공학박사 학위논문

Protecting Narrow Band Systems in Heterogeneous Wireless Networks

이기종 무선 네트워크에서의 협대역 시스템 보호 기법

2013년 8월

서울대학교 대학원

전기·컴퓨터 공학부

임 상 순

Protecting Narrow Band Systems in Heterogeneous Wireless Networks

이기종 무선 네트워크에서의 협대역 시스템 보호 기법

指導敎授 金鍾權

이 論文을 工學博士 學位論文으로 提出함

2013년 8월

서울大學校 大學院
전기·컴퓨터 工學部
林 尙 諄

林尙諄의 工學博士 學位論文을 認准함
2013년 8월

위 원 장 최 양 희 (인)
부위원장 김 종 권 (인)
위 원 권 태 경 (인)
위 원 김 종 덕 (인)
위 원 최 재 혁 (인)

Abstract

Protecting Narrow Band Systems in Heterogeneous Wireless Networks

Sangsoon Lim
School of Electrical Engineering and Computer Science
The Graduate School
Seoul National University

Recent deployment of various wireless technologies such as Wi-Fi, Bluetooth, and ZigBee in the 2.4GHz ISM band has led to the heterogeneous devices coexistence problem. The coexistence problem is particularly challenging since wireless technologies use different PHY/MAC specifications. This thesis deals with the ZigBee and Wi-Fi coexistence problem where a less capable ZigBee device may often experience unacceptably low throughput due to the interference from a powerful Wi-Fi device.

We propose a novel time reservation scheme called Narrow Band Protection (NBP) that uses a protector to guard ongoing ZigBee transmissions. The NBP protector detects a ZigBee transmission by cross-correlating the ZigBee signals with pre-defined Pseudo-random Noise (PN) sequences. A cross-correlation, designed for apprehending certain patterns in signals, not only reduces the control overhead but also guarantees robustness against collisions. In addition, a ZigBee node can still encode its packet length as a PN sequence such that the protector guards a proper length of channel time. We show the feasibility of NBP by implementing it on the USRP/GNURadio platform. We also evaluate the performance of NBP through mathematical analysis and NS-2 simulations. The results show that NBP enhances the ZigBee throughput by up to 1.77x compared to an existing scheme.

Keywords: Coexistence, Interference Mitigation, Signal Correlation, Time Reservation, ZigBee, Wi-Fi, Heterogeneous Wireless Networks

Student Number: 2007-30838

Contents

List of Figures

List of Tables

1. Introduction

1.1 Background

The unlicensed 2.4GHz ISM band has become a common playground for a plethora of wireless technologies such as Wi-Fi [1], Bluetooth, ZigBee [2], Radio-Frequency Identification (RFID) and so on. When multiple wireless technologies that run their own protocols coexist in the same channel, they usually cannot detect each other. This happens because they use different PHY/MAC specifications. As a result, a device to freely transmits even when a device of heterogeneous technology is transmitting, thus causing severe interference to each other. This is called as the *cross-technology interference problem* [3-7].

The cross-technology interference creates particularly unfavorable environments for less-capable technologies, i.e., low priority networks. Low priority networks are often equipped with less powerful hardware than high priority networks. Also low priority networks are designed to operate in small areas and their transmission ranges are much shorter than those of high priority networks. Let us examine the cross-technology interference problem in a greater detail with an example of two most popular networks; ZigBee - a low priority network and Wi-Fi - a high priority network. ZigBee devices, that coexist with Wi-Fi stations, occasionally cannot send any packets due to their significantly disadvantageous medium access control (MAC) layer protocol timings [8–10]. ZigBee takes 192 μs to switch between Radio Frequency (RF) modes (i.e., RX-TX or TX-RX), while Wi-Fi can finish its backoff in only 72 μs. As a consequence, Wi-Fi stations can preempt a ZigBee node even if the ZigBee node first grabs the medium.

The interference relation between ZigBee and Wi-Fi can be either symmetric or asymmetric [11]. In the symmetric interference case, ZigBee node and Wi-Fi node are proximate each other such that a Wi-Fi station can sense weak ZigBee transmission. The Wi-Fi station therefore does not interfere ongoing ZigBee transmission. However, it still can starve the ZigBee node because of the MAC timing differences as explained before. The cross-technology interference problem becomes even more critical in the asymmetric case where the Wi-Fi node, unwitting of ZigBee existence can interfere ZigBee transmission at any time. In this case, the ZigBee nodes often experience significant throughput degradation due to the interference from Wi-Fi nodes, even when the traffic intensity of Wi-Fi networks is moderate [8, 9, 12, 13].

Recently, many researchers have delved into the cross-technology interference problem and several clever schemes have been proposed. The approaches to solve the coexistence problem are categorized into three groups. First, an intuitive approach to avoid such interference is to assign the preferable channels that are less affected by the Wi-Fi transmission to ZigBee nodes [14–16]. However, such a solution is often infeasible as the shared spectrum band may already have been heavily loaded with many heterogeneous wireless devices. Secondly, ZigBee frame control mechanisms [8, 17] either adjust the ZigBee frame size or the inter-packet arrival time between ZigBee packets so that ZigBee packets opportunistically fit into the intervals of the Wi-Fi packets. However, these adjustments cannot guarantee the delivery of ZigBee packets and hence are inapplicable for delay-sensitive ZigBee applications. The third approach is to use a dedicated entity to protect ZigBee devices [18]. The dedicated entity, called protector, reserves the wireless medium on behalf of ZigBee devices. This scheme requires significant changes in ZigBee protocol because a ZigBee node needs to explicitly notify the protector that it has a packet to send. More importantly, the notification itself is vulnerable to the Wi-Fi interference degrading the performance and reliability of the scheme.

1.2 Goal and Contribution

In this thesis, we propose a novel time reservation scheme, called Narrow Band Protection (NBP) for the coexistence of Wi-Fi and ZigBee networks. NBP reduces the control overhead for the ZigBee channel reservation through a self-sensing mechanism. A NBP protector autonomously detects an ongoing ZigBee transmission without explicit notification. Detecting the ZigBee transmission, it immediately reserves the channel until the transmission is completed. Also, the autonomous signal detection and protection are not affected by the control packet collisions. To enhance the detection fidelity of low power ZigBee signals, we employ the reliable cross-correlation technique [19-21]. In addition, NBP can protect multiple continuous ZigBee packets by estimating the size of the burst. This is important because a ZigBee node is typically battery-powered and thus prefers low duty cycle operations [30–32].

We implement NBP on the USRP/GNURadio platform to show the feasibility of our proposal. We then demonstrate the performance of NBP via mathematical analysis and NS-2 simulations. The results show that our scheme enhances the throughput of ZigBee networks by up to 1.77x compared to that of the existing time reservation scheme. Performance gain is increased linearly by the number of multiple packets in a burst.

Our main contributions are summarized as follows.

- We characterize the collision problem of the state-of-the-art ZigBee protector. The problem significantly aggravates the performance gain of channel reservation.
- We propose NBP, a low overhead channel reservation scheme for a low priority network. NBP addresses the collision problem by autonomous detection based on signal correlation. Furthermore, the autonomous behavior enables backward compatibility.
- We devise a reliable burst length estimation method using a Pseudo-random Noise (PN) codebook. With this method, NBP gives advantage to the low duty-cycled ZigBee networks.
- We implemented NBP on the USRP/GNURadio platform as well as the NS-2 simulator. This shows the feasibility and practicality of NBP in real environments.

1.3 Thesis Organization

The rest of this thesis is organized as follows. Section 2 reviews the related work. We then give our motivation in Section 3. Section 4 describes the design of NBP in detail. We present the mathematical analysis in section 5 and Section 6 evaluates the performance of NBP via USRP experiments and NS-2 simulations. Finally, Section 7 concludes the thesis.

2. Related Work

2.1 The Cross-technology Interference Problem

The cross-technology interference is a common problem in the real-world ISM unlicensed band [8, 9, 11-13]. In [8], Angrisani *et al.* observed the mutual-interference between ZigBee and 802.11b in a real environment. The results show that ZigBee networks experience a packet loss rate from 0% to 85% under varying Wi-Fi traffic load. The authors in [11] investigated the interference patterns at the bit-level granularity. In particular, bit errors occur at the front part of a ZigBee packet in symmetric interference scenarios, while they are almost uniform throughout the entire packet in asymmetric interference scenarios. We analyze the throughput separately for both cases to account for the aforementioned observations. There have been some similar analytic work to study the cross-technology interference [44–47]. However, our work considers the effect of the low power packet bursting mechanism. Furthermore, it is implemented on a real testbed to show that it works practicality in a real environment.

2.2 The Cross-technology Interference Solutions

2.2.1 Channel Hopping

Pollin *et al.* [15] tried to find an optimal interference-free channel by using

Simulated Annealing and a Nash Q-learning method. The authors in [16], devised EM-MAC that avoids heavily loaded, interference, and jamming channels. It collects the channel information by overhearing regular TX-RX operations (e.g., CCA and collision results), thus does not incur any overhead to manage the channel. However, this work does not solve the fundamental challenge of the ISM band becoming much crowed. In other words, the ISM band may not provide the sufficient number of interference-free channels. Moreover, after discovering the proper channel, it may take additional overhead to maintain the multi-channel rendezvous. In contrast, our proposal does not try to avoid the interference from other devices but rather seeks a spectrum opportunity in the same channel.

2.2.2 ZigBee Packet Re-shaping

Huang *et al.* [17] measured and studied the Wi-Fi networks and found the behavioral features of the Wi-Fi traffic. They developed a ZigBee frame shaping protocol that adaptively adjusts the packet size to opportunistically fit into empty space between Wi-Fi transmissions. The authors in [8] proposed a ZigBee network having a larger inter-packet arrival time to make its retransmission more reliable. Specifically, a ZigBee node predicts the Wi-Fi transmission and controls its retransmission so that it is not corrupted by the ongoing strong Wi-Fi interference. Although these solutions provide a way for ZigBee to compete with the high priority network, they still do not guarantee fair access to a low priority network owing to the inherent PHY/MAC protocol differences.

2.2.3 ZigBee Communication Protector

A particular signaling mechanism can reserve the competing channel for a low priority network [18, 48]. Hou *et al.* [48] utilized a dual-radio system equipped with both ZigBee and Wi-Fi transceivers. Before transmitting a ZigBee packet, the hybrid device exchanges 802.11 RTS/CTS packets to prevent nearby Wi-Fi networks from sending traffic. The authors in [18] proposed a cooperative busy tone mechanism that not only transmits ZigBee data packets but also concurrently reserves the channel through the frequency flip. These proposals, however, require to send additional negotiation messages for the channel reservation. These ZigBee messages may also be corrupted by Wi-Fi transmissions, in effect, silencing both networks. Unlike previous protectors, a self-sensing mechanism of NBP correctly determines when to preempt the Wi-Fi transmissions and does not require any specific coordination.

2.3 Signal Correlation

Signal correlation is a common technique widely employed for wireless receivers to detect known signal patterns. ZigZag decoding [20] and CSMA/CN [21] use cross correlation to effectively detect packet collision. 802.11ec [22] mechanism uses the cross-correlation technique to reserve the channel and replace the legacy RTS/CTS. Our proposal also employs signal correlation for the NBP protector to detect the packets sent from ZigBee nodes. However, NBP differs from the other schemes since (i) the main objective of NBP is to protect ZigBee nodes from stronger Wi-Fi nodes, while other schemes are mainly for 802.11 collision detection [20, 21] or 802.11 protocol efficiency [22], and (ii) NBP uses distinctive methods explained in the following sections.

3. Motivation

3.1 Overview of ZigBee and Wi-Fi

This thesis mainly focuses on the coexistence problem of ZigBee (defined in IEEE 802.15.4 standard [2]) and Wi-Fi. Note that our work can be generally applied to the coexistence of other standards without much modification. Both ZigBee and Wi-Fi use the same 2.4GHz ISM band. The ZigBee standard defines sixteen channels within the spectrum band - each channel is 2MHz wide and has a 3MHz guard band between them. Each Wi-Fi channel occupies 22MHz (including the guard band) and may overlap with up to four ZigBee channels as depicted in Fig. 3.1.

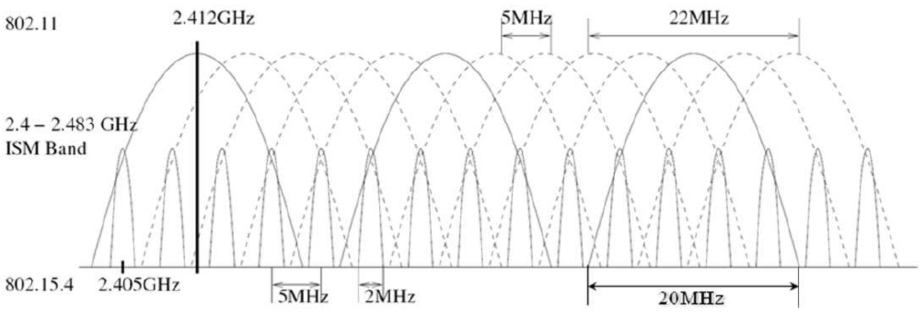


Figure 3.1: IEEE 802.15.4 and IEEE 802.11 channels

3.2 Collision between ZigBee and Wi-Fi packets

A single ZigBee transmission occupies only a portion of the Wi-Fi frequency channel bandwidth (1/4) and its TX power is very low compared to the Wi-Fi transmissions (1/10 ~ 1/100). Therefore, in most cases, the Wi-Fi device cannot effectively detect the ZigBee transmissions, while the ZigBee device can detect the Wi-Fi opponent. So, the Wi-Fi device will not defer its transmission even in the presence of ZigBee traffic. This behavior has shown to make the ZigBee network starve in many recent measurement studies [8, 11].

Even if the Wi-Fi device indeed senses the ZigBee's signals, collisions may occur. According to the 802.15.4 standard, the ZigBee slot time, Clear Channel Assessment(CCA) time, and RX-TX (or CCA-TX) turn-around time are 320 μs, 128 μs, and 192 μs [2] respectively. In contrast, the slot time (9 μs) and CCA time (28 μs) of Wi-Fi are much shorter. This implies that Wi-Fi may even complete its backoff and CCA within the RX-TX switching time of a ZigBee transceiver (Fig. 3.2). As a result, when a ZigBee node finishes its CCA and is ready to transmit a packet, in turn switches from CCA to Tx, a Wi-Fi node can quickly come in-between and finish its backoff and start transmitting a packet. These packets can collide.

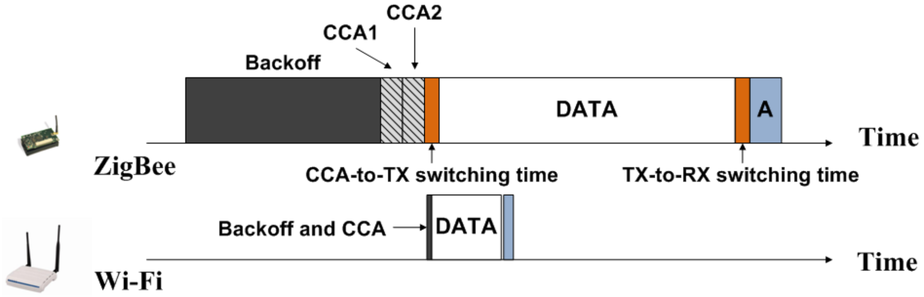


Figure 3.2: Basic operations of ZigBee and Wi-Fi

There have been many proposals that deal with this problem [15, 17, 18], but among them the dedicated high-power protector scheme [18] for ZigBee provides a preferable solution. The main reason of ZigBee's starvation is its relatively low TX power and slow PHY/MAC operations. So, the key idea of [18] is to improve the visibility of ZigBee signals by hiring a protector equipped with a more powerful hardware [49]. Fig. 3.3 illustrates the operation of the Cooperative Busy Tone (CBT) protector [18]. It protects the ZigBee transmissions using the following steps:

Step 1. A protector conducts a medium access process on behalf of ZigBee nodes.

Step 2. When the protector senses an idle medium, it notifies the ZigBee nodes by sending a channel-grant message (e.g., CTS in [18]).

Step 3. Once the ZigBee nodes receive this message, they contend to grab the reserved channel.

Step 4. The protector switches to the adjacent channel and emits a reservation signal, which prevents Wi-Fi from transmitting a packet.

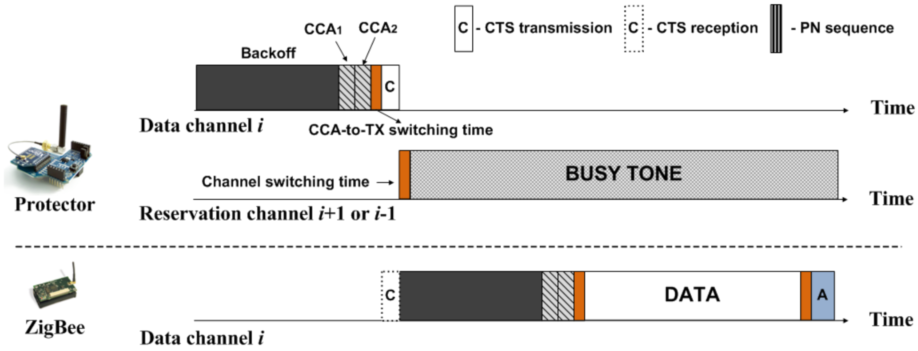


Figure 3.3: The basic operation of the CBT protector

3.3 The Limitation of the Protector Approach

The protector approach has the following limitations. In [18], the protector collects the ZigBee network traffic information by periodic reports from the ZigBee coordinator. Since the reports are transmitted by the low TX power ZigBee, they may suffer from the Wi-Fi interference. In addition, the channel-grant message sent by the protector can collide. In the latter case, the protector still sends a reservation signal in the adjacent channel, since it is unaware of the notification failure. This is particularly harmful because it wastes the channel time for both ZigBee and Wi-Fi transmissions.

Meanwhile, the busy-tone, sent by the protector, should cover the entire duration of a single ZigBee packet transmission, i.e., from the start of backoff to the ACK reception. However, since the protector does not know the exact transmission length, it conservatively sends the reservation signal for the maximum transmission duration. This takes about 7.2 ms, including data, ack and the maximum backoff duration of first backoff stage, and it wastes channel time for both ZigBee and Wi-Fi networks.

Furthermore, the ZigBee uses low duty-cycling [33-37], meaning that it is usually asleep and only periodically wakes up. In consequence, it is advantageous to send as many packets as possible, generally in bursts, when it wakes up. This burst transmission achieves both high throughput and low power consumption [30–32]. Accordingly, the protector should know how many packets a ZigBee node will transmit in order to protect the ZigBee transmission for the appropriate amount of time. It may either predict the ZigBee's traffic demand or explicitly be informed by a ZigBee node. Note that the latter may also be susceptible to interference and collision.

4. A Narrow Band Protection Technique

4.1 Overview

Fig. 4.1 shows the main operation of NBP. It protects ZigBee transmissions using the following procedure:

Step 1. A ZigBee node senses the idle medium and transmits a packet(s).[1]

Step 2. The NBP protector autonomously detects a ZigBee packet by cross correlating it with the pre-defined Pseudo-random Noise (PN) sequences. This enables the protector to detect the ZigBee transmission and estimate the transmission length.

Step 3. The protector switches to the adjacent channel and emits a reservation signal for the estimated duration, which prevents Wi-Fi nodes from transmitting a packet.

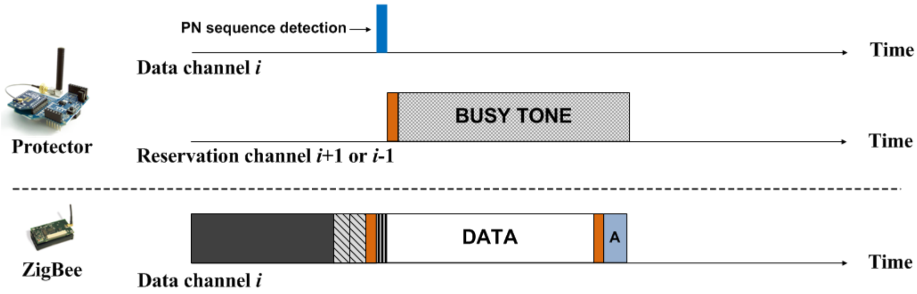


Figure 4.1: The basic operation of the NBP protector

[1] This is different from the previous scheme [18] where the protector senses the medium on behalf of the ZigBee node.

Note that NBP does not require any explicit message exchange between the protector and ZigBee nodes. Also, the ZigBee node completes its backoff before the protector sends the reservation signal. It means that the Wi-Fi devices can transmit during the lengthy ZigBee backoff duration, since NBP does not jam them. We will further discuss why and how much this change enhances both Wi-Fi and ZigBee performance via mathematical analysis in section 5.

When ZigBee and Wi-Fi channels overlap, the protector have to decide the reservation channel between i-1 and i+1 (i is data channel). If a ZigBee node uses channel 11, 12, and 13, the reservation channel i+1 covers interfering Wi-Fi channels. In a case of channel 24, 25, and 26, the reservation channel i-1 affects to interfering Wi-Fi channels. However, when a ZigBee channel suffers from the Wi-Fi interference at the edge of a Wi-Fi channel, the protector carefully selects the effective reservation channel. The protector first emits reservation signal on the reservation channel i-1. If the interference is not alleviated, it hops to reservation channel i+1 for the appropriate reservation.

4.2 Cross-correlation with PN Codebook

NBP exploits the cross-correlation method [20,21] to detect the ZigBee transmission. A PN codebook consists of *m* PN sequences. The NBP protector correlates one of the known PN sequences with the received signal. The signal correlation is a popular technique in wireless receivers for detecting known signal patterns. Say that the known PN sequences have *L* samples. The protector aligns these *L* samples with the first *L* received samples, computes the correlation, shifts the alignment by one sample and then re-computes the correlation. The PN sequence is independent of the shifted versions of itself, the other PN sequences in the codebook, and also the data packets. Hence the correlation is near zero except when a PN sequence is perfectly aligned with the beginning of the same PN sequence.

Mathematically, the correlation is computed as follows. Let *y[n]* be the n^{th} received symbol. Let the samples *s[k]*, $1 \le k \le L$, refer to the pre-defined PN sequence, and *s*[k]* represents the complex conjugate. The correlation, C(Δ), at a shifted position Δ is:

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

When the received signature is perfectly aligned with the beginning of *s*, the correlation value spikes, even when a non-negligible amount of (Wi-Fi) interference is given. The protector can easily detect a PN sequence by comparing the amplitude of a correlation value against the pre-set threshold, without demodulating an exact symbol. We have evaluated the correlation performance in terms of accuracy in our implementation. Under various received SNRs, the detection error of cross-correlation is less than 0.05% (see subsection 6.1).

The cross-correlation between the received ZigBee signal and the PN codebook allows a protector to acquire information about not only the presence of a ZigBee transmission but also its duration. The length of a PN sequence is *2L* bits and thus there can be 2^{2L} different PN sequences in the PN codebook. Among them, we choose *m* PN sequences that have the property of low cross-correlation (correlation between one another) and auto-correlation (correlation between one and its shifted version). NBP also uses this PN codebook to support burst ZigBee packets. Specifically, when a protector receives the i^{th} ($1 \leq i \leq m$) PN sequence, it will know that the ZigBee node will transmit *i* consecutive packets. Assuming the NBP protector and ZigBee nodes share the same PN codebook, the protector continuously attempts to cross-correlate the received signal with the PN sequences in its own codebook. If there is a ZigBee transmission, eventually the correlation value will spike at the i^{th} sequence. This enables NBP to determine the exact duration of a reservation signal. It is worthwhile noting that the protector does not emit excessive jamming signals that may degrade the Wi-Fi performance.

When a ZigBee node has *i* packets to transmit it embeds the i^{th} PN sequence, among *m* PN sequences in the PN codebook, at the head of the first packet. The signal correlation of PN sequences is highly robust to the interference and/or distortions and hence works well even at low SNR [21]. Therefore, a PN sequence does not require to be preceded by a preamble transmission [22].

One may argue that NBP may require modifying the current ZigBee packet format. On the contrary, it can be implemented by adding a very light-weight digital coding block (hard wired). We show the real implementation of NBP in subsection 6.1. Moreover, it does not affect the reception of a legacy ZigBee node. Since the PN sequence is added at the head of a preamble, it will not be decoded but considered as a noise. This makes NBP backward compatible to the legacy ZigBee nodes. Note also that the PN sequence length is short (4bytes - a typical ZigBee packet is about 100 bytes) and hence incurs little overhead in practice.

4.3 Protection Coverage

Protection coverage is one of the most important factors to decide protector configuration. As the coverage increases, the number of required protectors decreases, so that the protector can be deployed efficiently. Fig 4.2 illustrates the protection coverage of both schemes. In a case of CBT, the dedicated protector guards ZigBee nodes within ZigBee transmission range. Negotiation messages among the protector and the ZigBee nodes must be delivered to initiate protection mechanism. Thus message exchange limits the protector coverage to ZigBee transmission range. In contrast, a NBP protector has large coverage compared to the CBT protector. In a case of NBP, the signal correlation is robust from the interference and the noise, so that the NBP protector detects protection request information embedded in the PN sequences beyond ZigBee transmission range.

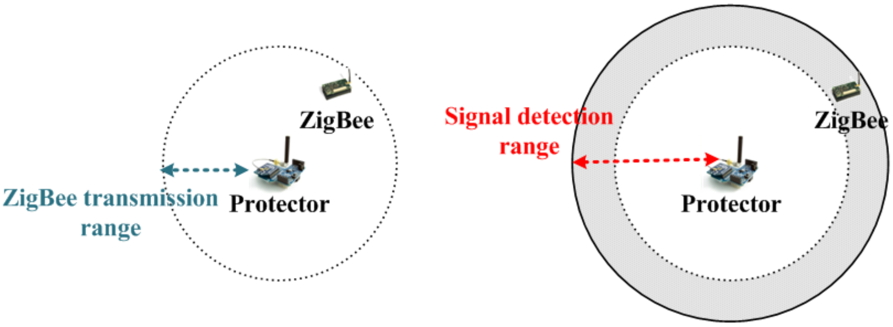


Figure 4.2: Protection coverage of (a) CBT and (b) NBP

We have evaluated the protection coverage of both CBT and NBP. To compare the detection rate of protection request, we have measured the Request Detection Rate (RDR) through TelosB [64]/TinyOS [65] and USRP [51]/GNURadio [52] platforms as shown in Fig. 4.3.

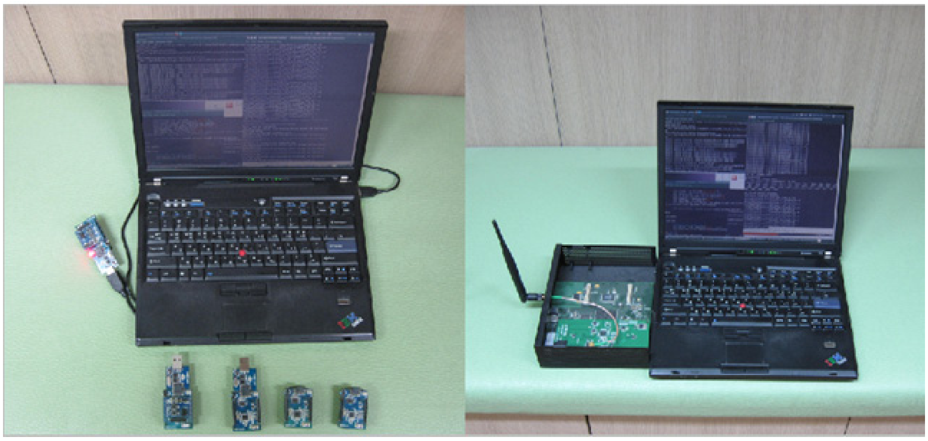


Figure 4.3: TelosB and USRP platforms

TelosB sensor node consists of a MSP430 Micro Control Unit(MCU) [66] and a CC2420 radio chipset. The CC2420 chipset is an 802.15.4 compliant device which operates in the 2.4GHz ISM band with a data rate of 250kbps.

GNURadio [52] is an open-source software development toolkit that allows to implement software radios via signal processing blocks. The main goal of GNU Radio is to create software-defined radios with a low-cost external RF hardware. GNU Radio provides useful signal processing primitives and a simple interface to the signal processing blocks from Python. Thus it can run at fast speed without any interpretation.

The USRP [51] is a low-cost and flexible platform to design software defined radios. It consists of an Altera Cyclone FPGA, 64 MS/s dual ADC, 128 MS/s dual DAC and USB 2.0 connectivity to provide data to host processors.

Fig. 4.4 shows the measured RDRs of both CBT and NBP protector. As Received Signal Strength Indicator (RSSI) decreases, decoding rate in CBT is also decreased significantly. However, under various RSSIs, the detection error of NBP is much smaller than the decoding error of CBT. The IEEE 802.15.4 standard specifies receiver sensitivity to -85dBm. While considering the receiver sensitivity, NBP achieves higher detection accuracy at very low RSSI. Thus NBP enhances the protection coverage at least 11 dB compared with CBT.

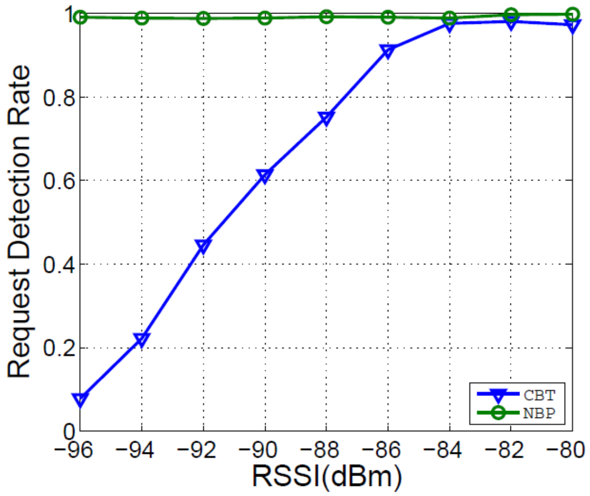


Figure 4.4: Request detection rate vs. RSSI

4.4 Protecting Wireless Sensor Networks

4.4.1 Energy Efficient Schemes in MAC Layer

In Wireless Sensor Networks (WSNs), energy efficiency is one of the most important performance criteria since WSNs consist of numerous battery-powered sensor devices. Especially, idle listening (i.e., listening for potential packets) and overhearing (i.e., receiving a packet destined for other nodes) problems are two main sources of energy consumption at the MAC layer [42].

To tackle these problems, novel and diverse schemes [33][34][35][36][37][38][39][40][41][43] have been proposed. These solutions adopt a duty-cycling mechanism which alternates periodically between sleep state and active state. Duty-cycling approaches are divided into the following two categories according to whether the sensor nodes in the same network are synchronized or not; (i) Scheduled Listening (SL) [33][34][35][41] and (ii) Low Power Listening (LPL) [36][37][38][39][40][43].

The SL approaches periodically broadcast a control packet specifying the asleep/awake period for all sensor nodes, and thereby maintain all nodes to be synchronized. Thus, it can reduce idle listening by turning off its radio during the asleep period. Since the synchronization among all nodes in a network is not a trivial work, the SL approaches fit well in small-sized WSNs in general.

In contrast, the LPL schemes do not require any time synchronization among sensor nodes and can be widely utilized in both large and small sized networks. The LPL approaches minimize idle listening by devising a preamble-based asynchronous rendezvous between a sender and a receiver. We can further divide the LPL schemes into two groups; (i) basic LPL [40] and (ii) ACK-based LPL [39].

As shown in the Fig. 4.5, the basic LPL scheme transmits a long preamble to wake up its one hop neighbors, obliterating tight time synchronizations among sensor nodes. However, the excessive preamble of basic LPL brings out an overhearing problem.

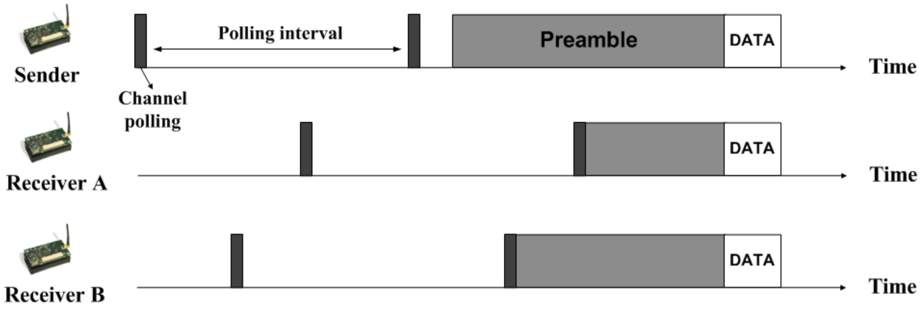


Figure 4.5: The operation of the basic LPL

To remedy this overhearing problem, the ACK-based LPL schemes (ACK-LPL) are proposed. Fig 4.6 shows the basic operation of the ACK-LPL. The ACK-LPL employs strobe (short) preambles and an early ACK. Each short preamble conveys a destination address. After sensing and decoding an ongoing short preamble, only an intended receiver among neighbors immediately replies via an early ACK. Briefly, the strobe preamble eliminates overhearing and the early ACK reduces per-hop latency significantly.

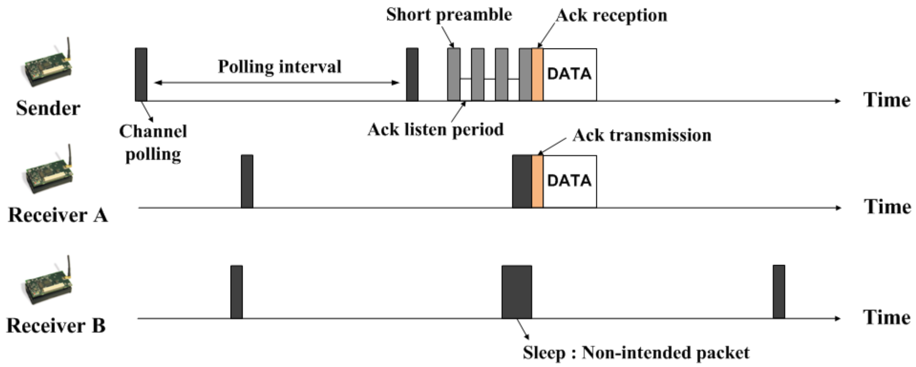


Figure 4.6: The operation of the ACK-LPL

4.4.2 Energy Efficient Schemes with NBP

In this section, we discuss about LPL schemes with NBP. In order to protect WSNs that employ the basic LPL, we divide a long preamble into multiple short preambles. After that, we embed the burst length information at the last preamble segment. As shown in the Fig. 4.7, the NBP protector can efficiently reserve the channel except long preamble period. This operation reduces the Wi-Fi throughput degradation in the asymmetric interference region.

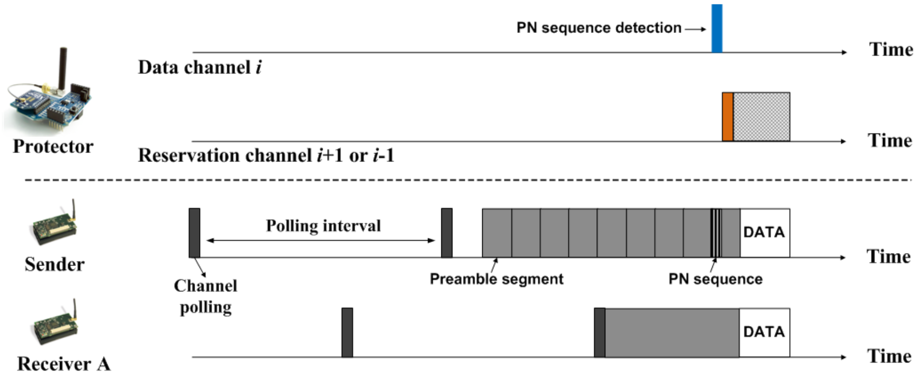


Figure 4.7: The basic LPL with NBP

In a case of the ACK-LPL, we modify the early ack to convey the burst length information. As shown in the Fig. 4.8, the NBP protector does not consider unnecessary short preamble to avoid meaningless interference. It also enhances the coexistence efficiency in the asymmetric interference region.

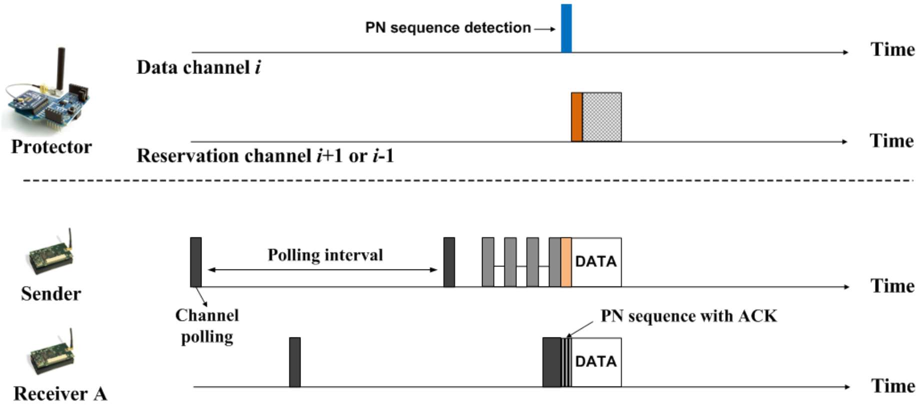


Figure 4.8: The ACK-LPL with NBP

4.5 Security Issues

In this section, we discuss malicious ZigBee nodes and protectors. Wilful channel reservations from malicious nodes significantly affect Wi-Fi performance degradation. In order to detect malicious nodes, we adopt well-known wireless intrusion detection schemes [78][79][80][81][82] and propose simple yet effective prevention schemes.

4.5.1 Signal Strength Measurement

Xu et al. [79][80] show that the average received signal power is not a valuable metric when detecting jamming scenarios. A threshold decision is not trivial. To overcome the drawback, Xu et al. proposed spectral discrimination techniques. The approach was useful to detect the constant and the deceptive jammers.

4.5.2 Carrier Sensing Time

In wireless networks, carrier sensing is a popular technique to check the channel states (busy or idle). Various wireless networks have their own distributions of the carrier sensing time [79][80]. Monitoring the distributions of the carrier sensing time can discriminate between malicious behaviors of the jammers and normal network conditions. The approach also discerned the constant and the deceptive jammer.

4.5.3 Packet Delivery Ratio Measurement

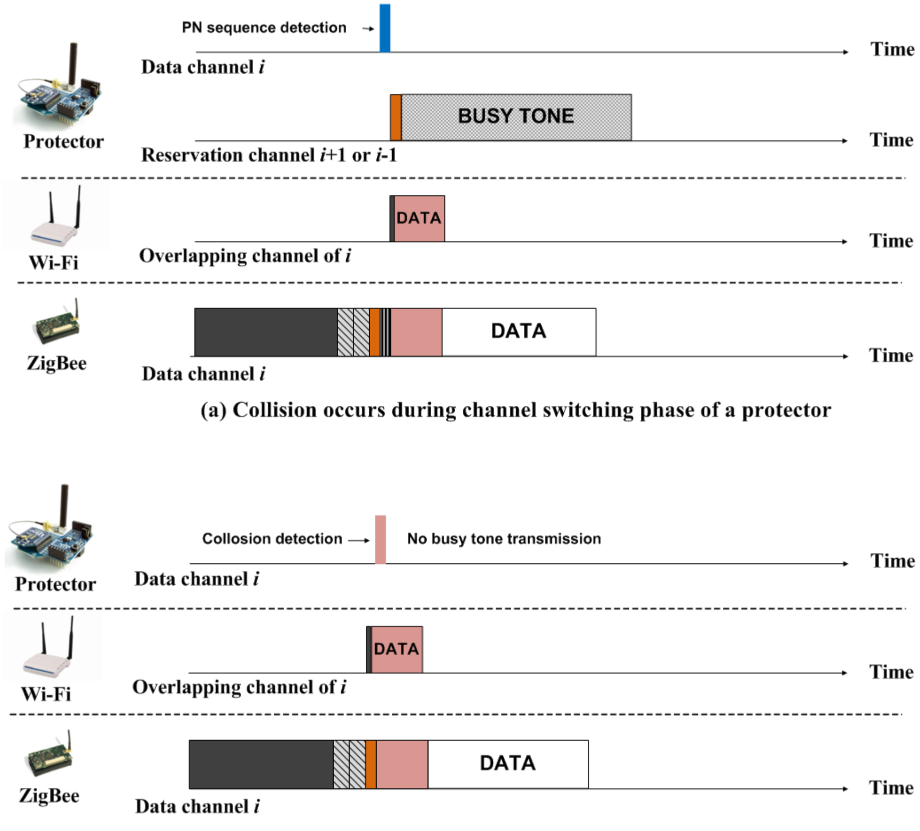
Measuring Packet Delivery Ratio (PDR) [79][80] is also a useful metric to detect diverse PHY layer jammers. A jamming attack causes severe packet collisions, thus significantly decreasing the PDR. Observing the difference of the PDR can easily distinguish between a congested network and a jammed network through dynamic thresholds.

4.5.4 Prevention Schemes

Based on these detection schemes, ZigBee nodes check signal strength, carrier sensing time and packet delivery ratio to detect ZigBee jammer. When detecting the malicious ZigBee node, they notify the jammer to ZigBee protector. Then, the protector denies the busy-tone request of the ZigBee jammer. In addition, Wi-Fi nodes observe the protector's jamming behavior periodically. If the Wi-Fi AP detects jamming pattern, jammed AP first adjusts its transmission power to capture the jamming attack. If the jammed AP cannot overcome jamming attack, it finally hops to orthogonal channel.

4.6 Discussions

A collision can still occur when the NBP protector is used to protect the ZigBee transmission. In Fig. 4.9, we depict two scenarios where a ZigBee transmission collides with a Wi-Fi transmission. We next describe how NBP deals with these two types of collisions.



(a) Collision occurs during channel switching phase of a protector

(b) Collision occurs during PN sequence detection phase of a protector

Figure 4.9: Collision cases when using the NBP protector

The first collision case shown in Fig. 4.9 (a) is when a Wi-Fi packet arrives and starts transmitting during the RX-TX switching of the protector. This case occurs since the RT-TX switching time takes 192 µs, while the Wi-Fi backoff may complete in about 72 µs. In this case, the protector simply continues to send the reservation signal since it has no way of detecting the presence of Wi-Fi packets. As a result, the first packet of the ZigBee burst will be corrupted, but the rest of the ZigBee packets in the burst will survive because the reservation signal will prevent Wi-Fi from transmitting anymore. This is generally true since a ZigBee transmission takes much longer time than a typical Wi-Fi transmission.

The second case is when a Wi-Fi packet arrives during the correlation. If the protector detects the collision before channel switching, it can simply abort. In more specific, the protector checks the corrupted bits in the first one byte preamble to detect the collision. In the IEEE 802.15.4 PHY layer, the one byte preamble is converted into two units of 32-bit chipping sequences by the spread spectrum technique. When the ZigBee nodes are the only ones that are occupying the channel, the preamble bits should match well at the receiver side. In contrast, considering that the Wi-Fi interference should be detected as a form of consistent and powerful noise, the number of corrupted bits of the ZigBee preambles significantly increases. After the NBP protector sees the correlation value spike, many erroneous bits in the first preamble means that it is very likely that some other simultaneous transmission exists. For this case, NBP takes a conservative approach; the protector does not send the reservation signal because the source of interference is unknown. This behavior may give more channel access opportunities to Wi-Fi nodes, and thus prevent the channel from being underutilized. We have measured the trend of erroneous bits in our implementation.

5. Mathematical Analysis

5.1 Assumptions and Notations

We consider a ZigBee network that shares the same frequency band with a Wi-Fi network that uses energy detection as well as preamble detection as a part of CCA. We assume that packet arrivals of both networks follow a Poisson distribution. We also assume the aggregated traffic pattern is approximately Poisson. Table 5.1 summarizes the notations that will be used in our analysis.

Table 5.1: Notations

Notations	Meaning
λ_z	Packet arrival rate for ZigBee
τ_z	Transmission time for a data packet for ZigBee
τ_{za}	Transmission time for an ACK packet for ZigBee
τ_{cts}	Transmission time for a CTS packet for ZigBee
β_z	Total time required from backoff to ACK for ZigBee
J_z	Channel switching time for ZigBee
γ_z	Handshake time for the exchange of data and ACK for ZigBee
U_z	Slot time for ZigBee
R_z	Retransmission limit (default to 3 [24]) for ZigBee
C_z	Time for a correlation with PN sequences
B_k	The duration of k-th backoff attempt
λ_w	Packet arrival rate for Wi-Fi
τ_w	Transmission time for a data packet for Wi-Fi
τ_{wa}	Transmission time for an ACK packet for Wi-Fi
β_w	Total time required from backoff to ACK for Wi-Fi

5.2 Collision Probability

For comparison, we first analyze the collision probability of the Cooperative Busy Tone (CBT). CBT uses a busy-tone to cover the entire ZigBee transmission duration from backoff to ACK. This assures that both the data and ACK packets do not collide with Wi-Fi transmissions. However a collision may still occur during the control message exchange. As shown in the Fig. 5.1, the CBT needs to conduct the RX-TX state transition to send a channel grant message, i.e., CTS. If a Wi-Fi packet arrives during the transition time, it will collide. This collision corrupts the ZigBee transmission as well as the Wi-Fi transmission, as a ZigBee node cannot send a data packet without the permission from the protector.

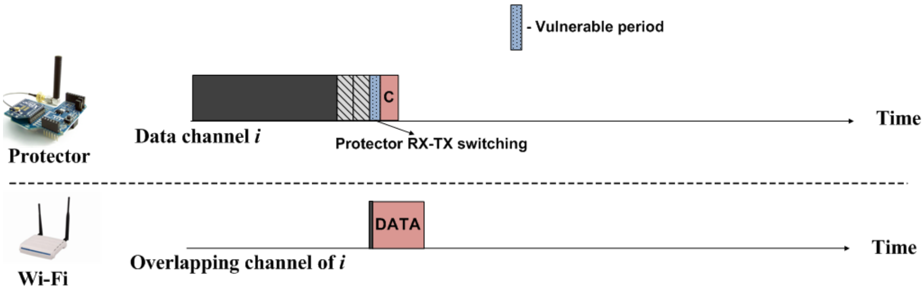


Figure 5.1: CBT vulnerable period

Since packets arrive according to the Poisson distribution, the collision probability of CBT can be derived as:

$$P_c^{CBT} = 1 - e^{-\lambda_W J_z} \tag{2}$$

CBT has identical collision probabilities in both symmetric and asymmetric interference regions because the protector-initiated contention eliminates the asymmetric property. However, in NBP, the collision probabilities differ; Fig. 5.2 (a) and (b) depict the vulnerable periods of NBP.

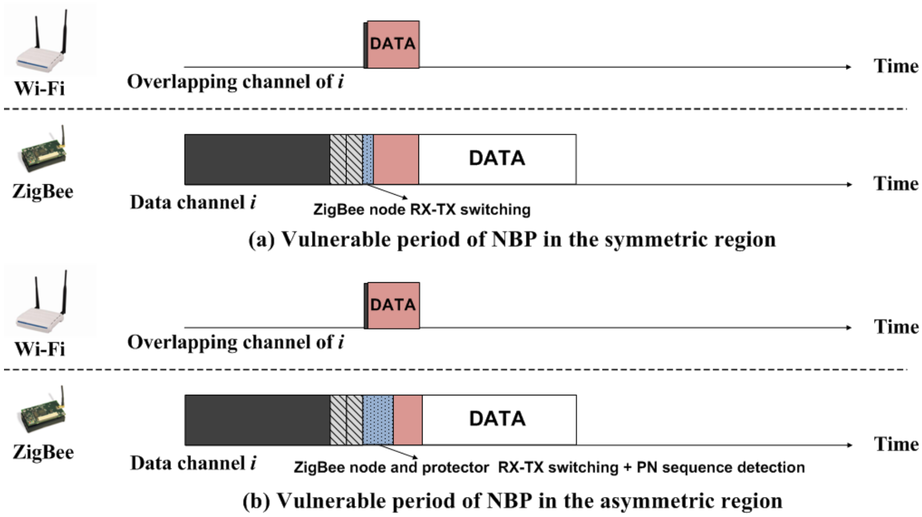

Wi-Fi
DATA
Overlapping channel of i
Time
ZigBee
DATA
Data channel i
ZigBee node RX-TX switching
Time
(a) Vulnerable period of NBP in the symmetric region
Wi-Fi
DATA
Overlapping channel of i
Time
ZigBee
DATA
Data channel i
ZigBee node and protector RX-TX switching + PN sequence detection
Time
(b) Vulnerable period of NBP in the asymmetric region

Figure 5.2: NBP vulnerable period

In the symmetric region, a collision can only occur during the ZigBee RX-TX state transition time. In the asymmetric region, however, the protector cannot prevent ZigBee signals colliding with Wi-Fi signals until the reservation signal is actually transmitted. This includes two RX-TX switching delays (one for ZigBee and the other for the protector) and the NBP's cross-correlation time. Therefore, the collision probabilities for these two cases are:

$$P_{c,sym}^{NBP} = 1 - e^{-\lambda_w J_z} \tag{3}$$

$$P_{c,asy}^{NBP} = 1 - e^{-\lambda_w (2J_z + C_z)} \tag{4}$$

Next, we derive the average achievable throughput for each scheme.

5.3 Network Performance

We compute the network performance using a renewal reward process. Let *R(t)* be the total reward earned up to time *t*. From the fundamental theorem of the renewal reward process [50], *R(t)* is expressed as:

$$\lim_{t\to\infty}\frac{R(t)}{t}=\frac{E[R]}{E[D]} \tag{5}$$

where *E[R]* is the average reward during a cycle, and *E[D]* is the average cycle duration. From Equ. (5), the throughput of ZigBee networks for NBP in both symmetric and asymmetric cases are computed as:

$$\Gamma_{z,sym}^{NBP}=\frac{[1-(P_{c,sym}^{NBP})^{R_z}]\tau_z}{\overline{T}_{z,sym}^{NBP}} \tag{6}$$

$$\Gamma_{z,asy}^{NBP}=\frac{[1-(P_{c,asy}^{NBP})^{R_z}]\tau_z}{\overline{T}_{z,asy}^{NBP}} \tag{7}$$

Each renewal interval is the duration from backoff to successful ACK, which may include multiple transmissions due to the transmission failures (the retry limit is 3 [2]). Therefore, the average renewal intervals in both symmetric and asymmetric cases are expressed as:

$$\overline{T}_{z,sym}^{NBP}=(E[B_z]+\gamma_{nbp})\sum_{k=0}^{R_z-1}(P_{c,sym}^{NBP})^k \tag{8}$$

$$\overline{T}_{z,asy}^{NBP} = (E[B_z] + \gamma_{nbp}) \sum_{k=0}^{R_z-1} (P_{c,asy}^{NBP})^k \tag{9}$$

where *E[B$_z$]* is the average backoff duration and $\gamma_{nbp} = 2J_z + \tau_z + \tau_{za}$ is the duration of a transmission attempt after backoff and CCA of a ZigBee node. The value of *E[B$_z$]* is derived using a small Markov chain for a backoff procedure as in [18]. For CBT, the average renewal interval is derived as:

$$\overline{T}_{z}^{CBT} = (E[B_z] + \gamma_{cbt}) \sum_{k=0}^{R_z-1} \{(1 - P_s^{CBT})^k \sum_{m=0}^{\infty} (P_c^{CBT})^m\} \tag{10}$$

where $\gamma_{cbt} = 3J_z + \tau_{cts} + B_1 + 2U_z + \tau_z + \tau_{za}$ and $\mathrm{P_s^{CBT}}$ is the transmission success probability of CBT. γ_{nbp} is much larger than γ_{nbp} because unlike NBP, CBT includes the contention overhead and coordination time.

For Wi-Fi, the throughput depends on the duration of the reservation signal which is a function of the ZigBee traffic load. So, a larger value of γ_{cbt} results in significant Wi-Fi throughput degradation in CBT while NBP ensures a reasonable Wi-Fi throughput. The NBP protector does not emit a reservation signal when a collision occurs in the symmetric region because it detects the collision during correlation. In contrast, the reservation signal only affects Wi-Fi transmissions in the asymmetric region. The mean Wi-Fi service times for both schemes are computed as:

$$\overline{T}_{w}^{CBT} = (1 - \frac{\lambda_z}{\lambda_w})\beta_w + \frac{\lambda_z}{\lambda_w}(\gamma_{cbt} - T_w + \beta_w) \tag{11}$$

$$\overline{T}_{w,sym}^{NBP} = (1 - \frac{N_{nbp}\lambda_z}{\lambda_w})\beta_w + \frac{N_{nbp}\lambda_z}{\lambda_w}(\tau_z + \beta_w) \tag{12}$$

$$\overline{T}_{w,asy}^{NBP} = (1 - \frac{N_{nbp}\lambda_z}{\lambda_w})\beta_w + \frac{N_{nbp}\lambda_z}{\lambda_w}(\gamma_{nbp} - T_w + \beta_w) \tag{13}$$

where N_{nbp} is the mean number of busy-tone attempts by a protector in its renewal interval. The values of N_{nbp} in both regions are different. In the asymmetric region, however, the NBP's the Wi-Fi protection feature (described in the subsection 4.4) allows Wi-Fi, not ZigBee, to transmit a packet. In this case, we compute the value of N_{nbp} by reducing the vulnerable period to the same as symmetric case and this value is derived as:

$$N_{nbp} = \sum_{r=1}^{R_z}[(1-(1-P_{tx})^K)P_{c,sym}^{NBP}]^{r-1} \tag{14}$$

where K is the maximum backoff stage. P_{tx} is the attempt rate for a protector and is given by:

$$P_{tx} = P_{idle}P_{idle|idle} = (1 - \frac{\gamma_w}{T_w})e^{-\lambda_w U_z} \tag{15}$$

Following the renewal model as in the ZigBee network, the throughput of the Wi-Fi network with NBP is:

$$\Gamma_w^{NBP} = \frac{\tau_w}{\overline{T}_w^{NBP}} \tag{16}$$

Similarly, the throughput of the Wi-Fi network with CBT is:

$$\Gamma_w^{CBT} = \frac{\tau_w}{\overline{T}_w^{CBT}} \tag{17}$$

5.4 Multiple Packet Transmissions

By adopting the cross-correlation, the protector of NBP can accurately estimate the duration for *m* consecutive transmissions in each burst. This protects all the ZigBee packets except for the first one that may collide with the Wi-Fi transmission. The throughput and average renewal interval for *m* transmissions are given by:

$$\Gamma_{z,m}^{NBP} = \frac{[1-(P_c^{NBP})^{R_z}]\tau_z + (m-1)\tau_z}{\overline{T}_{z,m}^{NBP}} \tag{18}$$

$$\overline{T}_{z,m}^{NBP} = (E[B_z] + \gamma_{nbp}) \sum_{k=0}^{R_z-1} (P_c^{NBP})^k + (m-1)\gamma_{nbp} \tag{19}$$

6. Performance evaluation

6.1 USRP Experiments

6.1.1 Experimental setup

We implement the two detection schemes of NBP, namely the burst length estimation and collision detection scheme, on the USRP [51] running GNU Radio 3.4.2 [52]. We employ the basic UCLA ZigBee PHY module [53], and modify it to include the 4 byte-PN sequences at the beginning of the preamble. Fig. 6.1 shows the ZigBee frame format with predefined ZigBee signature.

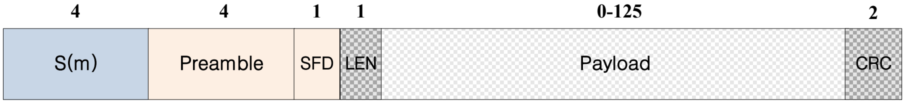


Figure 6.1: ZigBee frame format in NBP

In IEEE 802.15.4, each data bit is encoded to data symbols and then direct sequence spread spectrum (DSSS) spreads the data symbols according to the given chipping sequences. This generates a stream of chips and the stream is modulated with the offset-quadrature phase shift keying (O-QPSK). As shown in Table 6.1, each chipping sequence in the IEEE 802.15.4 becomes the shifted version of the other chipping sequences. Due to this property, if we insert the PN sequence prior to the DSSS spread without a preamble synchronization, different PN sequences cannot be properly distinguished.

Table 6.1: The spreading sequence of IEEE 802.15.4 [53]

Symbol	Chip sequence (C0, C1, C2, ... , C31)	uInt32 value
0	11011001110000110101001000101110	3653456430
1	11101101100111000011010100100010	3986437410
2	00101110110110011100001101010010	786023250
3	00100010111011011001110000110101	585997365
4	01010010001011101101100111000011	1378802115
5	00110101001000101110110110011100	891481500
6	11000011010100100010111011011001	3276943065
7	10011100001101010010001011101101	2620728045
8	10001100100101100000011101111011	2358642555
9	10111000110010010110000001110111	3100205175
10	01111011100011001001011000000111	2072811015
11	01110111101110001100100101100000	2008598880
12	00000111011110111000110010010110	125537430
13	01100000011101111011100011001001	1618458825
14	10010110000001110111101110001100	2517072780
15	11001001011000000111011110111000	3378542520

For this reason, we insert the PN sequence after the chipping sequence conversion as depicted in Fig. 6.2.

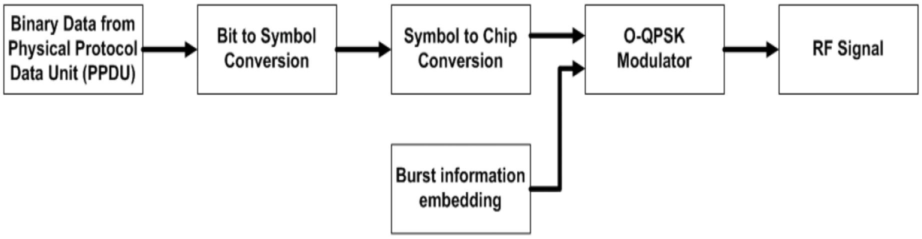

Binary Data from Physical Protocol Data Unit (PPDU)
Bit to Symbol Conversion
Symbol to Chip Conversion
O-QPSK Modulator
RF Signal
Burst information embedding

Figure 6.2: Block diagram for modulation and spreading

After correlating the PN sequence, the NBP protector counts the number of erroneous bits of the first 32-bit chipping sequence in the preamble and determines whether a Wi-Fi collision occurred. In our experiment, we measure the detection accuracy for a particular PN sequence while multiple ZigBee nodes are transmitting their PN sequences. We performed our experiments in our indoor lab (Fig. 6.3) where the channel is relatively dynamic; the SNR of the ZigBee packets varies from 0dB to 12dB. We have randomly chosen four positions, and let one node serve as a protector and the other three nodes as ZigBee clients transmitting PN sequences. In addition, we measure the number of corrupted bits under various Wi-Fi interference scenarios. The difference in signal strengths between ZigBee and Wi-Fi transmitter varies from -4dB to 10dB.

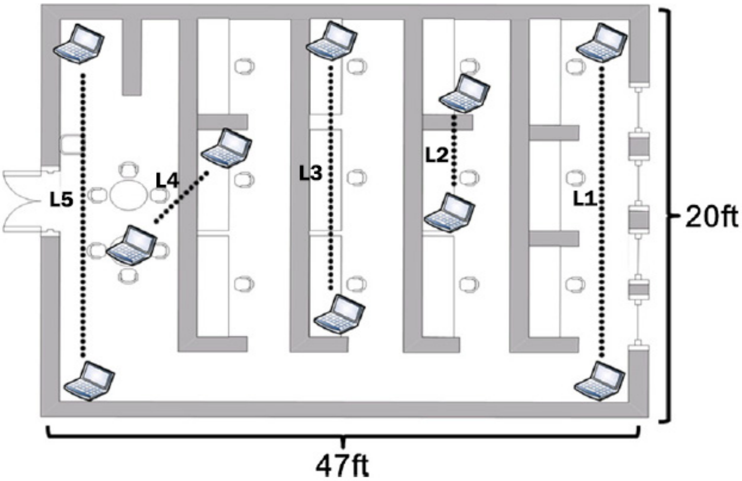


Figure 6.3: Experimental setup - the topology

To explore the effect of link locations, we also measure the collision probabilities of NBP and CBT in various locations. We set four pairs of ZigBee nodes (L2 ~ L5) and one pair of Wi-Fi nodes (L1). The Wi-Fi link L1 can only sense L2, L3 and L4 ZigBee links.

6.1.2 Experimental Results

Fig. 6.4 shows the false negative rate of detecting the PN sequences. As the SNR at the receiver increases, the false negative clearly rate decreases. The non-spread PN sequences do not incur false positives in correlation. The false detection rates are below 0.05% in all cases, which validates that our cross-correlation method is feasible in practice.

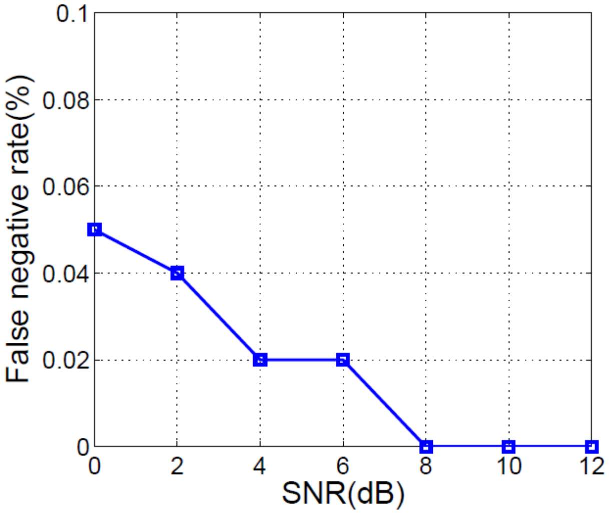


Figure 6.4: False negative rate vs. SNR

Fig. 6.5 shows the average erroneous bits of the 32-bit chipping sequence in the ZigBee preamble in the presence of Wi-Fi interference. The average number of corrupted bits steadily increases with the larger Wi-Fi interference, until it shows a sharp escalation at 0dB. This indicates that a collision occurred, since the majority of the packets were corrupted. Notice that the erroneous bits do not exceed a certain point (e.g., 18 bits), since some corrupted bits are randomly matched with the chipping sequence. When the ZigBee signal is stronger than the Wi-Fi signal by just 2 dB or more, ZigBee correctly detects the preamble. The results show that NBP can determine the Wi-Fi collision by configuring the bit threshold by around 10. When the erroneous bits exceed 10, the ZigBee node eventually misses the preamble.

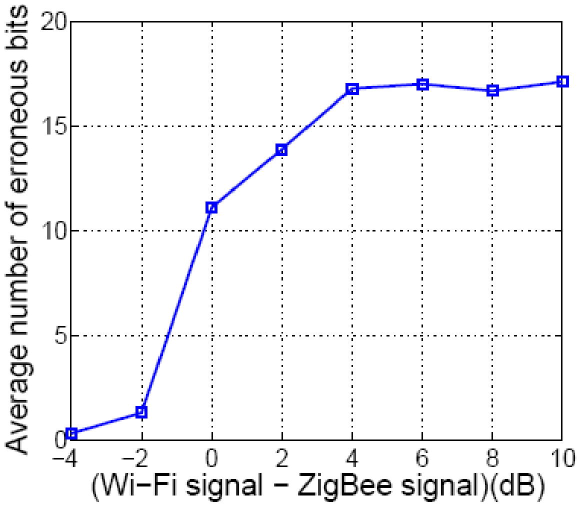


Figure 6.5: Average number of erroneous bits

Fig. 6.6 shows the mean packet duration for transmitting a single packet at the ZigBee link. The mean packet duration consists of the data transmission time, various overheads, and packet collisions. The mean packet duration of NBP is continuously smaller than CBT for all links. This occurs since the coordination overhead and large reservation cycle of CBT incurs very large overhead. In NBP, however, the vulnerable period of the symmetric region (L2, L3, and L4) is smaller than that of the asymmetric region (L5), since the collisions incur additional retransmission overheads. In contrast, CBT eliminates the asymmetric property and gives similar packet durations. Table 6.2 summarizes normalized throughput of each ZigBee link. NBP outperforms CBT in all links due to its low overhead operation in both regions. We further discuss the network performance of both NBP and CBT in the section 6.2.2 with NS-2 simulations.

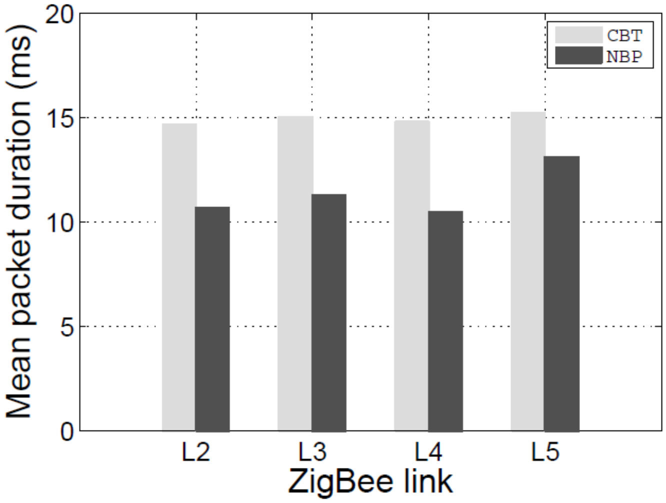


Figure 6.6: Mean packet duration of ZigBee links L2 – L5

Table 6.2: The throughput of ZigBee links L2 – L5.

ZigBee Link	**Normalized throughput of CBT**	**Normalized throughput of NBP**
L2	**0.1524**	**0.2116**
L3	**0.1489**	**0.2005**
L4	**0.1510**	**0.2158**
L5	**0.1471**	**0.1727**

6.2 NS-2 Simulations

6.2.1 Simulation Setup

In this subsection we conduct NS-2 [54] simulations to evaluate our proposal in various scenarios. Furthermore, we validate our mathematical analysis in the previous section. In the simulations, NBP and CBT employ the IEEE 802.15.4 protocol stack and Wi-Fi uses the IEEE 802.11g standard. The PHY/MAC protocol parameters are set to their default values in the standards. Fig. 6.7 shows the network topology. We set just one pair of ZigBee TX-RX nodes and one pair of Wi-Fi TX-RX nodes to just focus on the coexistence problem. We study both symmetric (d=5m) and asymmetric (d=30m) regions for the ZigBee pair in the simulations. However, the Wi-Fi pair is always visible to the ZigBee pair so that ZigBee nodes are apt to suffer from starvation without the help from the protector.

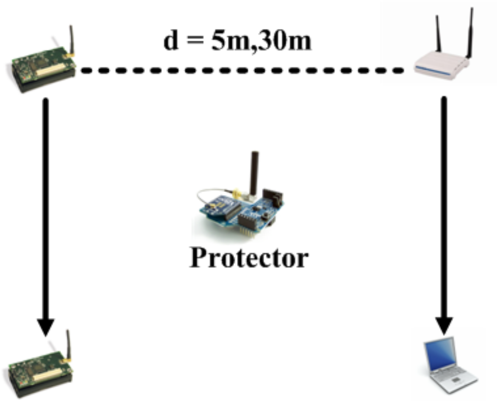


Figure 6.7: Network topology

ZigBee sends 70 byte data packets with bit-rate of 250Kbps. Wi-Fi uses 1K byte packets with bit-rate of 18 Mbps. We compare the throughput results of ZigBee and Wi-Fi networks under varying traffic loads. We define the traffic load as a normalized term, the ratio of packet arrival rate over the physical capacity:

$$\text{traffic load} = \frac{\text{packet size} \times \text{packet arrival rate}}{\text{PHY layer bit rate}} \qquad (20)$$

6.2.2 Simulation Results

Fig. 6.8 shows the throughput of ZigBee networks as a function of Wi-Fi interference traffic ranging from 0% to 60%. We observe that the analytic and the simulation results match well. As expected, there are more collisions with the increasing Wi-Fi traffic load, resulting in lower throughput. In the asymmetric region, when the Wi-Fi traffic load is lesser or equal to 41%, NBP outperforms CBT for both ZigBee and Wi-Fi. The reason is that the CBT coordination messages are sent by a ZigBee node, and it may collide with the Wi-Fi packets. In that case, the ZigBee node suspends its transmission to the next reservation cycle and hence the throughput decreases. In case of the symmetric region, NBP consistently outperforms CBT. Due to the visibility of data packets, the ZigBee's collision probability with NBP is smaller than that of the asymmetric region.

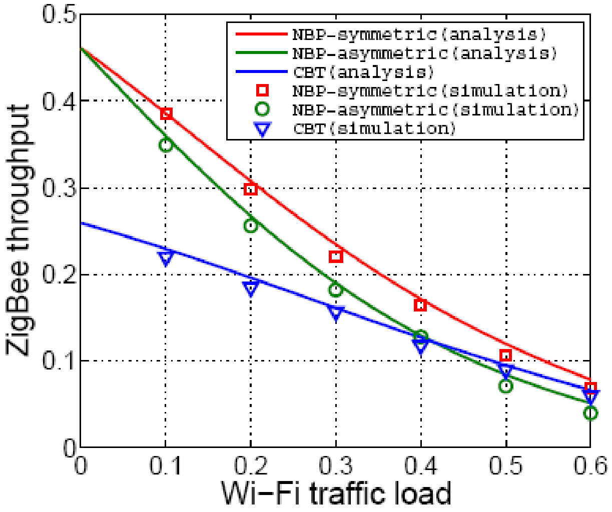


Figure 6.8: ZigBee throughput vs. Wi-Fi traffic load

When the Wi-Fi traffic load exceeds 41%, the ZigBee pair in the asymmetric region of NBP shows lower throughput. CBT does not have the asymmetric property because the high-power protector directly contends with the Wi-Fi nodes. Moreover, the vulnerable period of NBP in the asymmetric region is larger than that of CBT. Thus NBP's rate of service time increase is slightly higher as the Wi-Fi traffic load increases. However, as shown in recent measurement studies [55, 56], the median utilization of Wi-Fi networks is typically lesser than 30%. This implies that NBP is suitable for the real coexistence environment. In summary, NBP improves the ZigBee throughput by up to 1.77x compared to CBT. When there exist multiple Wi-Fi APs, the ZigBee throughput is affected by the aggregated interference intensity of the Wi-Fi channels that overlap with the same ZigBee channel.

We next discuss the Wi-Fi performance under both schemes. Fig. 6.9 shows the throughput of Wi-Fi networks under varying ZigBee traffic load. Since NBP's reservation does not include the contention process, NBP jams Wi-Fi for a shorter duration. Therefore, unlike CBT, Wi-Fi can coexist with NBP-assisted ZigBee, achieving reasonable throughput. When detecting the collision during correlation, NBP does not transmit the reservation signal to protect the ZigBee located in the asymmetric region. Therefore, it avoids unnecessary channel preemption of the protector. Most of the ZigBee applications perform a low duty-cycle mechanism (traffic load of 1% ~ 10%). Even under this scenario, the achievable throughput of Wi-Fi with NBP is greater than that with CBT.

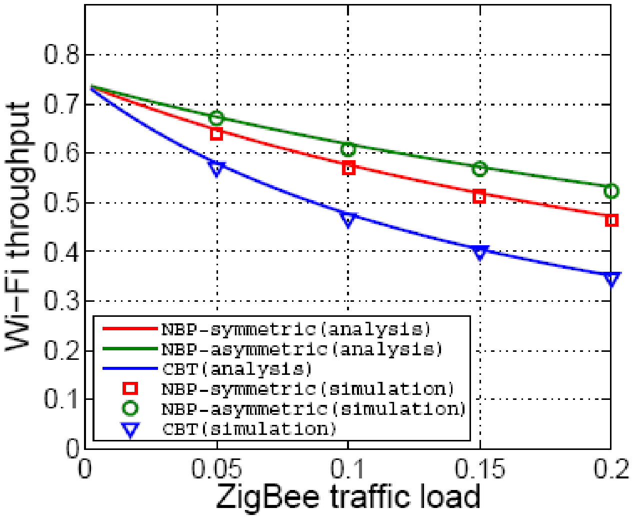


Figure 6.9: Wi-Fi throughput vs. ZigBee traffic load

Fig. 6.10 demonstrates the throughput gain of using a burst of multiple packet transmissions over a single packet transmission with NBP. We fix the Wi-Fi interference traffic to 20% and vary the number of multiple packets. When a burst of ZigBee packets are transmitted, $m - 1$ consecutive packets are successfully delivered. In addition, as the number of multiple packets protected by a single reservation increases, the congestion overhead is reduced. As a result, supporting m consecutive packets achieves higher throughput than a single packet transmission by up to 2.07x.

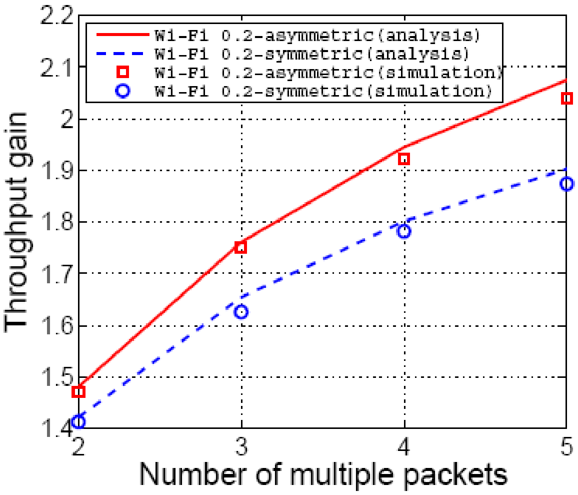


Figure 6.10: Throughput gain of ZigBee as a function of the number of multiple packets

Fig. 6.11 shows the throughput gain of multiple packets transmission as a function of Wi-Fi traffic load. We fix the burst length and vary the Wi-Fi traffic load. Although the transmission opportunity of a ZigBee node decrease in the high Wi-Fi traffic loads, NBP prevents collisions for the $m-1$ packets in various Wi-Fi traffic loads. Therefore, the throughput gain increases as the Wi-Fi traffic load increases.

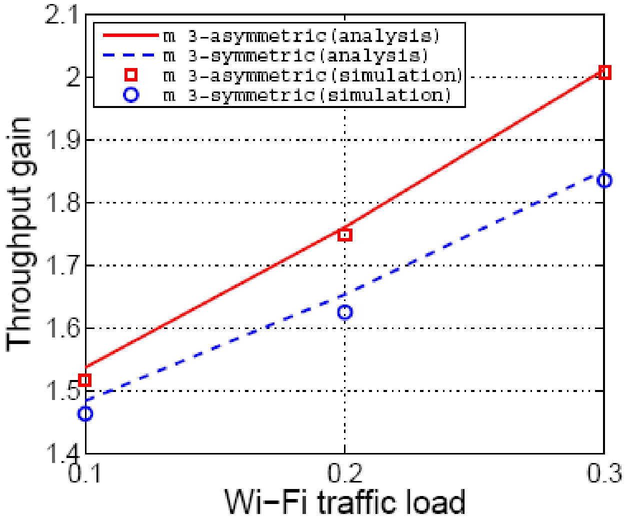


Figure 6.11: Throughput gain of ZigBee as a function of Wi-Fi traffic load

7. Conclusion

This thesis presented a new Narrow Band Protection scheme that addresses the cross-technology interference problem between ZigBee and Wi-Fi. By the PHY-layer correlation technique, the NBP protector effectively detects the ongoing ZigBee transmissions with light-weight overhead. In addition, it protects the burst of ZigBee packets by using the correlation with the PN codebook. We showed the feasibility of NBP by implementing it on the real USRP/GNURadio platform. Furthermore, our simulation and analysis show that NBP significantly outperforms the state-of-the art protection scheme in various environments.

Bibliography

[1]Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specications. IEEE Std. 802.11, 2007

[2]Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specications for Low-Rate Wireless Personal Area Networks (LR-WPANs). IEEE Std. 802.15.4, 2003

[3]Shyamnath Gollakota, Fadel Adib, Dina Katabi, Srinivasan Seshan, "Clearing the RF Smog: Making 802.11 Robust to Cross-Technology Interference", Sigcomm 2011

[4]Shravan Rayanchu, Ashish Patro, Suman Banerjee, "Catching Whales and Minnows using WiFiNet: Deconstructing NonWiFi Interference using WiFi Hardware", NSDI 2012

[5]Shravan Rayanchu, Ashish Patro, Suman Banerjee, "Airshark: Detecting Non-WiFi RF Devices using Commodity WiFi Hardware", IMC 2011

[6]Coexistence of wireless personal area networks with other wireless devices operating in unlicensed frequency bands, IEEE Std 802.15.2, 2003.

[7]Coexistence Analysis of IEEE Std 802.15.4 With Other IEEE Standards and Proposed Standards, IEEE 802.15 Working Group, 2010.

[8]Leopoldo Angrisani, Matteo Bertocco, Daniele Fortin and Alessandro Sona, "Experimental Study of Coexistence Issues Between IEEE 802.11b and IEEE 802.15.4 Wireless Networks", IEEE Transactions on Instrumentation and Measurement 2008

[9]Ramakrishna Gummadi, Hari Balakrishnan, Srinivasan Seshan, “Metronome: Coordinating Spectrum Sharing in Heterogeneous Wireless Networks”, COMSNETS 2009

[10]Schneider Electrics. ZigBee Wi-Fi Coexistence. http://www.zigbee.org/LearnMore/White Papers.aspx, 2008

[11]Chieh-Jan Mike Liang, Nissanka Bodhi Priyantha, Jie Liu, Andreas Terzis, “Surviving Wi-Fi Interference in Low Power ZigBee Networks”, Sensys 2010

[12]Sofie Pollin, Ian Tan, Bill Hodge, Carl Chun, Ahmad Bahai, “Harmful Coexistence Between 802.15.4 and 802.11: A Measurement-based Study”, CrownCom 2008

[13]Axel Sikoral, Voicu F. Groza, “Coexistence of IEEE 802.15.4 with other systems in the 2.4Ghz-ISM band”, IMTC 2005

[14]Chulho Won, Jong-Hoon Youn, Hesham Ali, Hamid Sharif, and Jitender Deogun, “Adaptive Radio Channel Allocation for Supporting Coexistence of 802.15.4 and 802.11b”, VTC 2005

[15]Sofie Pollin, Mustafa Ergen, Antoine Dejonghe, Liesbet Van der Perre, Francky Catthoor, Ingrid Moerman, Ahmad Bahai, “Distributed cognitive coexistence of 802.15.4 with 802.11”, Crowncom 2006

[16]Lei Tang, Yanjun Sun, Omer Gurewitz, David B. Johnson , “EM-MAC: A Dynamic Multichannel Energy-Efficient MAC Protocol for Wireless Sensor Networks”, Mobihoc 2011

[17]Jun Huang, Guoliang Xing, Gang Zhou, Ruogu Zhou, “Beyond Co-existence: Exploiting Wi-Fi White Space for ZigBee Performance

Assurance”, ICNP 2010

[18]Xinyu Zhang and Kang G. Shin, “Enabling Coexistence of Heterogeneous Wireless Systems: Case for ZigBee and Wi-Fi”, Mobihoc 2011

[19]Bozidar Radunovic, Ranveer Chandra, Dinan Gunawardena , “Adaptive Preambles for Coexistence”, MSR Technical Report 2011

[20]Shyamnath Gollakota, Dina Katabi, “Zig-Zag Decoding: Combating Hidden Terminals in Wireless Networks”, Sigcomm 2008

[21]Souvik Sen, Romit Roy Choudhury, Srihari Nelakuditi, “CSMA/CN: Carrier Sense Multiple Access with Collision Notification”, MobiCom 2010

[22]Eugenio Magistretti, Omer Gurewitz, Edward W. Knightly, “802.11ec: Collision Avoidance without Control Messages”, MobiCom 2012

[23]H. Meyr, M. Moeneclaey, and S. A. Fechtel, “Digital Communication Receivers: Synchronization, Channel Estimation, and Signal Processing”, John Wiley & Sons, 1998

[24]D. Tse and P. Vishwanath, “Fundamentals of Wireless Communications”, Cambridge University Press, 2005

[25]P. Castoldi, “Multiuser Detection in CDMA Mobile Terminals”, Artech house Publishers, 2002

[26]S. M. Kay, “Fundamentals of Statistical Signal Processing, Volume 2: Detection Theory”, Prentice Hall, 1998

[27]K. Kyouwoong, I. Akbar, K. Bae, J. Urn, C. Spooner, and J. Reed, “Cyclostationary approaches to signal detection and classification in cognitive radio”, DySpan 2007

[28]S. M. Mishra, R. W. Brodersen, S. ten Brink, and R. Mahadevappa, “Detect and avoid: An ultra-wideband/WiMAX coexistence mechanism”, IEEE Communications Magazine, 45(6):68–75, 2007.

[29]S. Nagaraj, S. Khan, C. Schlegel, and M. Burnashev, “Differential preamble detection in packet-based wireless networks”, IEEE Transactions on Wireless Communications, 8(2):599–607, 2009.

[30]S. Duquennoy, F. Osterlind, and A. Dunkels, “Lossy links, low power, high throughput”, SenSys 2011

[31]M. Anwander, G. Wagenknecht, T. Braun, and K. Dolfus, “Beam: A burst-aware energy-efficient adaptive mac protocol for wireless sensor networks”, INSS 2010

[32]F. Osterlind, L. Mottola, T. Voigt, N. Tsiftes, A. Dunkels, “Strawman: Resolving Collisions in Bursty Low-Power Wireless Networks”, IPSN 2012

[33]W. Ye, J. Heidemann and D. Estrin, “An energy efficient mac protocol for wireless sensor networks”, INFOCOM 2002

[34]Shu Du, Amit Kumar Saha, and David B. Johnson, “RMAC: A Routing-Enhanced Duty-Cycle MAC Protocol for Wireless Sensor Networks”, INFOCOM 2007

[35]Y. Sun, S. Du, O. Gurewitz, and D. B. Johnson. “DW-MAC: A Low Latency, Energy Efficient Demand-Wakeup MAC Protocol for Wireless Sensor Networks”, Mobihoc 2008

[36]A. El-Hoiydi, “Aloha with Preamble Sampling for Sporadic Traffic in Ad Hoc Wireless Sensor Networks”, ICC 2002

[37]A. El-Hoiydi and J-D. Decotignie. “WiseMAC: An Ultra Low Power

MAC Protocol for Multi-hop Wireless Sensor Networks.” ALGOSENSORS 2004

[38]Sangsoon Lim, Jiwoong Jeong, Jongkeun Na, Chong-kwon Kim, “Performance enhancement of low power listening MAC for duty cycled wireless sensor networks”, ICOIN 2009

[39]M. Buettner, Gary V. Yee, E. Anderson and R. Han, “X-MAC: a short preamble MAC protocol for duty-cycled wireless sensor networks”, SenSys 2006

[40]J. Polastre, J. Hill and D. Culler, “Versatile low power media access for wireless sensor networks”, SenSys 2004

[41]T. van Dam and K. Langendoen, “An adaptive energy-efficient MAC protocol for wireless sensor networks”, SenSys 2003

[42]Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, “A survey on sensor networks”, IEEE Communications Magazine, vol. 40, no. 8, pp. 102-114, Aug. 2002

[43]S. Lim, Y. Ji, J. Cho and S. An, “An ultra low power medium access control protocol with the divided preamble sampling”, UCS 2006

[44]I. Howitt, “WLAN and WPAN coexistence in UL band”, IEEE Trans. Veh. Technol., vol. 50, no. 4, pp. 1114-1124, Jul. 2001

[45]I. Howitt and J. Gutierrez, “IEEE 802.15.4 low rate-wireless personal area network coexistence issues”, WCNC 2003

[46]Soo Young Shin, Hong Seong Park, Sunghyun Choi and Wook Hyun Kwon, “Packet Error Rate Analysis of ZigBee Under WLAN and Bluetooth Interferences”, IEEE Trans. Wireless Communications 2007

[47]Soo Young Shin, Hong Seong Park, Wook Hyun Kwon, “Mutual interference analysis of IEEE 802.15. 4 and IEEE 802.11 b”, Computer Networks 2007

[48]James Hou, Benjamin Chang, Dae-Ki Cho, Mario Gerla, “Minimizing 802.11 Interference on ZigBee Medical Sensors”, Bodynets 2009

[49]Digi International Inc. XBee-PRO 802.15.4 OEM RF Modules. http://www.digi.com/

[50]Sheldon M. Ross, “Stochastic process”, second edition, 1996

[51]Ettus Research, LLC. http://www.ettus.com

[52]GNU Radio Project. http://gnuradio.org/redmine/wiki/gnuradio

[53]T. Schmid, “GNU Radio 802.15.4 En- and Decoding”, Technical Report, UCLA NESL, 2006.

[54]Network simulator 2. http://www.isi.edu/nsnam/ns/

[55]A. Schulman, D. Levin, and N. Spring, “Crawdad data set umd/sigcomm2008 (v. 2009-03-02)”, 2009

[56]R. Chandra, R. Mahajan, V. Padmanabhan, and M. Zhang, “Crawdad data set microsoft/osdi2006 (v.2007-05-23)”, 2007

[57]Ioannis Glaropoulos, Viktoria Fodor, Loreto Pescosolido, Chiara Petrioli, “Cognitive WSN transmission control for energy efficiency under WLAN coexistence”, CROWNCOM 2011

[58]Jing Zhu, Alan Waltho, Xue Yang, and Xingang Guo, “Multi-Radio Coexistence: Challenges and Opportunities”, ICCCN 2007

[59]Yufei Wang, Qixin Wang, Zheng Zeng, Guanbo Zheng, Rong Zheng, “WiCop: Engineering Wi-Fi Temporal White-Spaces for Safe Operations of

Wireless Body Area Networks in Medical Applications”, RTSS 2011

[60]Ruitao Xu, Gaotao Shi, Jun Luo, Zenghua Zhao, Yantai Shu, “MuZi: Multi-channel ZigBee Networks for Avoiding WiFi Interference”, CpsCom 2011

[61]M. Petrova, Lili Wu, P. Mahonen, and J. Riihijarvi, “Interference Measurements on Performance Degradation between Colocated IEEE 802.11g/n and IEEE 802.15.4 Networks”, ICN 2007.

[62]M. Rodrig, C. Reis, R. Mahajan, D. Wetherall, and J. Zahorjan, “Measurement-based Characterization of 802.11 in a Hotspot Setting”, SIGCOMM E-WIND 2005

[63]Crossbow Technology Inc., “MICAz Datasheet”, 2007.

[64]Crossbow Technologies. TelosB

[65]TinyOS Version 1.1.

[66]Texas Instruments Inc., MSP430 MCU

[67] Gahng-Seop Ahn, Se Gi Hong, Emiliano Miluzzo, Andrew T. Campbell, Francesca Cuomo, “Funneling-MAC: a localized, sink-oriented MAC for boosting fidelity in sensor networks”, SenSys 2006

[68]Y. Kang, S. Lim, J. Yoo, C. Kim, “Design, Analysis and Implementation of Energy-Efficient Broadcast MAC Protocols for Wireless Sensor Networks”, KSII Transactions on Internet and Information Systems, vol. 5, No. 6, June 2011.

[69]R. Musaloiu-E. and A. Terzis, “Minimising the Effect of WiFi Interference in 802.15.4 Wireless Sensor Networks”, International Journal of Sensor Networks, 3(1):43–54, 2007

[70]H. Rahul, N. Kushman, D. Katabi, C. Sodini, and F. Edalat, “Learning to share: Narrowband-friendly wideband networks”, Sigcomm 2008

[71]P. K. Pothuri, V. Sarangan, and J. P. Thomas, “Delay-constrained, energy-efficient routing in wireless sensor networks through topology control”, ICNSC 2006

[72]Farshad Ahdi, Vikram Srinivasan, and Kee-Chaing Chua, “Topology control for delay sensitive applications in wireless sensor networks”, Mobile Networks and Applications, Volume 12 Issue 5, December 2007, Pages 406-421

[73]James Brown, Joe Finney, Christos Efstratiou, Ben Green, Nigel Davies, Mark Lowton and Gerd Kortuem, “Network Interrupts: Supporting Delay Sensitive Applications in Low Power Wireless Control Networks”, CHANTS 2007

[74]Prabal Dutta, Stephen Dawson-Haggerty, Yin Chen, Chieh-Jan (Mike) Liang, and Andreas Terzi, “Design and Evaluation of a Versatile and Efficient Receiver-Initiated Link Layer for Low-Power Wireless”, SenSys 2010

[75]Injong Rhee, Ajit Warrier, Mahesh Aia, Jeongki Min, “Z-MAC: a Hybrid MAC for Wireless Sensor Networks”, SenSys 2005

[76]Yanjun Sun, Omer Gurewitz, and David B. Johnson, “RI-MAC: A Receiver Initiated Asynchronous Duty Cycle MAC Protocol for Dynamic Traffic Loads in Wireless Sensor Networks”, SenSys 2008

[77]Lei Tang, Yanjun Sun, Omer Gurewitz, and David B. Johnson, “PW-MAC: An Energy-Efficient Predictive-Wakeup MAC Protocol for Wireless

Sensor Networks”, INFOCOM 2011

[78]K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, “Denial of service attacks in wireless networks: The case of jammers”, IEEE Communications Surveys & Tutorials, PP(99):1–13, second quarter 2011

[79]W. Xu, W. Trappe, Y. Zhang, and T. Wood, “The feasibility of launching and detecting jamming attacks in wireless networks”, MobiHoc 2005

[80]W. Xu, K. Ma, W. Trappe, and Y. Zhang, “Jamming sensor networks: Attacks and defense strategies”, IEEE Networks, Volume 20, Issue 3, May/June 2006

[81]W. Xu et al, “Channel surfing and spatial retreats: Defenses against wireless denial of service”, Wireless Security 2004

[82]V. Navda, A. Bohra, S. Ganguly, and D. Rubenstein, “Using channel hopping to increase 802.11 resilience to jamming attacks”, INFOCOM 2007

초 록

최근 다양한 무선 네트워크 기술들(와이파이, 블루투스, 지그비)이 2.4GHz 대역의 ISM 밴드에 공존함으로 인하여 이들 간의 상호공존이 큰 문제로 나타나고있다. 특히 지그비 네트워크는 현저히 높은 전송 파워로 통신하는 와이파이 네트워크가 동일한 주파수 대역에 존재할 때 통신이 불가능해 질 정도의 심각한 성능 저하를 겪게 된다. 본 논문에서는 지그비 네트워크의 통신을 와이파이 네트워크의 간섭으로 부터 보호할 수 있는 좁은 대역 보호 방법(Narrow Band Protection)을 제안한다. 자가 감지 보호자는 좁은 대역 보호 방법의 핵심 기술로 사전에 정의된 PN 시퀀스에 대해 상호 상관 기법을 이용하여 스스로 지그비 패킷을 발견할 수 있어 최소한의 오버헤드로 지그비 네트워크를 보호할 수 있다. 또한, 자가 감지 보호자는 신뢰성 있는 상호 상관 기법을 통해 기존 방법에서 발생하는 제어 패킷 손실로 인한 두 네트워크의 이용효율 감소를 대폭 줄일 수 있다. 마지막으로, 시맨틱이 부여된 PN 코드북을 통해 저전력 동작을 수행하는 지그비 네트워크의 다량 패킷 전송을 효율적으로 감지하여 지그비 네트워크의 높은 처리량을 지원해 줄 수 있는 장점이 있다. 제안하고 있는 자가 감지 보호자는 시맨틱이 부여된 PN 시퀀스를 지그비 패킷의 프리앰블(Preamble) 앞에 임베딩 하는 기법을 사용한다. 이는 해당 기법을 적용하지 않는 지그비 노드들의 동기화를 방해하지 않는다. 즉, 좁은 대역 보호 방법은 기존 지그비 네트워크와 하위

호환성(backward compatibility)을 유지하며 기존 방법에 비해 단일 패킷에 대해서 1.77배 가량 높은 처리량을 제공해 줄 수 있으며, 다량 패킷 전송 보호시 보호하는 패킷의 수가 증가함에 따라 선형으로 이득이 증가하게 된다. 또한, 실제 USRP/GNURadio 플랫폼에 핵심 기능을 구현하여 실효성을 입증하였으며, 수학적인 분석과 확장된 NS-2 시뮬레이션을 통해 다양한 시각에서 상호공존 문제를 해석하고 있어 향 후 관련 분야에 큰 기여를 할 연구이다.

주요어: 상호 공존, 간섭 완화, 신호 상관 기법, 지그비, 와이파이, 이기종 무선 네트워크

학 번: 2007-30838