Computers, Materials & Continua
DOI:10.32604/cmc.2020.013430
Article

Towards Interference-Aware ZigBee Transmissions in Heterogeneous Wireless Networks

Sangsoon Lim[1] and Sanghyun Seo[2,*]

[1]Department of Computer Engineering, Sungkyul University, Anyang, South Korea
[2]School of Computer Art, Chung-ang University, Anseong, South Korea
*Corresponding Author: Sanghyun Seo. Email: sanghyun@cau.ac.kr
Received: 06 August 2020; Accepted: 12 September 2020

Abstract: Cross-technology interference (CTI) from diverse wireless networks such as ZigBee, Bluetooth, and Wi-Fi has become a severe problem in the 2.4 GHz Industrial Scientific and Medical (ISM) band. Especially, low power and lossy networks are vulnerable to the signal interferences from other aggressive wireless networks when they perform low power operations to conserve the energy consumption. This paper presents CoSense, which accurately detects ZigBee signals with a reliable signal correlation scheme in the presence of the CTI. The key concept of CoSense is to reduce false wake-ups of low power listening (LPL) by identifying the pre-defined ZigBee signatures. Our scheme is robust in the coexistence environment of diverse wireless technologies since the signal correlation works well in bad wireless channel conditions. It achieves standard compliance and transparency without any hardware and firmware changes. We have implemented CoSense on the Universal Software Radio Peripheral (USRP) platform to verify its feasibility. The experimental exploration reveals that CoSense significantly reduces the false-positive and false-negative rate under typical setting and the additional overhead is negligible. The results show that our scheme saves much energy by up to 63% in dynamic network interference scenarios where low-power ZigBee transmissions are overwhelmed by strong Wi-Fi signal interferences.

Keywords: Heterogeneous wireless networks; interference; ZigBee detection; energy efficiency; low-power listening

1 Introduction

The explosive growth of battery-powered wireless devices over the last decade has brought great convenience to our daily lives. To achieve diverse service requirements in the Internet of Things (IoT), several wireless networks such as Wi-Fi [1], Bluetooth [2], and ZigBee [3] have been devised in the 2.4 GHz ISM band. They compete with each other to efficiently utilize spectrum resources. Coexistence problem among incompatible wireless networks has led to severe interferences that degrade overall network performance [4]. This is particularly true for battery-powered sensor nodes with low-power wireless technologies. In low-power wireless networks such as ZigBee, energy is the main concern and

low power operations directly improve the network lifetime [5]. Since each node consumes a large amount of power while transmitting and receiving a sensed data, it is important to devise a clever communication mechanism to conserve energy consumption. Several previous studies in fact show that idle listening and overhearing are the main sources of energy wastes [5,6]. The approaches to solve the energy wastes are categorized into two groups: synchronous approach [5] and asynchronous approach [6]. Synchronous approaches are more efficient in terms of energy consumption than asynchronous approaches [7,8]. However, it is difficult to provide a global synchronization among deployed nodes with limited computing power in unstable channel conditions. In case of asynchronous approach, there are two types of low-power listening (LPL) protocols; sender-initiated [9] and receiver-initiated rendezvous mechanisms [10,11].

In sender-initiated LPL protocols [9], an intended receiver periodically senses the ZigBee packet every duty-cycle interval while performing Clear Channel Assessment (CCA). During the CCA operation, the receiver checks whether the medium is idle of busy. Once it detects the busy status of the medium, the intended receiver stays awake waiting for the incoming ZigBee packet. After the operation, a transmitter consecutively sends data packets until detecting an acknowledgement or reaching the start of sleep period in a duty-cycle interval. In receiver-initiated LPL protocols [11], a receiver periodically transmits probing packets every duty-cycle interval. When a node has a data packet to send, the node changes the status of its RF transceiver to active state and listens the medium for a pre-defined negotiation packet. If the pre-defined negotiation packet from the intended receiver reaches to the sender, it immediately transmits data packets. Both approaches are stably operated in many well-known testbeds.

However, the dense deployment of heterogeneous wireless devices in the shared 2.4 GHz ISM band extremely aggravates the overall energy efficiency and reliability of low-power ZigBee networks. The CTI from other wireless devices can cause frequent false wake-ups, which activate false idle listening. Due to the increasing idle listening period, a ZigBee device consumes much energy during LPL operations. To mitigate the problem, ContikiMAC [8] identifies a ZigBee packet with two phase CCA and ZiSense [12] classifies energy levels of signals with a rule-based pattern matching mechanism. Due to the unexpected variation of RSSI processing in the real environment, RSSI-based approaches have severe limitations in performance improvement. Especially, when heterogeneous wireless signals of different wireless networks exist, the RSSI-based approaches cannot effectively mitigate the false-wake up problem. CrossZig [13] detects the CTI in corrupted packets with PHY layer hints such as signal power, hamming distance, and soft values of demodulated bits. AccuEst [14] estimates corruptions of ZigBee packets with link layer characteristics of pilot symbols. However, those approaches rely on the PHY and link layer components, which are simply inaccessible.

In this paper, we devise a clever approach, called CoSense, to accurately identify ZigBee signals in a noisy-environment. CoSense leverages both the RSSI pattern-based approach and signal correlation technique. Signal correlation is an effective mechanism to recognize pre-defined signal patterns in noisy wireless environment. ZigZag decoding [15] and CSMA/CN [16] employ cross-correlation to identify corrupted wireless packets effectively. In 802.11ec [17], the main approach is to reserve the shared medium without any legacy RTS/CTS by using the cross-correlation technique. Our key concept is to accurately classify ZigBee transmissions with the pre-defined ZigBee signatures in the presence of the CTI. CoSense achieves a high detection accuracy in the ZigBee detection phase by extracting the signal feature of the ZigBee packet. In addition, CoSense avoids unnecessary wake-ups of LPL protocols by checking two-phase identification during duty-cycling. Due to the randomness of the pre-define signature in our scheme, it does not aggravate the performance of traditional ZigBee transmissions. Normal ZigBee nodes regard the signatures as noise and ignore them.

We have implemented a prototype of CoSense on a software-defined radio (SDR) to prove the feasibility of our proposed scheme. In addition, we evaluate the overall performance of our scheme through trace-based

simulations and experiments. The experimental results show that our scheme conserves much energy compared to well-known LPL mechanisms. It improves the robustness while existing diverse CTI patterns. We summarize the main contributions of this paper as follows.

- We analyzed the realistic features of CTI on low power and lossy networks employing a well-known duty-cycling mechanism such as ContikiMAC. In real environment, consecutive CCA mechanism of ContikiMAC cannot alleviate false wake-up problem due to the limitations of RSSI processing.
- We devise an accurate ZigBee signal detection scheme in the presence of other signal interferences. Our scheme senses ZigBee transmissions while running duty-cycling operations. We also point out false triggering problem of a traditional ZigBee transceiver.
- We developed our scheme with USRP/GNURadio platform and measure its overall performance with diverse realistic scenarios. We verify its feasibility and practicality in highly noisy wireless environment deployed multiple heterogeneous wireless devices.

The rest of this paper proceeds as follows. Section 2 introduces related works. Section 3 describes the limitation of prior work. We present the detailed operations of CoSense in Section 4. Section 5 evaluates our new design. Finally, Section 6 concludes the paper.

2 Related Works

2.1 Cross-Technology Interference

The 2.4 GHz ISM band is commonly shared wireless medium that inherently susceptible to interferences from diverse concurrent transmissions among Wi-Fi, Bluetooth, and ZigBee. Traditional coexistence solutions among them mainly focus on a carrier sense mechanism or a channel allocation to avoid concurrent transmissions in time and frequency domain.

However, this is unfavorable for low-power ZigBee networks because they more prone to starvation due to their hardware limitations such as relatively small transmission power and computing capability of micro control unit (MCU) [18]. When ZigBee networks compete with Wi-Fi networks, ZigBee networks occasionally cannot preempt the wireless medium due to their disadvantageous MAC layer protocol timing. A ZigBee node takes 192us to switch the transceiver modes (i.e., RX-TX or TX-RX). On the other hand, a Wi-Fi node immediately can transmit its packet during the switching period because its backoff takes only 72us.

In a real environment, ZigBee networks experience a packet loss rate by up to 85% in the presence of Wi-Fi traffic load [19]. To investigate the interference patterns in ZigBee networks, BuzzBuzz [4] measured interactions among Wi-Fi and ZigBee networks at the bit-level granularity. In symmetric interference scenarios, a lot of bits are corrupted at the front part of a Zigbee packet. On the other hand, bit errors occur uniformly throughout the entire packet in asymmetric interference scenarios. There have been several similar studies to analyze the CTI problem [20,21,22]. However, our work considers the detailed duty-cycling operations of LPL protocols to show that it works practicality in a real low-power ZigBee network.

2.2 Cross-Technology Communication

Although wireless coexistence causes severe interferences among sharing wireless devices in the same public spectrum, it can provide new opportunities to mitigate the CTI. Cross-technology communication (CTC) is a promising approach to deal with the coexistence problem of heterogeneous wireless technologies [23,24,25]. Wireless devices operating in the same band sense the energy level of wireless medium such as received signal strength indicator (RSSI) and channel state information (CSI). Due to different features of the PHY/MAC layers, they cannot decode raw signals of other wireless technologies.

The key concept of the CTC is to provide a packet-level or physical-level modulation/demodulation mechanism to establish direct communication among heterogeneous senders and receivers. FreeBee [23] embeds symbols into the timing of periodic beacon frames of Wi-Fi APs by slightly shifting them. In the receiver side, FreeBee extracts position-modulated beacon frames via an 802.15.4-compliant RF chip [26] on the ZigBee node and decodes them. In the overlapping frequencies, different wireless technologies can exchange coordination information to schedule packet transmissions through the CTC. Although these solutions provide a direct communication to exchange coordination information, they still do not guarantee fair access to a low-power duty-cycled ZigBee networks.

3 Problem Statement

3.1 Heterogeneous Wireless Networks

In the real Internet of Things (IoT) environment, there exist heterogeneous wireless technologies adopting different PHY and MAY layers. Each transmission of a wireless technology can effectively aggravate normal transmissions of other wireless technologies since they cannot communicate each other. In this paper, we mainly concentrate on detecting low power ZigBee transmissions while existing 2.4 GHz ISM band interference from Wi-Fi and bluetooth. Our scheme can be easily extended to additional interferences in the shared 2.4 GHz ISM band such as cordless phone, baby monitor, microwave oven, and so on. The false wake-up problem of low-power operations in ZigBee networks wastes much energy every duty-cycle interval. We design our scheme to remedy the problem.

Fig. 1 illustrates Wi-Fi, ZigBee and Bluetooth channels in the 2.4 GHz ISM band. ZigBee uses a MAC layer of the IEEE 802.15.4 standard. There are sixteen available channels in the 2450 MHz band.

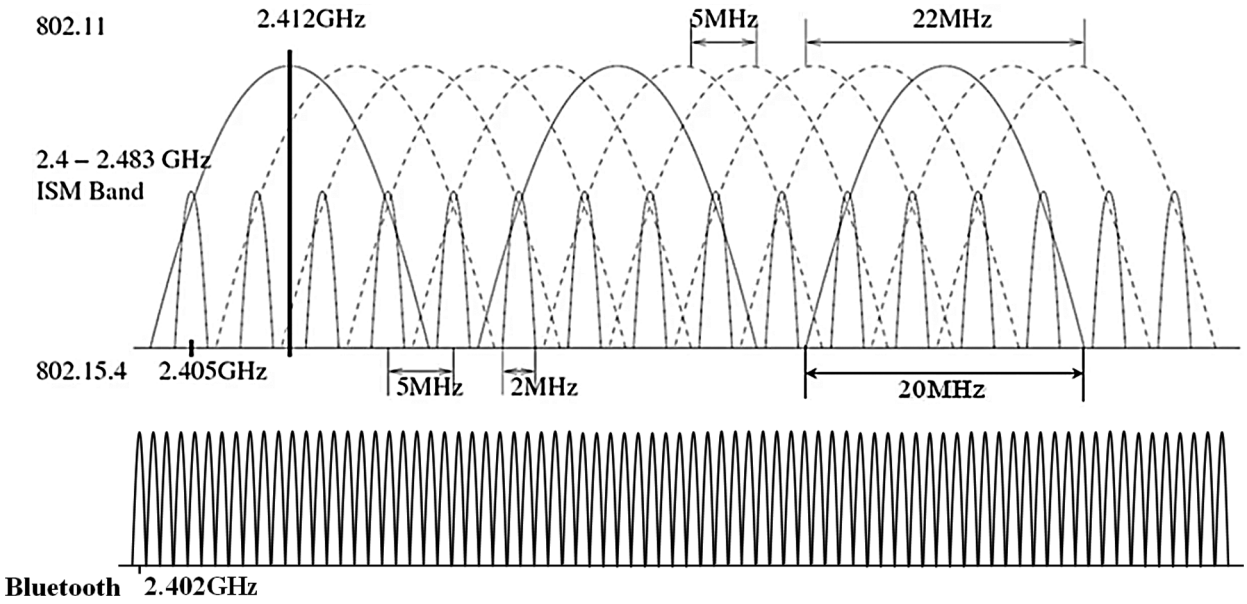

Figure 1: Wi-Fi, ZigBee, and Bluetooth channels in 2.4 GHz ISM band

$$F_c = 2405 + 5(k - 11), \text{for } k = 11, 12, \ldots, 26 \quad (1)$$

where k is the channel number. The channel employs O-QPSK modulation with 5 MHz channel spacing. The channel width is 2 MHz wide and the inter-channel spacing is 3 MHz wide. The IEEE 802.11 standard operates in the same 2.4 GHz ISM band. It consists of thirteen channels with a 22 MHz wide and each channel interferes

with four 802.15.4 channels. The basic features of both wireless technologies are quite different, resulting in a severe coexistence problem. The maximum transmission power level of a ZigBee is 0 dBm, whereas the transmission power level of a Wi-Fi is around 15 dBm or above. In addition, the sensins slot of a ZigBee is much larger than a Wi-Fi, so that it dramatically increases collision probabilities of both networks. The Bluetooth standard performs frequency hopping spread spectrum (FHSS) technology in the shared 2.4 GHz ISM band. Although the signal of Bluetooth occupies only 1 MHz, a Bluetooth device deterministically changes its center frequency over seventy nine channels and sends a traffic with lower power compared to a Wi-Fi. Thus, it causes a sparse interference to a ZigBee device.

3.2 Features of Low Power Operations

The energy efficiency is the foremost apprehension in ZigBee networks. Most MAC protocols of a ZigBee network performs a duty-cycling mechanism to remedy idle listening and overhearing time by periodically turning the RF module on/off. It significantly prolongs the lifetime of a battery-powered ZigBee node. TinyOS [27] and Contiki, which are well-known operating systems in WSNs, use asynchronous duty-cycling operations. Asynchronous approaches are much better than synchronous approaches in terms of scalability and energy efficiency in a heterogeneous wireless environment. The asynchronous approaches can reduce negotiation overheads and avoid a global synchronization problem of synchronous approaches. In real WSN testbeds, sender-initiated low power MAC protocols are more preferable due to its simplicity. Although our scheme is applied for sender-initiated low power MAC protocols, it can be generally extended to the receiver-initiated low power MAC protocols with a negligible modification.

3.3 False Wake-up Problem

The transceiver of a ZigBee device estimates energy level of the received signal strength within the channel bandwidth. It only identifies the presence of the signal on the channel during eight symbol periods. The channel assessment mechanism based on the energy level detection is susceptible to the interference from heterogeneous wireless technologies since it cannot easily separate the mixed signals. Eventually, the incorrect operation of channel assessment causes a false wake-up problem that considerably consumes the energy in idle listening time. Figs. 2(a) and 2(b) show the problem of a basic low power operation in a negotiation process when there exist multiple interferences from diverse sources such as Wi-Fi, Bluetooth, and microwave oven. When a node has a data to transmit, the node first sends successive data packets until receiving an acknowledgement from the target receiver. If the sender does not receive any response from the designated receiver while transmitting consecutive data packets during an entire duty-cycle interval, the transmission attempt fails and it re-initiates in the next period. In a case of a receiver, it wakes up to sense the energy level of the medium and waits for the incoming packets after detecting the presence of the signal. The detection mechanism decides whether the node goes to the sleep mode or stays awake. However, the signals of the mixed heterogeneous wireless networks generate a signal level higher than the threshold of the channel assessment, leading to incorrect judgment. Thus, the receiver falsely waiting for an incoming data wastes much energy during unnecessary idle listening.

We examine the interference patterns of a well-known asynchronous low power operation of a ZigBee network. We measure a lot of raw signals in various scenarios such as home, office and cafe. We embed our measurement component to NETSTACK-RDC in Contiki 2.7 as shown in Fig. 3. One of the most important features of Contiki is a well-defined and simple network protocol stack, called NETSTACK. Contiki OS consists of four layers to cover all traditional OSI layers. The performance of our scheme is closely related to the following three components; NETSTACK-RADIO, NETSTACK-RDC, and NETSTACK-MAC. NETSTACK-RADIO modules handle TX/RX operations in the lowest layer of the network stack. NETSTACK-RDC modules provide a low power duty-cycling mechanism by allowing a node to stay its

RF transceiver off during idle listening time. During the duty-cycling mechanism, we can accurately analyze the behaviors of false-ups from our measurement component. NETSTACK-MAC modules sense the medium before sending based on CSMA/CA. If NETSTACK-NETWORK modules determine the number of transmissions, the NETSTACK-MAC decides whether it should backoff a transmission or not based on the medium status and the timing of NETSTACK-RDC. We implement the component on a TelosB device, which is one of the most popular wireless sensor nodes. It uses 802.15.4 compliant RF transceiver and MSP430 Micro Control Unit (MCU). We set up the experimental environment with one transmitting node and one receiving node. The sender transmits its measured channel information every 10 seconds. The reception node operates with the low power operation of NETSTACK-RDC turned on. At this time, the default duty-cycle interval is set to 125 ms and the channel assessment threshold is set to −77 dBm in consideration of the CC2420 reception sensitivity.

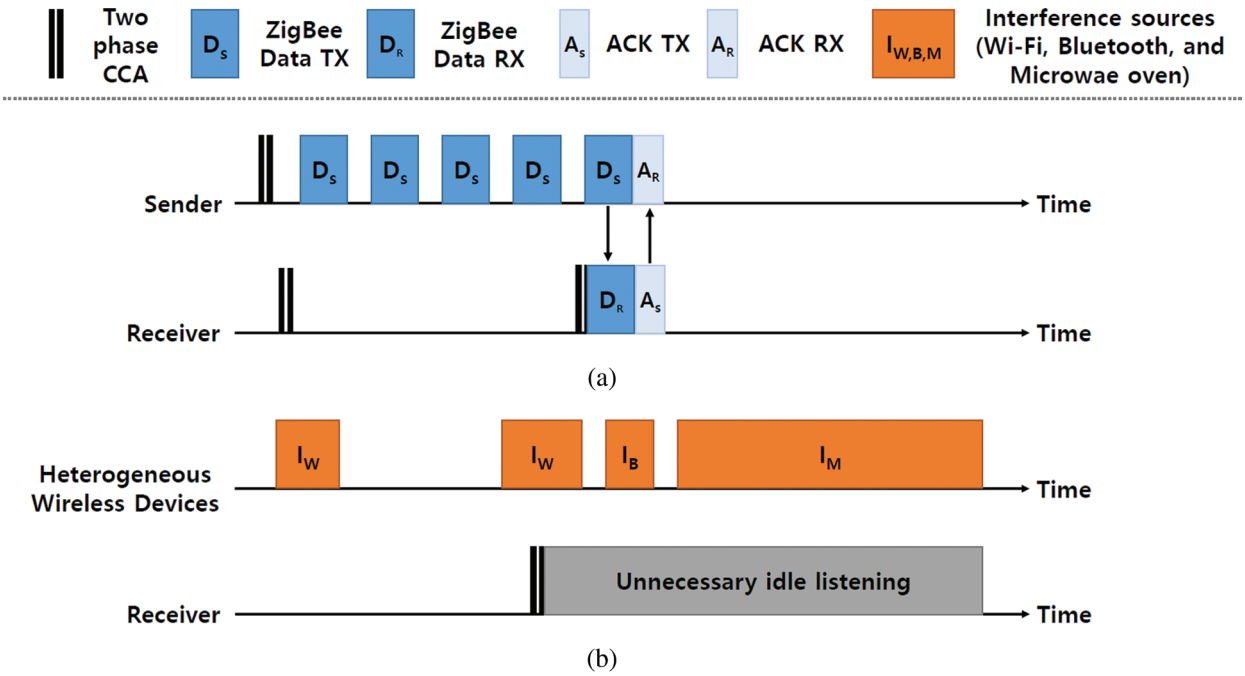

Figure 2: (a) A basic low power operation (b) Unnecessary idle listening caused by multiple interferences

Fig. 4(a) shows the incorrect operation rates of the traditional low power operation used in Contiki OS. A relatively small number of wireless devices are operated in home environment. As a result of measuring with a ZigBee node performing low power operation, we confirm that 10% unnecessary wake-ups occur when there is no ZigBee traffic. In the office where more than ten wireless devices are operating, we can see more severe cross-technology interference. More than 30% of abnormal wake-ups occurred at most points. This shows that the number of Wi-Fi and Bluetooth devices increases in the same space, the false wake-up problem of the existing low power operation in a ZigBee network steadily increases. In order to verify the energy level detection scheme, we modify the two phase CCA by changing the number of channel assessment to one and three. Fig. 4(b) illustrates the effect of the successive channel assessment in terms of false wake-up rates. When the receiver checks the energy level only once to evaluate the channel status, the false-wake up rate is increased by 2.5% at home and 5.6% at office compared to the two phase CCA. It means that the receiver can avoid small interference traffics during the second channel assessment. However, even if the receiver performs energy level sensing three times, the rate is slightly

decreased. The results explain that the existing channel sensing scheme based on energy level is weak to simultaneous transmissions of heterogeneous wireless technologies in real environments.

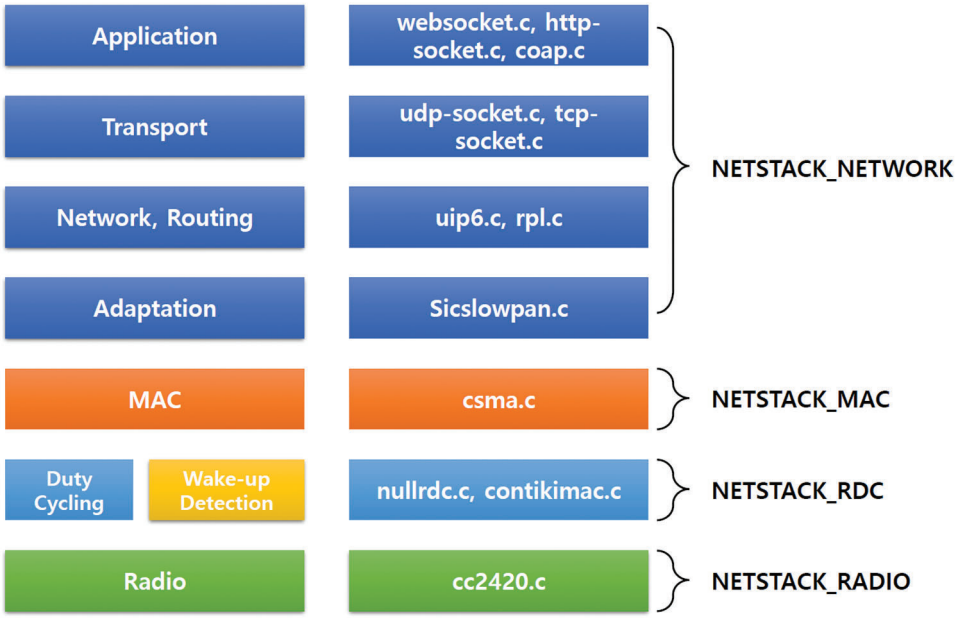

Figure 3: Contiki network stack with the wake-up detection component

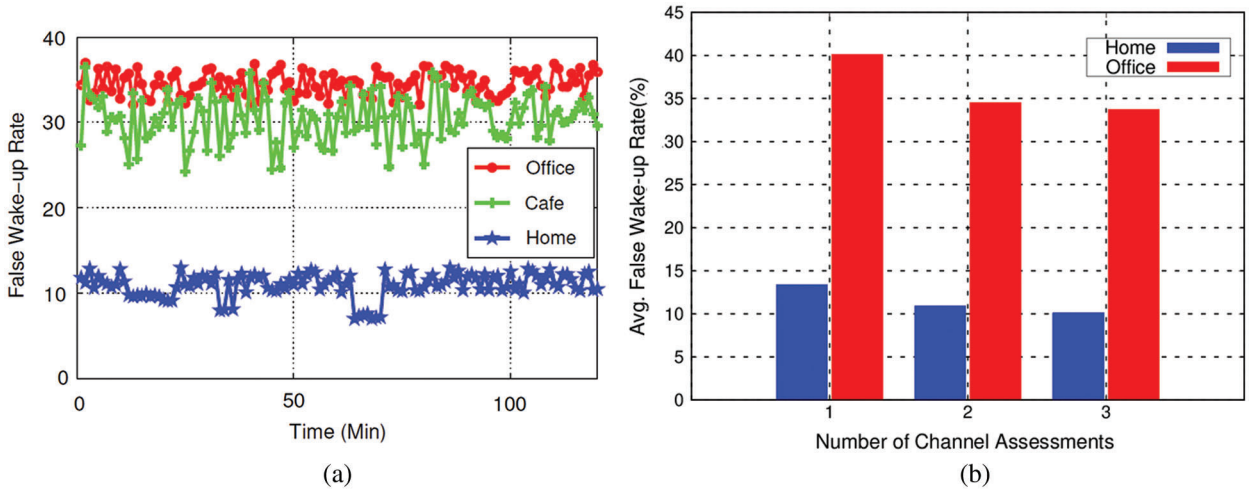

Figure 4: (a) False wake-up rate of two phase CCA (b) False wake-up rate as a function of the number of channel assessments

4 Design of Interference Resilient ZigBee Detection

4.1 Overview

Fig. 5 sketches the architecture of the CoSense mechanism. The RSSI sampler reads from the RSSI register of a ZigBee transceiver at a designated frequency. Then, the channel estimator processes a series of RSSI samples to determine whether channel is in an idle or a busy state. The signal sampler gathers

raw samples of signal and the feature detector correlates them with the pre-defined ZigBee signature to accurately check the existence of ZigBee transmissions. Combining the results from the channel estimator and the feature extractor, the radio duty-cycle controller decides whether to turn the transceiver on or off. Note that the main purpose of CoSense is to get rid of false alarms. The node wakes up only when the channel is busy and the result of the feature detector is true.

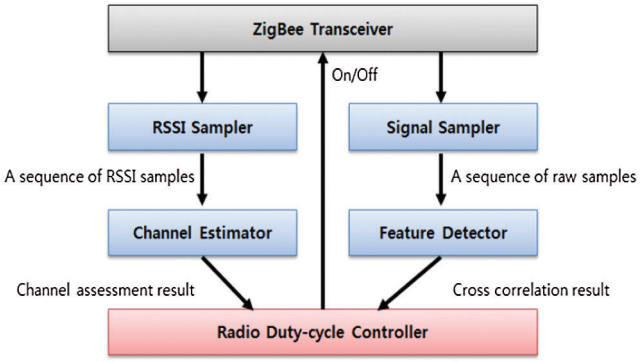

Figure 5: Radio duty-cycle control mechanism

Note that CoSense does not affect normal ZigBee transmissions and thus it is compatible with existing ZigBee networks. CoSense embeds a pre-defined signature in front of the frame preamble. If a normal ZigBee node without the CoSense function receives the signature, it regards the signature as a noise. This means that CoSense is backward compatible to the legacy ZigBee system. To effectively extract the feature of the signature, CoSense exploits the signal correlation method. The node can identify the presence of the signature by correlating the raw signal samples with the known signature pattern.

4.2 Interference Resilient ZigBee Detection

In designing CoSense, we aim to achieve following three objectives: 1) Robustness. ZigBee nodes are expected to operate in the interference-prone environments. The sources of interferences include not only the heterogeneous wireless communication technologies such as Wi-Fi and Bluetooth, but also include microwave ovens, baby monitors and so on. Some of these interference sources emit signals whose strengths are order of magnitude higher than that of ZigBee. CoSense should be robust to perform well in such a harsh environment. 2) Low power. This is of particular importance for ZigBee networks as some nodes may operate with coin sized batteries. The wireless transceiver drains much energy in the idle listening state waiting for potential transmissions. Most of previous work assumed interference free environments and ignored the false alarm problem. As shown in ZiSense, interferences can be a severe problem in realistic environments. 3) Backward compatibility. To be commercially viable, CoSense should coexist with ordinary ZigBee nodes without the functionalities of CoSense. CoSense adds 4 bytes of signature with the small overhead of header length, it does not affect the correct operation of the ordinary nodes.

Let us examine the mechanism of CoSense in a greater detail. As mentioned previously, CoSense amends CCA based detection for correct recognition of ZigBee signals. The CCA based detection scheme is vulnerable to the interference from other technologies. We equip a dual checking mechanism to make robust detections. The channel estimator is similar to that of the traditional CCA method. When the RSSI is below a certain threshold, it indicates an idle state and the channel estimator returns positive. Otherwise, the result indicates a busy state. The CC2420 radio transceiver defines the minimum time

required for a stable channel assessment as 0.128 ms. Although it can quickly discern signaling activities, it fails to identify the source of the signals.

To overcome this drawback, CoSense adds the cross-correlation method. Signal correlation is a common technique used to detect known signal patterns. CoSense equipped transmitter and receiver share the predefined Pseudo-random Noise (PN) sequence. The sender embeds a 4 bytes long signature in front of the preamble. Signal correlation of PN sequences is highly robust to imperfect radio parameter tuning and permits reliable detection even at very low SINR. Thus, the signature does not need to be preceded by a preamble.

Suppose $y[n]$ and L as the nth received symbol from sender and the length of signature, respectively. Then, the correlation value at a shift position Δ can be computed by:

$$C(\Delta) = \sum_{k=1}^{L} s^*[k]y[k+\Delta] \tag{2}$$

where $s[k]$ refers to the pre-defined signature symbols and s*[k] represents its complex conjugate. When the received signature is perfectly aligned with the beginning of s[·], the correlation value spikes very shapely. The receiver still recognizes the presence of a ZigBee signature when the correlation value is above a certain threshold. We have conducted various experiments to measure the detection performance in real environments. The false positive probability of cross-correlation is less than 0.035%, extremely low compared to energy-based assessment. We further discuss the empirical results in the Subsection 5.2.

Fig. 6 illustrates LPL operations of CoSense sender and receiver. A sender first senses the idle medium and transmits a series of data packets, each of which contains a ZigBee signature, during the entire duty-cycle interval. The sender only makes use of energy-based CCA to avoid other interferences for the first transmission attempt. A receiver periodically wakes up every duty-cycle interval and performs signal correlation to detect ZigBee transmissions by using (2). Differentiating the real signals from interferences, the node goes to the sleep state even though there exists strong interference signals. This enables the receiver to avoid false idle listening.

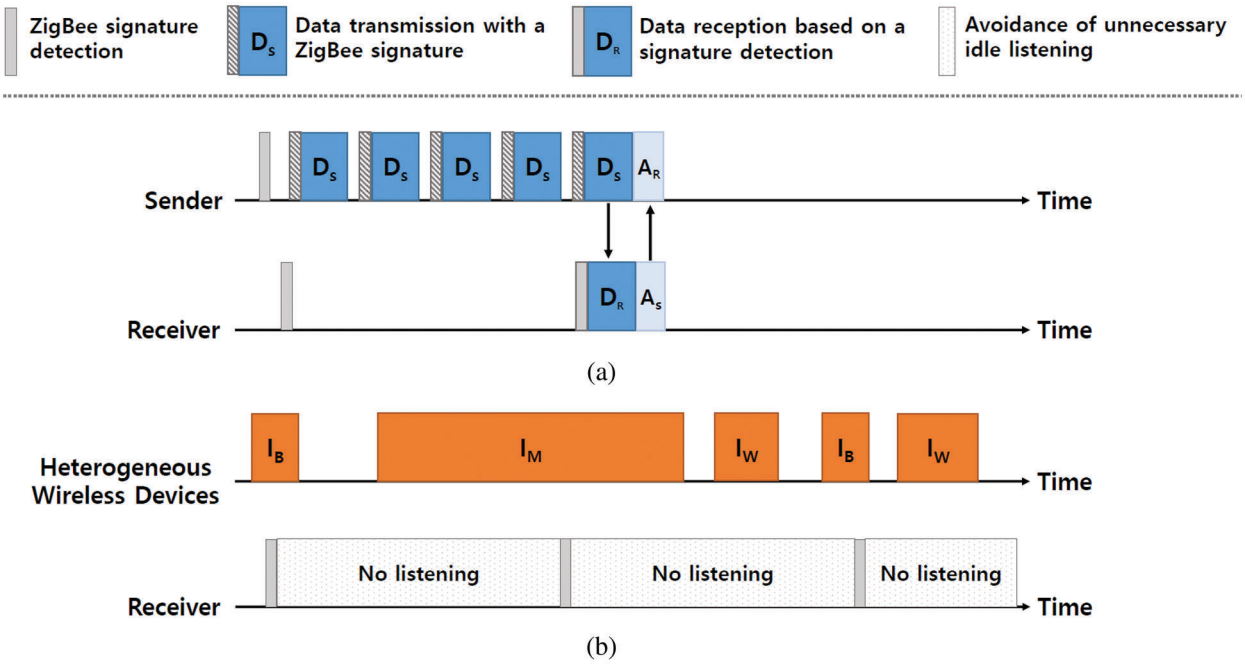

Figure 6: (a) A basic operation of ZigBee signature detection scheme (b) Avoidance of unnecessary idle listening

CoSense inserts an additional digital coding block modifying the traditional ZigBee packet format, to accommodate the ZigBee signature. Since the PN sequence is embedded in front of a preamble, a legacy ZigBee node considers it as a background noise before the preamble. Therefore, CoSense is backward compatible with legacy ZigBee nodes. Note also that the PN sequences is 4 bytes long and this causes a little overhead.

In case of receiver-initiated rendezvous mechanisms, a receiver first sends a probing packet to a potential sender. It does not occupy a large portion of a medium compared to the sender-initiated rendezvous mechanism. Suppose the probing packet is corrupted by interference. The intended sender will wait for a probing packet and suffers from considerable and unnecessary energy waste during the entire duty-cycle interval. Since decoding a probing packet is much vulnerable to interferences than the CCA method, the sender will miss transmission opportunities. This further incurs improper and continuous activation of the radio until the end of the current duty-cycle interval. A ZigBee signature preceding the preamble of a probing packet may solve this problem. Instead of decoding probing packets, CoSense robustly detects the existence of a probing packet via the ZigBee signature, which is irrelevant with detecting the probing packet for this mechanism. Of course, signal cross-correlation should be performed at the sender instead of the receiver. Our empirical results demonstrate the feasibility of identifying probing packets. With the simple modifications, CoSense can be applied to the receiver-initiated MAC protocols as well as to the sender-initiated protocols.

4.3 Discussion

To avoid the energy waste due to false wake-ups, several RSSI-based approaches have been proposed. ContikiMAC mitigates this problem with two additional features. First, it performs two consecutive CCAs to identify the air-time of 802.15.4 transmission. Second, it quickly goes to the sleep state to minimize the energy waste caused by false wake-ups. ZiSense analyzed the short-term characteristics of the time domain RSSI sequences. It proposes a rule-based identification mechanism to accurately pinpoint ZigBee transmissions under noise environments. These approaches determine their operations based on the classification of RSSI signal patterns. However, RSSI can fluctuate dynamically according to the surrounding environment features such as temperature, furniture arrangement, people movements and so on. Also, when there exist diverse wireless devices employing different standards, the shape of RSSI samples will be severely corrupted due to overlapped signals. Eventually, it causes dynamics and uncertainty in measured RSSIs and a node may fail to sense ZigBee transmissions correctly. However, the ZigBee signature detection is much simpler and more reliable than RSSI dissolution in heterogeneous network scenarios. Although other signals overlap with the ZigBee signature, an evident spike appears only when the signature exists.

5 Performance Evaluation

5.1 Experimental Set-up

We implemented the CoSense signature detection mechanism on the USRP [28] running GNU Radio [29]. We make use of the basic ZigBee PHY module [30] and add a 4 byte-ZigBee signature at the beginning of preambles. To the receiver side, we embedded the signal correlation function for raw signal samples. We also implemented the ContikiMAC to compare the performance between the basic ContikiMAC and the ContikiMAC with CoSense. We deployed one pair of CoSense nodes, three pairs of Wi-Fi clients and two pairs of Bluetooth clients to emulate a heterogeneous wireless network scenario. We performed our experiments at home environment. In the heterogeneous interference scenario, one Wi-Fi client makes use of iperf to generate 1,500 bytes UDP datagrams with a fixed 5 Mbps data rate and two other clients continuously request video streams from a web site. Two Bluetooth clients listen to

music. To explore the effect of detecting a ZigBee signature, we first measured the false wake-up rate in various scenarios. Then, we evaluated the energy efficiency of CoSense through experiments. To compute the energy consumption, we recorded the sojourn times of the transceivers active and sleep states and, then multiplied the time by the current consumption value shown in the CC2420 datasheet. Additionally, we obtained all RSSI traces and simulated the performance of the ContikiMAC with ZiSense.

5.2 Detection Accuracy

We first investigated the effectiveness of the cross-correlation mechanism in the heterogeneous network environment. One concern is the effect of signature length: Long signature increases the overhead while shorter ones may lead to misdetection of ZigBee frames. We compared two signature lengths; 4 bytes and 6 bytes. In Fig. 7(a), the false positive rates-the probability to consider interferences as ZigBee frames-are around 0.03% when signature length is 4 bytes long. A longer signature-6 bytes long signature-further decreases the false alarm rate to around 0.015%. However, 4 bytes long signatures already perform satisfactorily and we expect longer than 4 byte signatures may gain significant improvements in practice. We also analyzed the effect of signature length to the false negative rate. As shown in Fig. 7(b), the impact of signature length is very low. The false negative rate is around 0.02% regardless of signature length. We can also observe from Figs. 5(a) and 5(b) that the distance of CoSense nodes does not affect the performance of CoSense significantly. We increased the distance up to 10 meters a practical limit in home environments. We can conclude that CoSense rarely incurs false alarms or misdetection whether a ZigBee network employs the sender-initiated MAC protocol or the receiver-initiated MAC protocol.

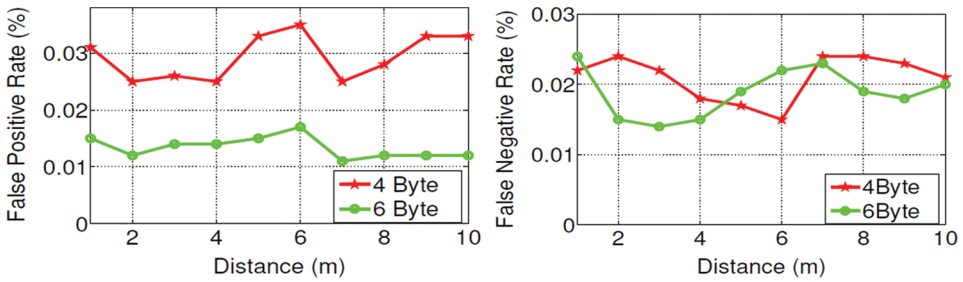

Figure 7: Error rate measurements with varying the length of signature. (a) False-positive. (b) False-negative

5.3 CoSense Performance

Fig. 8 compares the false alarm rate of CoSense with those of ContikiMAC and ZiSense. We varied the operating environments to simulate various interference scenarios. First, we set up just one Wi-Fi AP to analyze the performance under simple interference pattern. Then we add two more Wi-Fi APs and two Bluetooth nodes to simulate more complex and heterogeneous network scenarios. The vanilla ContikiMAC experiences huge false alarm rates-around 35%-in both scenarios. While the performance of the vanilla ContikiMAC is about the same in the simple network environment and the heterogeneous network environment, ZiSense is sensitive to the network configuration. The false alarm rate of ZiSense in the heterogeneous environment is almost two times higher than that in the simple environment. We guess that the complex superposition of various signals from heterogeneous network technologies damages the RSSI analysis of ZiSense. The ContikiMAC performs two-step CCA. We measured the power consumption of the ContikiMAC by using the monsoon power monitor.

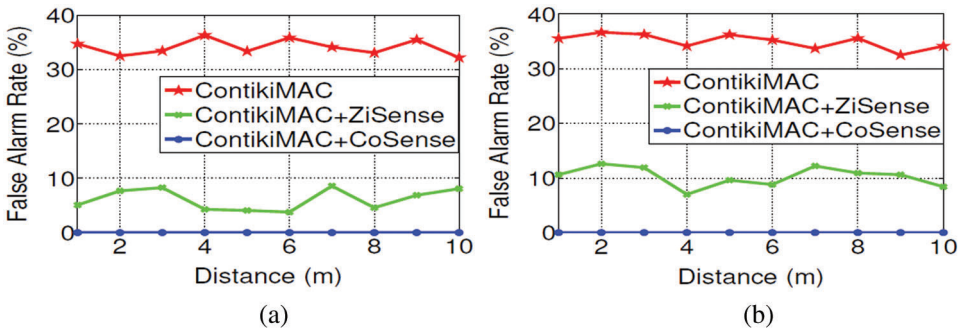

Figure 8: False alarm rate measurements: CoSense, ZiSense and Vanilla ContikiMAC. (a) False-positive. (b) False-negative

Fig. 9 shows the power consumption of normal wake-up and a false wake-up event during the first CCA stage, and the power consumption of a false wake-up during the second CCA stage. The normal operation only takes 1.6 ms. However, in the case of a false alarm, excessive power consumption lasts 7.8 ms. The overhead is not trivial considering the maximum transmission time of ZigBee is around 4.2 ms.

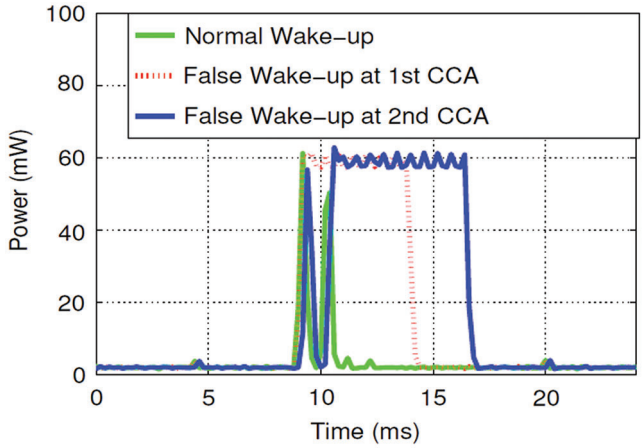

Figure 9: The power consumption of true and false wake-ups in ContikiMAC

Fig. 10 shows the energy consumption with three different duty-cycle intervals. In all cases, CoSense consumes less energy than the basic ContikiMAC and ZiSense. CoSense reduces the energy consumption by up to 63% compared to the ContikiMAC and up to 37% compared to ZiSense.

Fig. 11 shows the packet delivery ratio as a function duty-cycle intervals. In a typical ZigBee network, sensing data is periodically transmitted to the central gateway for the purpose of data analysis. To check the scenario, we periodically generate a data packet every 1 second. As the duty-cycle interval increases, several packets can be buffered in the sender side. It affects the overall packet delivery ratio. In addition, if the receiver falsely wakes up and fails to grab the packet, it also aggravates the packet delivery ratio. Due to the reduced unnecessary wake-up operations, CoSense improves the packet delivery ratio in three different duty-cycle intervals.

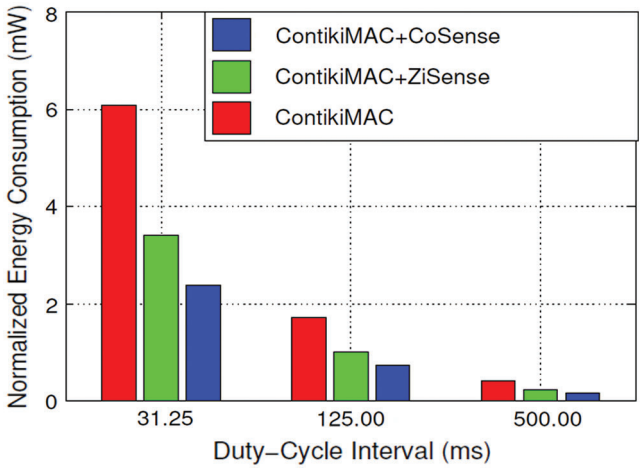

Figure 10: Normalized energy consumption measurements: CoSense, ZiSense and Vanilla ContikiMAC

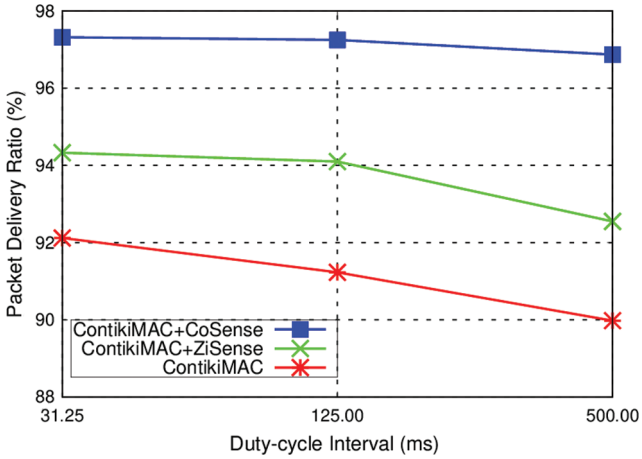

Figure 11: Packet delivery ratio: CoSense, ZiSense and Vanilla ContikiMAC

6 Conclusions

Low power lossy networks widely utilize a low power duty-cycling mechanism to identify their own traffics since the mechanism significantly minimizes energy consumptions caused by idle listening and overhearing. In particularly, it performs an energy detection scheme to simplify its channel assessment process. However, it can also incur severe CTI from heterogeneous wireless devices so that the concurrent transmissions of heterogeneous wireless devices considerably degrade the overall performance of the low power operation in the real environments. Especially, combined interferences from multiple wireless sources of different wireless technologies cause severe false wake-up problem leading unnecessary energy dissipation. We devised an intelligent ZigBee identification scheme that performs a clever signal correlation scheme and energy level-based channel assessment. We implemented our scheme on real USRP/GNURadio platform to verify various advantages of a dual checking mechanism. The results showed that the proposed scheme effectively reduces false wake-ups rate and improves the energy efficiency by up to 63% in diverse interference environments compared to the existing schemes. In addition, it can be generally adopted to the traditional ZigBee devices because of the ZigBee signature features.

Author Contributions: Sangsoon Lim: Conceptualization, Formal analysis, Writing-original draft, Writing-review & editing, Sanghyun Seo: Formal analysis, Validation, Writing-review & editing.

Acknowledgement: A preliminary version of this paper was presented at the IEEE ICC [31].

Funding Statement: This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea Government (MSIT) (No. NRF-2018R1C1B5038818).

Conflicts of Interests: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] "IEEE standard for information technology—Telecommunications and information exchange between systems local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications," *IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012)*, pp. 1–3534, 2016.

[2] S. Bluetooth, "Specification of the bluetooth system, version 4.1," 2013. [Online]. Available: http://www.bluetooth.com.

[3] "IEEE Standard for Low-Rate Wireless Networks," *IEEE Std 802.15.4-2015 (Revision of IEEE Std 802.15.4-2011)*, pp. 1–709, 2016.

[4] C. Liang, N. Priyantha, J. Liu and A. Terzis, "Surviving Wi-Fi interference in low power ZigBee networks," in *Proc. the 8th ACM Conf. on Embedded Network Sensor Systems (SenSys)*, Zurich, Switzerland, pp. 309–322, 2010.

[5] W. Ye, J. Heidemann and D. Estrin, "An energy-efficient mac protocol for wireless sensor networks," in *Proc. INFOCOM 2002. Twenty-First Annual Joint Conf. of the IEEE Computer and Communications Societies*, New York, NY, USA, pp. 1567–1576, 2002.

[6] J. Polastre, J. Hill and D. Culler, "Versatile low power media access for wireless sensor networks," in *Proc. the 2nd Int. Conf. on Embedded Networked Sensor Systems*, MD, Baltimore, USA, pp. 95–107, 2004.

[7] M. Buettner, G. V. Yee, E. Anderson and R. Han, "X-mac: a short preamble mac protocol for duty-cycled wireless sensor networks," in *Proc. the 4th Int. Conf. on Embedded Networked Sensor Systems*, Colorado, Boulder, USA, pp. 307–320, 2006.

[8] A. Dunkels, "The contikimac radio duty cycling protocol," 2011. [Online]. Available: http://soda.swedishict.se/5128/1/contikimac-report.pdf.

[9] D. Moss and P. Levis, "Box-macs: Exploiting physical and link layer boundaries in low-power networking," *Computer Systems Laboratory Stanford University*, vol. 64, no. 66, pp. 116–119, 2008.

[10] P. Dutta, S. Dawson-Haggerty, Y. Chen, C. J. M. Liang and A. Terzis, "Design and evaluation of a versatile and efficient receiver-initiated link layer for low-power wireless," in *Proc. the 8th ACM Conference on Embedded Networked Sensor Systems*, Zurich, Switzerland, pp. 1–14, 2010.

[11] Y. Sun, O. Gurewitz and D. B. Johnson, "Ri-mac: A receiver-initiated asynchronous duty cycle mac protocol for dynamic traffic loads in wireless sensor networks," in *Proc. the 6th ACM Conf. on Embedded Network Sensor Systems*, pp. 1–14, 2008.

[12] X. Zheng, Z. Cao, J. Wang, Y. He and Y. Liu, "Zisense: towards interference resilient duty cycling in wireless sensor networks," in *Proc. the 12th ACM Conf. on Embedded Network Sensor Systems*, Tennessee, Memphis, pp. 119–133, 2014.

[13] A. Hithnawi, S. Li, H. Shafagh, J. Gross and S. Duquennoy, "CrossZig: Combating cross-technology interference in low-power wireless networks," in *Proc. 15th ACM/IEEE Int. Conf. on Information Processing in Sensor Networks (IPSN)*, Vienna, pp. 1–12, 2016.

[14] G. Chen, W. Dong, Z. Zhao and T. Gu, "Towards accurate corruption estimation in ZigBee under cross-technology interference," in *Proc. IEEE 37th Int. Conf. on Distributed Computing Systems*, Atlanta, GA, pp. 425–435, 2017.

[15] S. Gollakota and D. Katabi, "Zigzag decoding: Combating hidden terminals in wireless networks," in *Proc. ACM SIGCOMM 2008 Conf. on Data Communication*, WA, Seattle, USA, pp. 159–170, 2008.

[16] S. Sen, R. R. Choudhury and S. Nelakuditi, "CSMA/CN: Carrier sense multiple access with collision notification," *IEEE/ACM Transactions on Networking (TON)*, vol. 20, no. 2, pp. 544–556, 2012.

[17] E. Magistretti, O. Gurewitz and E. W. Knightly, "802.11 ec: Collision avoidance without control messages," in *Proc. the 18th Annual Int. Conf. on Mobile Computing and Networking*, Istanbul, Turkey, pp. 65–76, 2012.

[18] P. Yang, Y. Yan, X. Li, Y. Zhang, Y. Tao *et al.,* "Taming cross-technology interference for Wi-Fi and ZigBee coexistence networks," *IEEE Transactions on Mobile Computing*, vol. 15, no. 4, pp. 1009–1021, 2015.

[19] L. Angrisani, M. Bertocco, D. Fortin and A. Sona, "Experimental study of coexistence issues between IEEE 802.11b and IEEE 802.15.4 wireless networks," *IEEE Transactions on Instrumentation and Measurement*, vol. 57, no. 8, pp. 1514–1523, 2008.

[20] I. Howitt and J. A. Gutierrez, "IEEE 802.15.4 low rate-wireless personal area network coexistence issues," *Proc. IEEE Wireless Communications and Networking*, vol. 3, pp. 1481–1486, 2003.

[21] S. Y. Shin, H. S. Park, S. Choi and W. H. Kwon, "Packet error rate analysis of ZigBee under WLAN and bluetooth interferences," *IEEE Transactions on Wireless Communications*, vol. 6, no. 8, pp. 2825–2830, 2007.

[22] H. Huo, Y. Xu, C. C. Bilen and H. Zhang, "Coexistence issues of 2.4 GHz sensor networks with other RF devices at home," in *Proc. 2009 Third Int. Conf. on Sensor Technologies and Applications*, Athens, Glyfada, pp. 200–205, 2009.

[23] S. Kim and T. He, "FreeBee: Cross-technology communication via free side-channel," in *Proc. the 21st Annual Int. Conf. on Mobile Computing and Networking (MobiCom '15)*, pp. 317–330, 2015.

[24] Z. Li and T. He, "WEBee: Physical-layer cross-technology communication via emulation," in *Proc. the 23rd Annual Int. Conf. on Mobile Computing and Networking*, Utah, Snowbird, USA, pp. 2–14, 2017.

[25] W. Jiang, Z. Yin, R. Liu, Z. Li, S. Kim *et al.,* "BlueBee: A 10,000x faster cross-technology communication via PHY emulation," in *Proc. the 15th ACM Conference on Embedded Network Sensor Systems*, Delft, Netherlands, pp. 1–13, 2017.

[26] T. Instruments, "Cc2420 datasheet," Reference SWRS041B, 2007.

[27] P. Levis, S. Madden, J. Polastre, R. Szewczyk, K. Whitehouse *et al.,* "Tinyos: An operating system for sensor networks, " in *Ambient Intelligence*. Berlin, Heidelberg: Springer, pp. 115–148, 2005.

[28] M. Ettus, "Ettus research, llc-Online information on USRP board," 2008. [Online]. Available: http://www.ettus.com.

[29] E. Blossom, "Gnu radio: Tools for exploring the radio frequency spectrum," *Linux Journal*, vol. 2004, no. 122, pp. 4, 2004.

[30] L. Choong, "Multi-channel ieee 802.15. 4 packet capture using software defined radio," *UCLA Networked Embedded Sensing Lab*, vol. 3, pp. 1–20, 2009.

[31] S. Lim, D. Ban, W. Park and C. Kim, "CoSense: Interference resilient ZigBee detection in heterogeneous wireless networks," in *Proc. IEEE Int. Conf. on Communications (ICC)*, Kuala Lumpur, pp. 1–6, 2016.