EURASIP Journal on
Wireless Communications and Networking
a SpringerOpen Journal

RESEARCH Open Access

NBP: light-weight Narrow Band Protection for ZigBee and Wi-Fi coexistence

Sangsoon Lim[1], Suchul Lee[1], Joon Yoo[2*] and Chong-Kwon Kim[1]

Abstract

The recent development of various wireless technologies in the 2.4GHz ISM band has led to the co-channel coexistence of heterogeneous wireless devices, such as Wi-Fi, Bluetooth, and ZigBee. This sharing of the common channel results in the challenging problem of cross-technology interference, since the wireless devices generally use diverse PHY/MAC specifications. In particular, the less capable ZigBee device may often experience unpredictably low throughput due to the interference from the powerful Wi-Fi. The ZigBee protector is an attractive solution, since it can reserve the channel on behalf of the weak ZigBee devices. The protector method, however, has a few limitations; (i) it may cause significant overhead to both ZigBee and Wi-Fi, and (ii) the ZigBee control packets are still vulnerable to the Wi-Fi interference. In this paper, we propose a novel time reservation scheme called Narrow Band Protection (NBP), that uses a protector to guard the ongoing ZigBee transmission. The key contributions are threefold: First, NBP autonomously detects any ongoing ZigBee transmissions by cross-correlating the ZigBee's packets with the pre-defined Pseudo-random Noise (PN) sequences. By using this cross-correlation, it significantly reduces the control overhead. Second, due to the reliable cross-correlation, NBP is robust from the control packet collisions, which typically wastes channel time for both ZigBee and Wi-Fi. Third, NBP protects the burst of ZigBee packets by estimating the size of the burst, in turn, giving a semantic to the PN codebook. This is important because ZigBee is typically battery-powered and thus the long burst is advantageous for the low duty cycle operations. We first show the feasibility of NBP by implementing it on the real USRP/GNURadio platform. Then, we 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 the existing scheme.

Keywords: Coexistence, Interference mitigation, Signal correlation, Time reservation, ZigBee, Wi-Fi

1 Introduction

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 generally use a predefined preamble sequence at the beginning of each packet to decode the signal. In result, this causes the heterogeneous devices to freely transmit even when another device is transmitting, thus causing severe interference to each other. This is called the *cross-technology interference problem* [3,4].

This is particularly unfavorable for less-capable technologies, i.e., *low priority networks*, because they often starve due to their relatively small transmission power and slow hardware. In particular, ZigBee networks that compete with *high priority networks* such as Wi-Fi networks, occasionally cannot send any packets due to their significantly disadvantageous medium access control (MAC) layer protocol timings [5-7]. 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 networks can preempt ZigBee networks even if a ZigBee node first grabs the medium and transmits.

The interference area between ZigBee and Wi-Fi can be divided according to the spatial interference relationship: the symmetric and asymmetric interference regions [8]. In

*Correspondence: joon.yoo@gachon.ac.kr
[2]Department of Software Design and Management, Gachon University, Seongnam, Korea
Full list of author information is available at the end of the article

the symmetric interference region, ZigBee nodes and Wi-Fi nodes are relatively close enough so that they can sense each other, thus collisions between them only occur at the very beginning of each transmission. In contrast, a ZigBee node in the asymmetric interference region may not be effectively sensed by a Wi-Fi node due to the ZigBee node's low transmission power (< 1mW). A Wi-Fi node will not defer its transmission even when there is an ongoing ZigBee transmission. 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 [5,6,9,10].

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 ZigBee channels that are less affected by the Wi-Fi transmission [11-13]. However, such a solution is often infeasible as the shared spectrum band may already have been heavily loaded with many heterogeneous wireless devices. Second, ZigBee frame control mechanisms [5,14] either adjust the size of the ZigBee packet or the inter-packet arrival time between ZigBee packets, so that the ZigBee packets opportunistically fit into the intervals of the Wi-Fi packets. However, these adjustments cannot guarantee the delivery of the ZigBee packets and hence are inapplicable for delay-sensitive ZigBee applications. The final approach is to use a dedicated entity to protect the ZigBee devices [15]. The dedicated entity, called protector, reserves the wireless medium on behalf of the ZigBee device. However, the ZigBee node still needs to explicitly notify the protector that it has a packet to send and hence the ZigBee MAC protocol has to be modified. More importantly, this method is still vulnerable to the Wi-Fi interference as this control packet itself is basically sent using ZigBee transmission.

In this paper, we propose a novel time reservation scheme, called Narrow Band Protection (NBP). NBP efficiently reduces the control overhead for the ZigBee channel reservation through a self-sensing mechanism, and allows ZigBee networks to compete with Wi-Fi networks even in an asymmetric scenario. Specifically, the NBP protector autonomously detects an ongoing ZigBee transmission and without any further delay, 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 give high fidelity of detection of low power ZigBee signals, NBP exploits the reliable cross-correlation technique [16,17]. 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 [18-20].

We implement NBP on the real 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 real USRP/GNURadio platform as well as the NS-2 simulator. This shows the feasibility and practicality of NBP in real environment.

The rest of this paper 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 NS-2 simulations. Finally, Section 7 concludes the paper.

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 [5,6,8-10]. In [5], 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 [8] 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 [21-24]. 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.* [12] tried to find an optimal interference-free channel by using Simulated Annealing and a Nash Q-learning method. The authors in [13], 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.* [14] 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 [5] 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 [15,25]. Hou *et al.* [25] 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 [15] 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 [16] and CSMA/CN [17] use cross correlation to effectively detect packet collision. 802.11ec [26] 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 [16,17] or 802.11 protocol efficiency [26], and (ii) NBP uses distinctive methods explained in the following sections.

3 Motivation

3.1 Overview of ZigBee and Wi-Fi

This paper 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 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 Figure 1.

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 $\sim$ 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 [5,8].

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 (Figure 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.

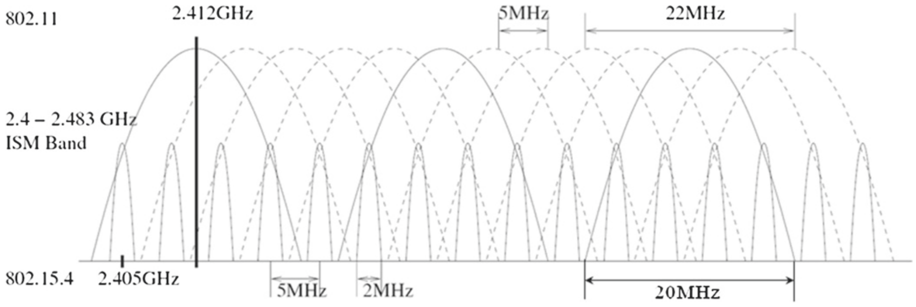

Figure 1 IEEE 802.15.4 and IEEE 802.11 channels.

There have been many proposals that deal with this problem [12,14,15], but among them the dedicated high-power protector scheme [15] 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 [15] is to improve the visibility of ZigBee signals by hiring a protector equipped with a more powerful hardware. Figure 3(a) illustrates the operation of the Cooperative Busy Tone (CBT) protector [15]. 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 [15]).
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.

3.3 The limitation of the protector approach

The protector approach has the following limitations. In [15], 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, 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 [18-20]. 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.

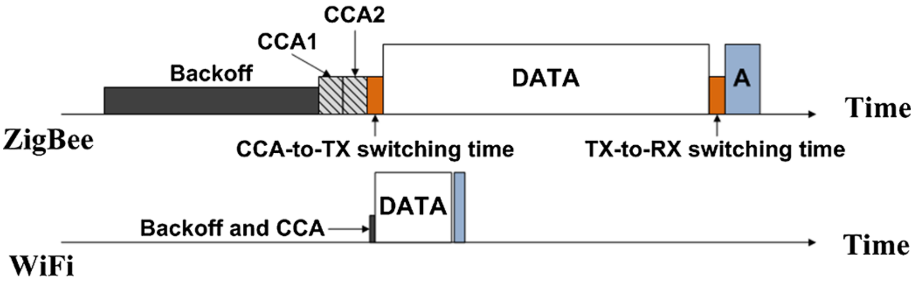

Figure 2 Basic operations of ZigBee and Wi-Fi.

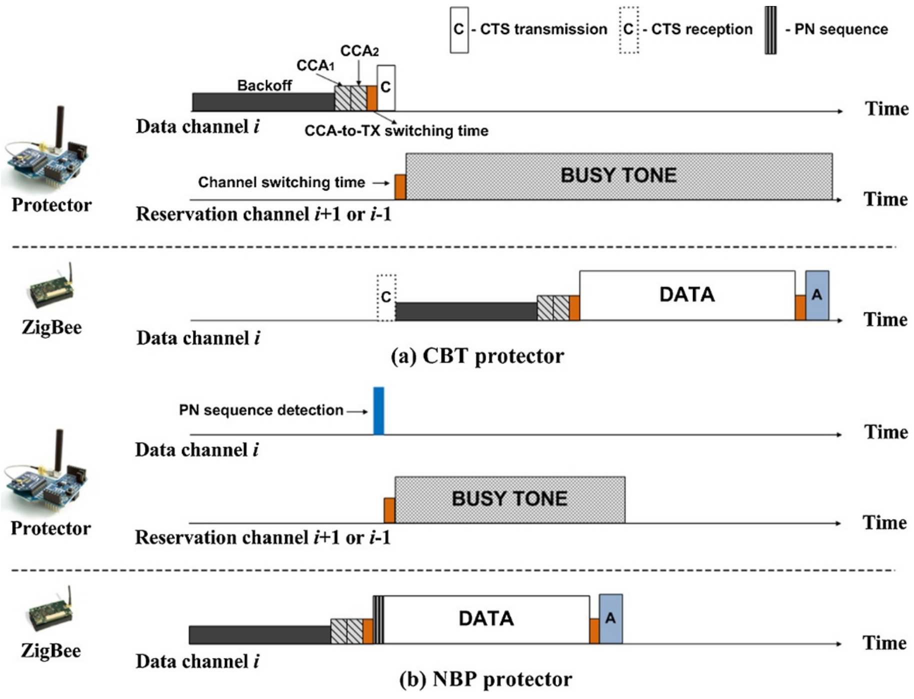

Figure 3 The basic operation of (a) the CBT protector and (b) the NBP protector.

4 NBP: Narrow Band Protection

4.1 Overview

Figure 3(b) 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).[a]

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.

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.

4.2 Cross-correlation with PN Codebook

NBP exploits the cross-correlation method [17] 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 has 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 $s[k]$, $1 \leq k \leq L$, refer to the pre-defined PN sequence, and $s^*[k]$ represents the complex conjugate. The correlation, $C(\Delta)$, at a shifted position Δ is:

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

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 k bits and thus there can be 2^k 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 m^{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 [17]. Therefore, a PN sequence does not require to be preceded by a preamble transmission.

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 (4 bytes - a typical ZigBee packet is about 100 bytes) and hence incurs little overhead in practice.

4.3 Discussions

A collision can still occur when the NBP protector is used to protect the ZigBee transmission. In Figure 4, 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.

The first collision case shown in Figure 4(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 NBP 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 under-utilized. 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. Table 1 summarizes the notations that will be used in our analysis.

5.2 Collision probability

For comparison, we first analyze the collision probability of the Cooperative Busy Tone (CBT) [15]. 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.

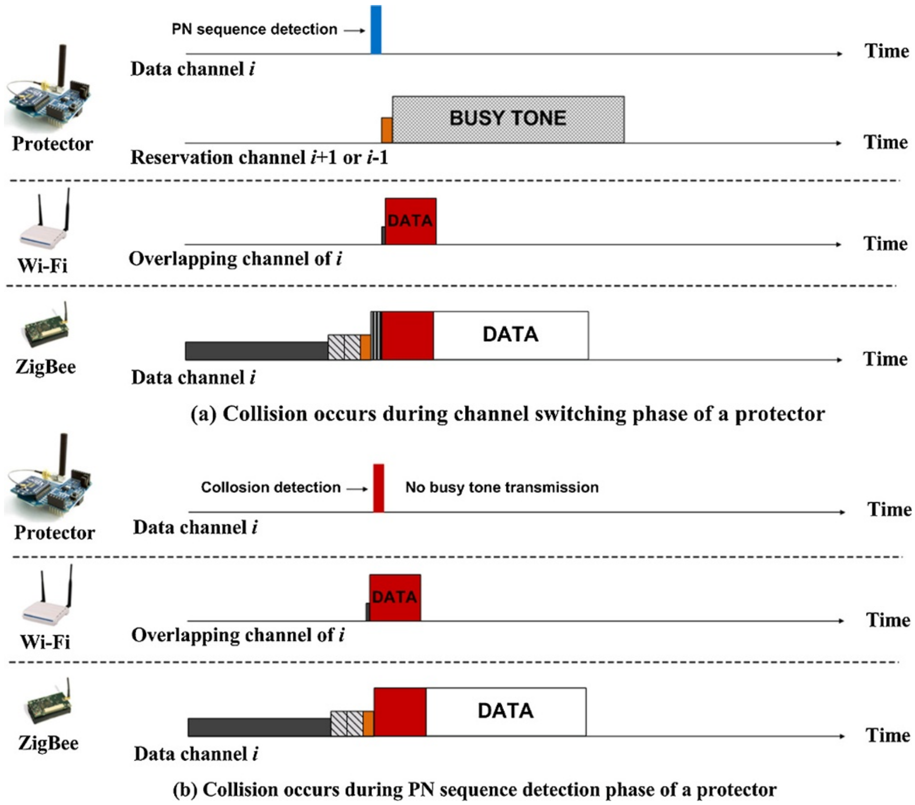
PN sequence detection
Data channel *i*
Time
Protector
BUSY TONE
Reservation channel *i*+1 or *i*-1
Time
Wi-Fi
DATA
Overlapping channel of *i*
Time
ZigBee
DATA
Data channel *i*
Time
(a) Collision occurs during channel switching phase of a protector
Collision detection
No busy tone transmission
Protector
Data channel *i*
Time
Wi-Fi
DATA
Overlapping channel of *i*
Time
ZigBee
DATA
Data channel *i*
Time
(b) Collision occurs during PN sequence detection phase of a protector

Figure 4 Collision cases when using the NBP protector.

Table 1 Notations

Notations	Meanings
λ_z	packet arrival rate for ZigBee
T_z	mean inter arrival time 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 [2]) 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
T_w	mean inter arrival time 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

However a collision may still occur during the control message exchange. The CBT needs to conduct the CCA-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. 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; 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:

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

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

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 [27], $R(t)$ 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:

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

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

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:

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

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

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 [15]. For CBT, the average renewal interval is derived as:

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

where $\gamma_{cbt} = 3J_z + \tau_{cts} + B_1 + 2U_z + \tau_z + \tau_{za}$ and P^{CBT}_s is the transmission success probability of CBT. γ_{cbt} 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 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:

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

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

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

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 4.3) 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:

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

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:

$$\Gamma^{NBP}_{w} = \frac{\tau_w}{\bar{T}^{NBP}_{w}} \tag{16}$$

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

$$\Gamma^{CBT}_{w} = \frac{\tau_w}{\bar{T}^{CBT}_{w}} \tag{17}$$

5.4 Multiple packet transmissions

By adopting the cross-correlation, the NBP protector 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

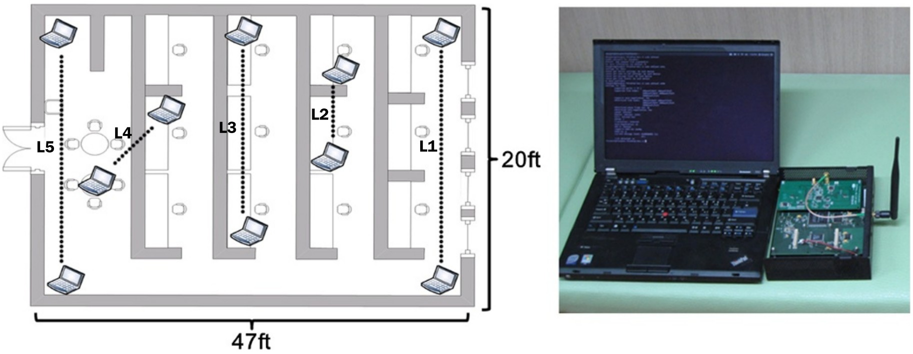

Figure 5 Experimental setup - the topology and the USRP platform.

Wi-Fi transmission. The throughput and average renewal interval for m transmissions are given by:

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

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

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 [28] running GNU Radio 3.4.2 [29]. We employ the basic UCLA ZigBee PHY module [30], and modify it to include the 4 byte-PN sequences at the beginning of the preamble. 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). To reliably detect the preamble, each chipping sequence becomes the shifted version of the other chipping sequences. Due to this property, if we insert the PN sequence prior to the DSSS spread, different PN sequences cannot be properly distinguished. For this reason, we insert the PN sequence after the chipping sequence conversion.

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 concurrently transmitting their PN sequences. We performed our experiments in our indoor lab (Figure 5) 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.

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) as shown in Figure 5. The Wi-Fi link L1 can only sense L2, L3 and L4 ZigBee links.

6.1.2 Experimental results

Figure 6 shows the false negative rate of detecting the PN sequences. As the SNR at the receiver increases, the false positive rate clearly decreases. The non-spread PN sequences do not incur false positives in correlation. The

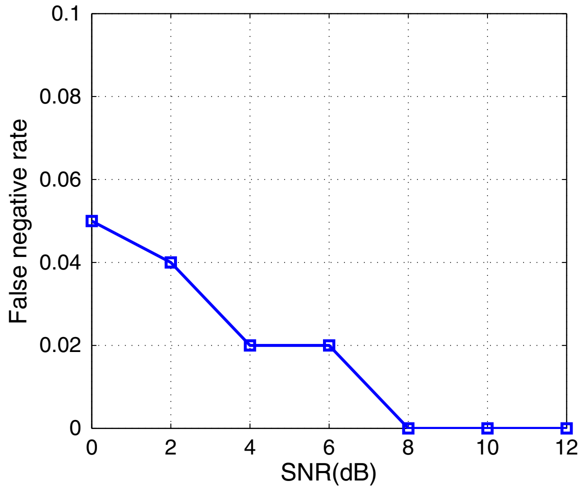

Figure 6 False negative rate vs. SNR.

false detection rates are below 0.05% in all cases, which validates that our cross-correlation method is feasible in practice.

Figure 7 shows the average erroneous bits of the 32-bit chipping sequence in the 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.

Figure 8 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 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.

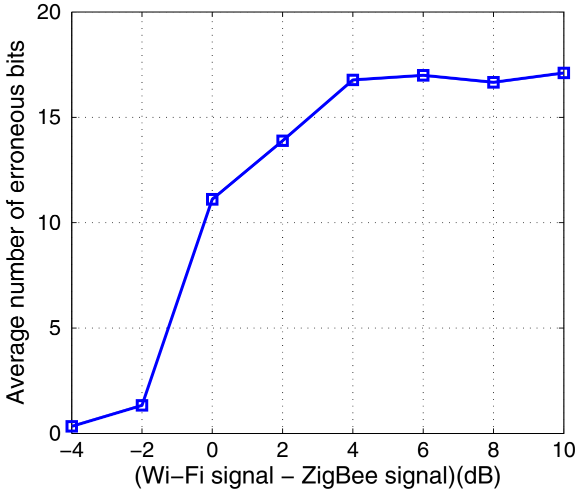

Figure 7 Average number of erroneous bits vs. increasing Wi-Fi interference.

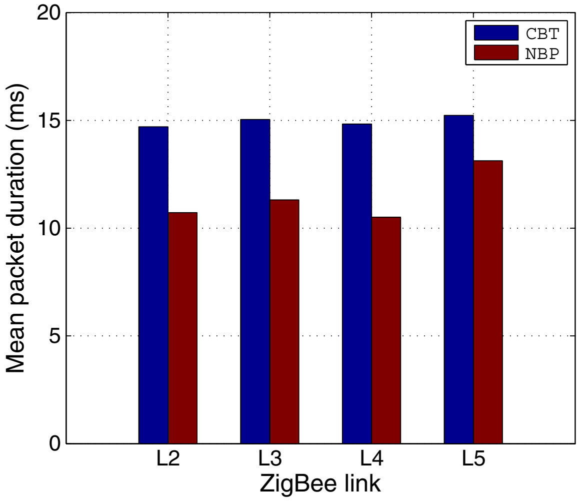

Figure 8 Mean packet duration of ZigBee links L2 - L5.

6.2 NS-2 simulations

6.2.1 Simulation setup

In this subsection we conduct NS-2 [31] 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.

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 and asymmetric 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.

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

Table 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

Link L5 is an asymmetric link.

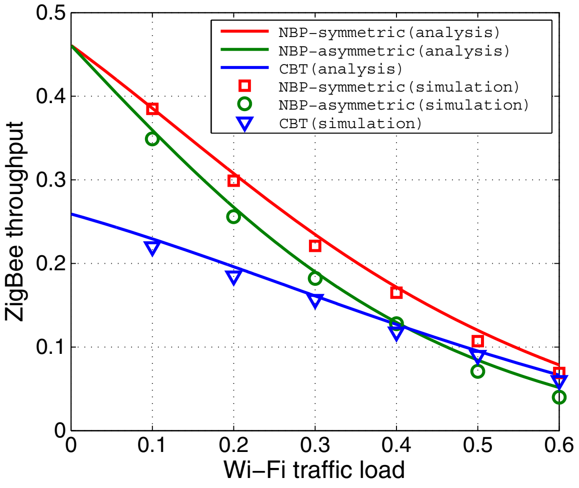

Figure 9 ZigBee Throughput vs. Wi-Fi traffic load.

traffic load as a normalized term, the ratio of packet arrival rate over the physical capacity:

$$\text{traffic load} = \frac{\text{packet size} \times \text{packet arrival rate}}{\text{PHY layer bitrate}} \tag{20}$$

6.2.2 Simulation results

Figure 9 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.

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

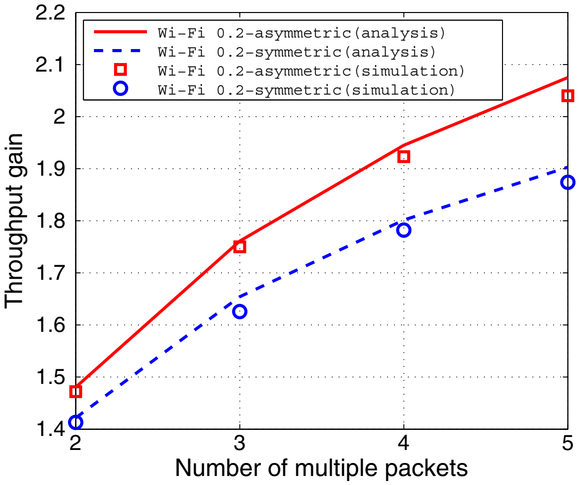

Figure 11 Throughput gain of ZigBee as a function of the number of multiple packets.

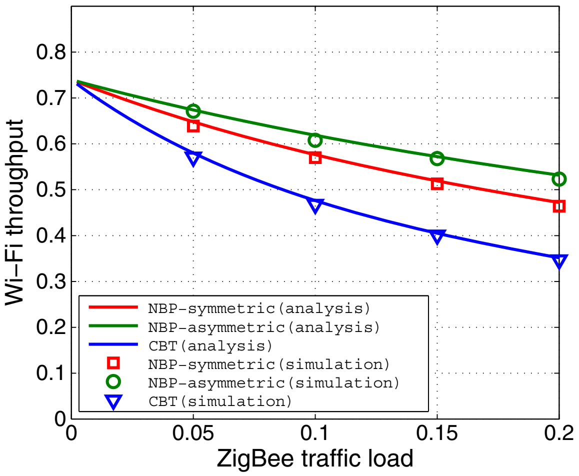

Figure 10 Wi-Fi throughput vs. ZigBee traffic load.

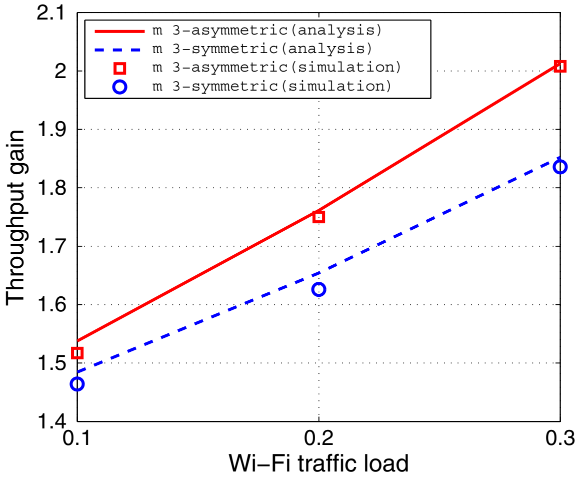

Figure 12 Throughput gain of ZigBee as a function of Wi-Fi traffic load.

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 [32,33], 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.

We next discuss the Wi-Fi performance under both schemes. Figure 10 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% $\sim$ 10%). Even under this scenario, the achievable throughput of Wi-Fi with NBP is greater than that with CBT.

Figure 11 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 12 shows the throughput gain of multiple packet transmissions 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.

7 Conclusion

This paper presented a new Narrow Band Protection scheme that addresses with 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 lightweight 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.

Endnote

[a] This is different from the previous scheme [15] where the protector sensed the medium on behalf of the ZigBee node.

Competing interests

The authors declare that they have no competing interests.

Acknowledgements

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MEST)(No.201208302002), the IT RND Program of MKE/KEIT [10035708, The Development of CPS (Cyber-Physical Systems) Core Technologies for High Confidential Autonomic Control Software] and the Industrial Strategic Technology Development Program (10041861, Development of Wired/Wireless i-AVB System Technology for Concurrent Transmission of HD Media and Control Data) funded by the Ministry of Knowledge Economy(MKE, Korea).

Author details

[1] Department of Computer Science, Seoul National University, Seoul, Korea. [2] Department of Software Design and Management, Gachon University, Seongnam, Korea.

Received: 9 December 2012 Accepted: 26 February 2013
Published: 19 March 2013

References

1. 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)
2. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specications. IEEE Std 802.11 (2007)
3. J Zhu, A Waltho, X Yang, X Guo, in *Proceedings of the 16th International Conference on Computer Communications and Networks (ICCCN)*. Multi-Radio Coexistence: challenges and opportunities (IEEE, Piscataway, NJ, USA, 2007), pp. 358–364. doi:10.1109/ICCCN.2007.4317845
4. S Gollakota, F Adib, D Katabi, S Seshan, in *Proceedings of ACM Sigcomm*. Clearing the RF Smog: Making 802.11 Robust to Cross-Technology Interference (ACM, New York, NY, USA, 2011), pp. 170-181. doi:10.1145/2018436.2018456
5. L Angrisani, M Bertocco, D Fortin, A Sona, Experimental study of coexistence issues between IEEE 802.11b and IEEE 802.15.4 wireless networks. IEEE trans. Instrum. Meas. **57**(8), 1514–1523 (2008)
6. R Gummadi, H Balakrishnan, S Seshan, in *Proceedings of First International Workshop on Communication Systems and Networks (COMSNETS)*. Metronome: coordinating spectrum sharing in heterogeneous wireless networks (IEEE, Piscataway, NJ, USA, 2009), pp. 157–166
7. Schneider Electrics, ZigBee Wi-Fi Coexistence (2008). http://www.zigbee.org/LearnMore/WhitePapers.aspx
8. CM Liang, NB Priyantha, J Liu, A Terzis, in *Proceedings of the 8th ACM Conference on Embedded Network Sensor Systems (SenSys)*. Surviving Wi-Fi interference in low power ZigBee networks (ACM, New York, NY, USA, 2010), pp. 309–322
9. S Pollin, I Tan, B Hodge, C Chun, A Bahai, in *Proceedings of the 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom)*. Harmful coexistence between 802.15.4 and 802.11: A measurement-based study (IEEE, Piscataway, NJ, USA, 2008), pp. 1–6. doi:10.1109/CROWNCOM.2008.4562460
10. A Sikora, VF Groza, in *Proceedings of the IEEE Instrumentation and Measurement Technology Conference (IMTC)*. Coexistence of IEEE 802.15.4 with other systems in the 2.4Ghz-ISM band (IEEE, Piscataway, NJ, USA, 2005), pp. 1786–1791. doi:10.1109/IMTC.2005.1604479
11. C Won, J Youn, H Ali, H Sharif, J Deogun, in *Proceedings of the 62nd IEEE Vehicular Technology Conference (VTC)*. Adaptive radio channel allocation for supporting coexistence of 802.15.4 and 802.11b (IEEE, Piscataway, NJ, USA, 2005), pp. 2522–2526. doi:10.1109/VETECF.2005.1559004

12. S Pollin, M Ergen, A Dejonghe, L Perre, F Catthoor, I Moerman, A Bahai, in *Proceedings of the first International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom)*. Distributed cognitive coexistence of 802.15.4 with 802.11 (IEEE, Piscataway, NJ, USA, 2006), pp. 1–5. doi:10.1109/CROWNCOM.2006.363456
13. L Tang, Y Sun, O Gurewitz, DB Johnson, in *Proceedings of the 12th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*. EM-MAC: A Dynamic Multichannel Energy-Efficient MAC protocol for wireless sensor networks (ACM, New York, NY, USA, 2011), p. 11. doi:10.1145/2107502.2107533
14. J Huang, G Xing, G Zhou, R Zhou, in *Proceedings of the 18th IEEE International Conference on Network Protocols (ICNP)*. Beyond Co-existence: exploiting Wi-Fi white space for ZigBee performance assurance (IEEE, Piscataway, NJ, USA, 2010), pp. 305–314. doi:10.1109/ICNP.2010.5762779
15. X Zhang, G Kang Shin, in *Proceedings of the 12th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*. Enabling coexistence of heterogeneous wireless systems: case for ZigBee and Wi-Fi (ACM, New York, NY, USA, 2011), p. 11. doi:10.1145/2107502.2107510
16. S Gollakota, D Katabi, in *Proceedings of ACM Sigcomm*. Zig-Zag Decoding: combating hidden terminals in wireless networks (ACM, New York, NY, USA, 2008), pp. 159–170. doi:10.1145/1402958.1402977
17. S Sen, RR Choudury, S Nelakuditi, in *Proceedings of ACM MobiCom*. CSMA/CN: Carrier Sense Multiple Access with Collision Notification (ACM, New York, NY, USA, 2010), pp. 25–36. doi:10.1145/1859995.1859999
18. S Duquennoy, F Osterlind, A Dunkels, in *Proceedings of the 9th ACM Conference on Embedded Network Sensor Systems (SenSys)*. "Lossy links, low power, high throughput" (ACM, New York, NY, USA, 2011), pp. 12–25. doi:10.1145/2070942.2070945
19. M Anwander, G Wagenknecht, T Braun, K Dolfus, in *Proceedings of the International Conference on Networked Sensing Systems (INSS)*. Beam: A burst-aware energy-efficient adaptive mac protocol for wireless sensor networks (IEEE, Piscataway, NJ, USA, 2010), pp. 195–202. doi:10.1109/INSS.2010.5573142
20. F Osterlind, L Mottola, T Voigt, N Tsiftes, A Dunkels, in *Proceedings of the 11th ACM/IEEE Conference on Information Processing in Sensor Networks (IPSN)*. "Strawman: Resolving collisions in Bursty low-power wireless networks" (ACM, New York, NY, USA, 2012), pp. 161–172. doi:10.1145/2185677.2185729
21. I Howitt, WLAN and WPAN coexistence in UL band. IEEE Trans. Veh. Technol. **50**(4), 1114–1124 (2001)
22. I Howitt, J Gutierrez, in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE 802.15.4 low rate-wireless personal area network coexistence issues (IEEE, Piscataway, NJ, USA, 2003), pp. 1481–1486. doi:10.1109/WCNC.2003.1200605
23. S Shin, H Park, S Choi, W Kwon, Packet error rate Analysis of ZigBee under WLAN and bluetooth interferences. IEEE Trans. Wireless Commun. **6**(8), 2825–2830 (2007)
24. S Shin, H Park, W Kwon, Mutual interference analysis of IEEE 802.15. 4 and IEEE 802.11b. Comput. Netw. **51**(12), 3338–3353 (2007)
25. J Hou, B Chang, D Cho, M Gerla, in *Proceedings of 4th International Conference on Body Area Networks Bodynets (BodyNets)*. Minimizing 802.11 interference on ZigBee medical sensors (ICST, Brussels, Belgium, 2009), p. 8. doi:10.4108/ICST.BODYNETS2009.6029
26. E Magistretti, O Gurewitz, EW Knightly, in *Proceedings of ACM MobiCom*. 802.11ec: Collision Avoidance without Control Messages (ACM, New York, NY, USA, 2012), pp. 65–76. doi:10.1145/2348543.2348555
27. SM Ross, *Stochastic process*, second edition, (1996)
28. Ettus Research, http://www.ettus.com, Accessed Dec. 2012
29. GNU Radio Project, http://gnuradio.org/redmine/wiki/gnuradio, Accessed Dec. 2012
30. UCLA ZigBee PHY, https://www.cgran.org/wiki/UCLAZigBee, Accessed Dec. 2012
31. Network simulator 2, http://www.isi.edu/nsnam/ns/, Accessed Dec. 2012
32. Crawdad data set umd/sigcomm 2008 (v. 2009-03-02), http://crawdad.cs.dartmouth.edu/umd/sigcomm2008, Accessed Dec. 2012
33. Crawdad data set microsoft/osdi2006 (v. 2007-05-23), http://crawdad.cs.dartmouth.edu/microsoft/osdi2006, Accessed Dec. 2012

doi:10.1186/1687-1499-2013-76
Cite this article as: Lim *et al.*: **NBP: light-weight Narrow Band Protection for ZigBee and Wi-Fi coexistence.** *EURASIP Journal on Wireless Communications and Networking* 2013 **2013**:76.