its spatial orientation. By a similar procedure, we obtain the reference values for the interferer and construct the unit vector $\hat{a}$, prior to the deployment of the network. The difference between the reference power values and those obtained by the current measurement is expressed as the angular difference θ_{obs} between the two unit vectors given by the scalar dot product $\theta_{obs} = \cos^{-1}\{\hat{a}.\hat{b}\}$. Thus, the unit vector becomes independent of the actual measured power in the individual channels. We define a conical region around the reference vector $\hat{a}$ by an angle θ, such that, any measured vector $\hat{b}$ within that region ($\theta > \theta_{obs}$) can be considered as a positive match. We discuss the effect of choosing θ on the sensing accuracy in Section IV-A.

1) Microwave Detection: From our experiments in Section II-B, we observe that the $802.15.4$ channels affected by the microwave operation are given by $C_M = \{16, 17, 20, 21, 25\}$, and this set does not change with time. Thus, the procedure to construct the unit reference vector $\hat{a}_M$

[1]The channel power is attenuated by at least $-30\,\mathrm{dB}$ at $\pm 11\,\mathrm{MHz}$ on either side of its center frequency [4]



(a) (b) (c) (d)

Fig. 2. The PER and the RSS for the WLAN and the microwave experiments are shown

follows along the lines of the above example, but considering an orthogonal axis for each affected channel. Using the reference power values from our test experiments, we obtain the reference unit vector $\hat{a}_M$ as, $\hat{a}_M = -0.477\hat{c_1} - 0.458\hat{c_2} - 0.418\hat{c_3} - 0.399\hat{c_4} - 0.478\hat{c_5}$.

2) WLAN Detection: With the WLAN tuned to channel 8, we observe that the sensor channels most affected are the four channels $18 - 21$. Thus, we construct the reference unit vector $\hat{a}_W$ in the four dimensional space with the power values obtained in the test experiments (Figure 2(a)) as, $\hat{a}_W = -0.561\hat{c_1} - 0.378\hat{c_2} - 0.41\hat{c_3} - 0.612\hat{c_4}$.

In order to use $\hat{a}_W$ as the reference vector, we must first prove that irrespective of the WLAN channel, the adjacent sensor channels, based on the IEEE 802.15.4 standard and used for measurements, have the same proportions of the leakage power as is seen in the test case (Section II-A). This will ensure that the observed received powers in these sensor channels are proportional to the values seen in the test experiments, and allow the reference vector $\hat{a}_W$ to be applied in practical deployment conditions.

Let the channel numbers for the WLAN and the 802.15.4 based WSN be given by $M = 1, \ldots, 11$ and $K = 11, \ldots, 26$, respectively. The channel center frequencies for the WLAN (f_M^W) and the sensors (f_K^S) in the ISM band, for the channels M and K, are defined by their respective standards as,

$$\begin{aligned} f_M^W &= 2412 + 5(M-1),\ M = 1, \ldots, 11 \\ f_K^S &= 2405 + 5(K-11),\ K = 11, \ldots, 26 \end{aligned} \quad (1)$$

In addition, simplifying the set of equations in (1), we obtain the following relationship between the channel numbers of the two different standards,

$$M = \frac{(f_{K+1}^S + 2) - 2412}{5} + 1,\ K = 11, \ldots, 23 \quad (2)$$

Substituting in equation (1) the channels $\{18, 19, 20, 21\}$ affected by the WLAN operation on channel $M = 8$ as found in Section II-A, we find that their respective center frequencies were $7, 2, 3$ and $8\,\mathrm{MHz}$ respectively from f_8^W. This can be trivially extended for the general case, implying that a well defined and constant frequency separation ($\delta_{i,M}$) exists between the four closest sensor channels, $i = K, \ldots, K+3$, and a given WLAN channel M. This constant difference ensures that the shape of the reference spectral signature is the same irrespective of the WLAN channel used.

The problem of WLAN detection is finding the set of 4 contiguous channels used by the sensors, in which, the received power best matches the reference shape derived in Section II-A. Using equation (2), for $K = 21$, we get $M = 11$, which is the upper limit on the channels for the WLAN. Thus, K is varied in the range $[1, 21]$ and each time the next three channels are considered along with it for the purpose of finding a match with $\hat{a}_W$, e.g. the set $\{11, 12, 13, 14\}$ if $K = 11$.

D. Channel Selection

We recall that the sensor channels affected by the microwave oven are constant, while depending upon the WLAN center frequency, different sensor channels are affected. The WSN nodes sense the available channels and classify the interferers once every epoch time T. First, the channels that have the ambient noise floor above the allowed threshold η_T are selected. In this selection, if there exists a channel that has no WLAN or microwave oven detected, then such a channel is chosen as the operational channel. If no such free channel exists, then the channel that is affected by the microwave device is chosen over the others that perceive WLAN activity. This is because the well defined duty cycle of the microwave allows for longer sleep times and easier inter-node synchronization. We next describe how the sensors adapt their transmission for mutual co-existence with the interferer in the chosen channel.

III. Interferer-aware Transmission Adaptation (ITA)

In this section, we show how the sensor nodes adapt their operation through our proposed interferer-aware transmission adaptation (ITA) scheme, for the following interferer types:

A. WLAN Interferer

Figure 3 shows the timing diagram for packet transmissions between two IEEE 802.11b WLAN nodes 1 and 2. The RTS-CTS message exchange is followed by the data packet and the ACK, each separated by the Short Inter-Frame Space ($SIFS$). After the data packet is successfully sent, the nodes sense the channel for a duration given by the Distributed Inter-Frame Space ($DIFS$), defined as $DIFS = SIFS + 2 \cdot \sigma$,

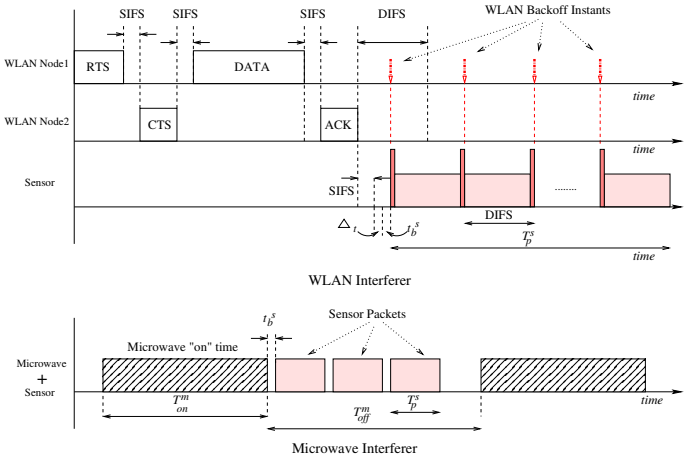
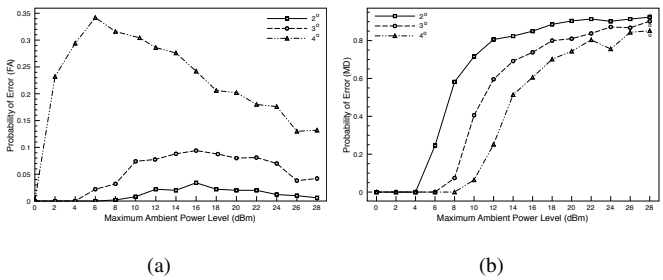


Fig. 3. The sensor transmits whenever the channel is free based on the WLAN traffic or microwave duty cycle.



(a) (b)

Fig. 4. The probabilities for false alarm (FA) and missed detection (MD) for the spectral signature matching technique are given in (a) and (b), respectively.

where σ is the slot time. If the channel is indeed free for the DIFS time, the contending WLAN nodes set a backoff timer before initiating the next data transmission. As the packet transmission by a sensor takes comparatively longer time, it must silence the WLAN devices in this duration to prevent interference. Moreover, an ongoing transmission by the WLAN nodes must not be affected and thus, the sensor node may initiate the sending of the data packet of duration T_p^s only after the ACK (Figure 3). This condition is identified by the channel being free for a duration greater than $SIFS$.

After a sensor node awakens from its sleep schedule, it continues to monitor the channel till it finds it to be free for a duration given by $t_{sense}^s = SIFS + \triangle_t$, where $\triangle_t$ is taken as $5\,\mu$s. The sensor then sets a random backoff for a duration t_b^s to resolve intra-WSN contention and then transmits its own data packet. Additionally, the sensor packet has a transmission power peak at each DIFS interval to silence the WLAN nodes whose magnitude is set as the maximum WLAN power measured during channel sensing. The rest of the sensor packet is sent at the lower power (typically $35\,\mathrm{mW}$ [10]). The other sensor nodes that find the channel already captured by an ongoing sensor transmission enter into the sleep mode for the minimum duration $t_{sleep}^s = T_p^s + DIFS + RTS + CTS + DATA + 3SIFS$. This duration covers the sensor transmission time as well as the minimum time needed to transmit a WLAN packet. The peaked power pulses emitted by the sensor nodes interrupts the DIFS carrier sense timer at the WLAN nodes. This forces a *backoff* among the contending WLAN devices, and leaves the channel free for the sensor to complete its transmission.

B. Microwave Interferer

During the interferer classification stage, if the microwave oven radiation is detected, the sensor nodes determine the duty cycle of the device. The duty cycle estimation is based on averaging the time the channel is sensed busy (T_{on}^m) and the duration for which it is free (T_{off}^m). This duty cycle is at most 50% [7] for most residential devices and the comparatively long free channel duration ($T_{off}^m = 0.5 - 1\mathrm{s}$) allows several WSN packets can be scheduled in succession, as shown in Figure 3. The sensors align their own sleep cycles with the duty cycle of the microwave oven, i.e. $t_{sleep}^s = n \cdot (T_{on}^m + T_{off}^m),\ n \in \mathrm{I}$, and synchronized at the start of the *off* time. Thus, whenever the sensor node wakes up, the channel is free for the duration T_{off}^m for packet transmissions. Between two consecutive sensor packets, there is a contention period of t_b^s, as in the case of the WLAN interferer, for channel contention.

We next evaluate the performance of our proposed interferer classification technique the ITA approach.

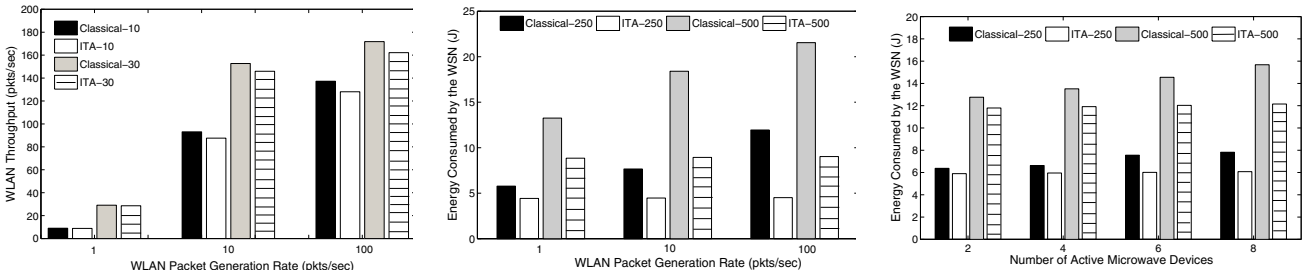
IV. Performance Evaluation

In our simulation, 300 nodes are placed in a square region of side $300\,\mathrm{m}$ as the default configuration. The number of nodes in the WLAN operation are varied between 10 and 20, while $1, 10$ and $100\,\mathrm{pkts/sec}$ are the packet generation rates at each WLAN node. As we use two different medium access control schemes, i.e. simple CSMA/CA for the WSN and the IEEE 802.11b for the WLAN in the same network, we have implemented our approach in a custom C++ simulator. The WLAN transmission radius is $300\,\mathrm{m}$, while the transmit and receive power for the sensor nodes are $35\,\mathrm{mW}$ at $-5\,\mathrm{dBm}$, and $38\,\mathrm{mW}$, respectively [10], with the power consumption during idle time is comparable to the receiving power. The sensor packet is of $50\,\mathrm{bytes}$, and the default sleep time is $1\,\mathrm{s}$.

A. Interferer Type And Channel Estimation

We consider the reference waveform from Figure 2(c) for the microwave oven, and measure the false positive errors returned by our algorithm. Similar results obtained for the case of the WLAN are excluded owing to space constraints.

The noise floor is set at $-92\,\mathrm{dBm}$ and due to channel outages and ambient power sources, each of the 16 sensor channels experience different received power values. We vary the maximum amplitude of this received power and measure the probability of false alarm (FA), i.e., returning a positive match when the channel actually experiences an ambient power in Figure 4(a). Here, each channel is randomly assigned a power value bounded by this maximum possible level and three cases of the angle threshold θ_{max} are shown. We observe that for $\theta_{max} < 3^{\mathrm{o}}$, the resulting error is contained within 5% for moderate to high $(2 - 8\,\mathrm{dBm})$ ambient noise power and is



(a) (b) (c)

Fig. 5. The effect on the WLAN throughput (a), the energy consumption of the WSN in presence of WLAN (b) and microwave oven (c).

still less than 10% for very high values. The increase in the error and its subsequent fall can be attributed to the following: for small ambient power levels, our algorithm classifies the observed readings as noise. Similarly, for large ambient power values ($26 - 28\,\mathrm{dBm}$), there is significant deviation in the RSS and the classification error occurs with lower probability. For moderate ambient power, there is a greater probability that adjacent channels may experience power values within the acceptable range and this is reflected in the high number of incorrect classifications. In Figure 4(b), we measure the probability of missed detection (MD), in which, the microwave interferer is actually present but could not be detected with the threshold limit at 3°. We observe this increases with noise and the performance for the different values of θ_{max} is indistinguishable after $22\,\mathrm{dBm}$.

B. Interferer-aware Transmission Adaptation (ITA)

We now study the co-existence issues when our proposed approach is disabled (defined as *classical*) and when the interferer-aware transmission adaptation (ITA) is enabled. Though, the sensor nodes capture the channel between successive WLAN transmissions, we observe that the throughput of the WLAN is affected minimally in Figure 5(a), for different number of WLAN nodes (10 and 30), and also for increasing packet generation rates. For this result, we compare the ITA scheme with the WLAN throughput in absence of the WSN operation (*classical*). The energy consumed by the WSN in the presence of the WLAN interferer is shown in Figure 5(b), for 250 and 500 sensors, respectively deployed in the area of consideration. In the *classical* approach, the WSN nodes operate with the default sleep schedule and without the periodic pulsed power transmissions in ITA, that silences the WLAN nodes. The resulting packet loss results in frequent retransmissions, thus giving an energy saving of more than 50% in the ITA approach. Our approach ensures that the WLAN nodes *backoff* during the entire packet transmission time of the sensor nodes, thereby avoiding interference related packet losses. For the microwave oven, the difference between the energy consumption of the *classical* scheme that does not adapt to the duty cycle, and the ITA scheme is primarily caused by *idle* listening (Figure 5(c)). Our approach ensures that the sleep time of the sensors is aligned with the microwave oven duty cycle ($1\,\mathrm{s}$) and the transceivers are switched on only at the microwave cycle *off* duration. Interestingly, though the time for which the channel is free for a given microwave interferer is much larger, as compared to the WLAN, the number of transmitted sensor packets is not significantly higher. This is because the different ovens do not have a synchronized duty cycle, and the sensor nodes must wait for an *off* duration that is overlapping with all the microwave devices.

V. Conclusions

In this work, we have proposed algorithms that allow spectrum-aware WSNs to detect the presence of a WLAN or a microwave oven coexisting in the $2.4\,\mathrm{GHz}$ band. Based on the interferer classification, our scheme estimates the free channel durations in advance, thereby preventing packet loss. The ITA approach yields $50 - 70\%$ reduction in the WSN energy consumption, and there is minimal performance degradation in the service of the interfering network, such as the WLAN.

Acknowledgement

This work is supported by the US National Science Foundation under contract CNS-07251580.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless Sensor Networks: A Survey *Elsevier Computer Networks Journal*, 38(4):393–422, March 2002.

[2] Steibeis-Transfer Centre. Compatibility of IEEE 802.15.4 (Zigbee) with IEEE 802.11 (WLAN), Bluetooth, and Microwave Ovens in 2.4GHz ISM-Band *Online*:http://www.ba-loerrach.de

[3] S. Pollin, M. Ergen, M. Timmers, A. Dejonghe, L. van der Perre, F. Catthoor, I. Moerman and A. Bahai. Distributed cognitive coexistence of 802.15.4 with 802.11. *In Proc. of IEEE CrownCom*, pp.1–5, 2006.

[4] IEEE Std 802.11b-1999/Cor 1-2001, 2001.

[5] Draft Standard for Low-Rate Personal Area Networks *IEEE 802.15.4/D17*, October 2002.

[6] T. W. Rondeau, M. F. D'Souza, and D. G. Sweeney. Residential Microwave Oven Interference on Bluetooth Data Performance. *IEEE Trans. on Consumer Electronics*, 50(3):856–863, August 2004.

[7] T. M. Taher, M. J. Misurac, J. L. LoCicero, and D. R. Ucci. Microwave Oven Signal Modelling. *In Proc. of IEEE WCNC*, pp.1235–1238, April 2008.

[8] A. Sikora, and V. F. Gora. Coexistence of IEEE 802.15.4 with Other Systems in the 2.4 GHz ISM Band. *In Proc. of the IMTC Instrumentation and Measurement Tech. Conf*, vol. 3, pp. 1786–1891, May 2005.

[9] M. Zeghdoud, P. Cordier, and M. Terre. Impact of Clear Channel Assessment Mode on the Performance of ZigBee Operating in a WiFi Environment *In Proc. of the IEEE Wkshp. on Operator-Assisted (Wireless Mesh) Community Networks*, pp.1–8, September 2006.

[10] CC2420 radio datasheet
Website: http://focus.ti.com/docs/prod/folders/print/cc2420.html